Lecture 7 — Direct Proof, Counterexample

Table of contents

Learning goals . . . 1
Definitions to know . . . 1
Two facts, and where "not prime" bites . . . 2
Proof or disproof of $\forall x \in D, P(x) \to Q(x)$ . . . 3
Worked: which values give a counterexample? (pre-class Q1) . . . 3
Example proof . . . 5
Worked: if $x + 6 = 4y$ then $\frac{x}{2}$ is odd . . . 5
Worked: prove or disprove . . . 6
Worked: disprove by proving the negation . . . 7
See also . . . 7

Pre-work: Video 009 (Direct Proofs and Counterexamples). First lecture of the number theory and methods of proof topic — see proof-techniques[1] for the reference definitions, proof templates and the catalogue of common proof errors.

Learning goals

- How to write a direct proof.
- How to disprove a statement by exhibiting a counterexample.

Definitions to know

Proofs and disproofs need the precise definitions of even, odd, prime, composite, rational, divides, … Each of the six below is a **biconditional**, because a proof reads a definition in both directions: unfolding it in the hypothesis, and folding it back up in the conclusion.

[1] courses/math1061/proof-techniques.pdf

n is an **even** integer	$\leftrightarrow$	$n = 2k$ for some integer k
n is an **odd** integer	$\leftrightarrow$	$n = 2k + 1$ for some integer k
n is a **prime** number	$\leftrightarrow$	$n \in \mathbb{Z}$, $n > 1$, and $\forall r, s \in \mathbb{Z}^+$, if $n = rs$ then ($r = 1$ and $s = n$) or ($r = n$ and $s = 1$)
n is a **composite** number	$\leftrightarrow$	$n \in \mathbb{Z}$, $n > 1$, and $\exists r, s \in \mathbb{Z}^+$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$
r is a **rational** number	$\leftrightarrow$	$\exists a, b \in \mathbb{Z}$ such that $r = \frac{a}{b}$ and $b \neq 0$
$d \mid n$	$\leftrightarrow$	$d \neq 0$ and $n = dk$ for some integer k

Two points about these definitions:

- **"Odd" has a second, equally valid form.** $n = 2k+1$ for some integer k and $n = 2k-1$ for some integer k are equivalent: they define the same set, and you may finish a proof in whichever form drops out of the algebra. The proof that $\frac{x}{2}$ is odd, below, is where it pays off: it lands on the $2k - 1$ form.
- **The $b \neq 0$ in the definition of rational is its own requirement**, separate from $r = \frac{a}{b}$. A "rational" claim is two claims: that the fraction exists, *and* that its denominator is non-zero. Dropping the second half is the standard way to lose the mark — see rational-and-irrational-numbers[2].

How much detail to give in a proof. Demonstrate facts **using the definitions**. That is the whole answer, and it is why the definitions come first.

Two facts, and where "not prime" bites

> **Fact**: the sum, difference, and product of integers is an integer.
>
> **Fact**: every integer is either even or odd.

The first is what licenses lines like "since $k \in \mathbb{Z}$, we have $3k + 2 \in \mathbb{Z}$" — cheap, but it has to be *said*, because the definition of odd demands an integer witness and nothing else supplies it.

What "not prime" means. For $n \in \mathbb{Z}^{>1}$, "n is not prime" means "n is composite". For $n \in \mathbb{Z}$ generally, "n is not prime" means "composite **or** $n \leq 1$". Primality and compositeness only carve up the integers from 2 upwards; 1, 0 and the negatives are in neither class.

[2] courses/math1061/rational-and-irrational-numbers.pdf

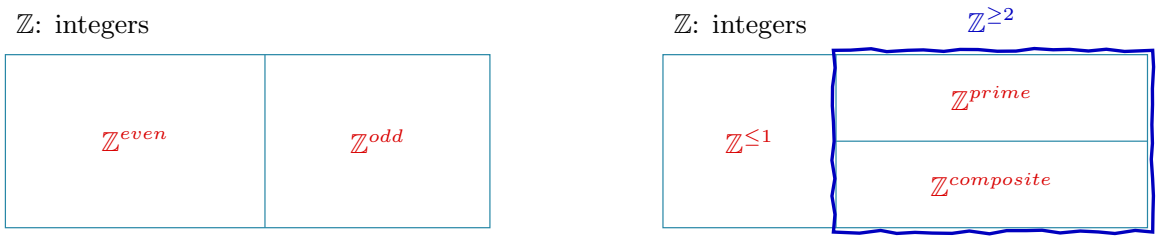

Figure 1: Two ways of splitting $\mathbb{Z}$. Left: even and odd exhaust the integers, which is what makes 'every integer is either even or odd' usable as a case split. Right: prime and composite do *not* — they only partition $\mathbb{Z}^{\geq 2}$, and everything from 1 downwards falls in $\mathbb{Z}^{\leq 1}$. The heavy blue box round the two right-hand cells marks $\mathbb{Z}^{\geq 2}$, the same restriction as $\mathbb{Z}^{>1}$.

The asymmetry between the two panels is the point. The left one is a genuine two-case split you may argue by; the right one is not, and a proof that reasons "n is not prime, so n is composite" is only sound once $n \geq 2$ has been established. The proof about $n^2 + 5n + 6$ below turns on exactly that.

Proof or disproof of $\forall x \in D, P(x) \to Q(x)$

Every method in this topic attacks one row of the truth table for $p \to q$: the only row that makes it false is p true, q false.

Why a direct proof supposes $P(x)$ is true. $P(x) \to Q(x)$ would still be true if $P(x)$ is false, so that case needs no argument. We just need to rule out the case that $P(x)$ is true and $Q(x)$ is false — so we suppose $P(x)$ is true and prove that in this case $Q(x)$ must also be true. The other three rows of the table are true for free, so there is nothing to do in them.

The mirror image is what makes a counterexample work: because the statement fails as soon as *one* x occupies that row, exhibiting one such x is a complete disproof. See conditional-statements[3] for the truth table itself.

Worked: which values give a counterexample? (pre-class Q1)

Which values for m and n give a counterexample disproving: *for all integers m and n, if $2m+n$ is odd, then m and n are both odd*?

[3] courses/math1061/conditional-statements.pdf

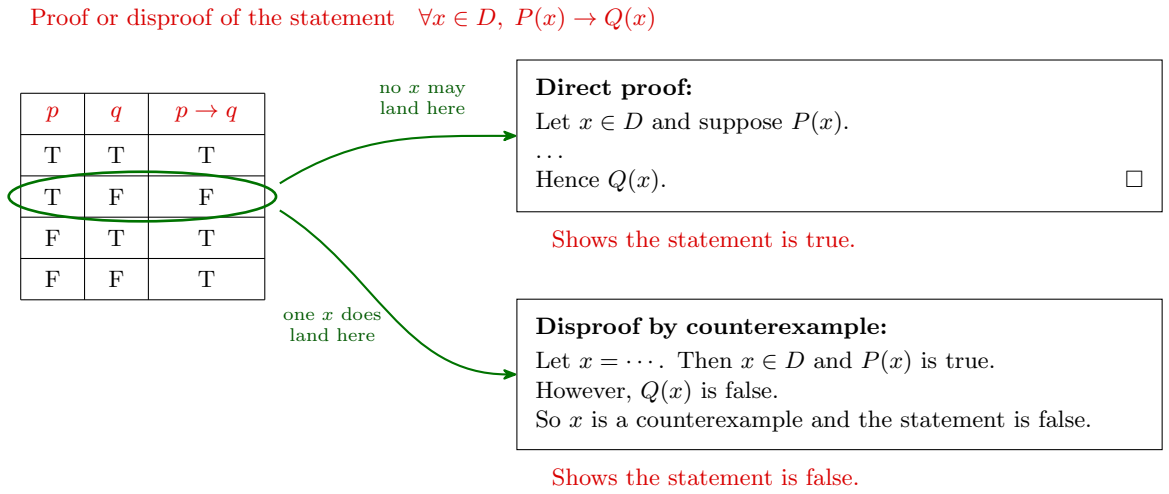

Figure 2: The truth table for $p \to q$ beside the skeletons of a direct proof and a disproof by counterexample. The green ring marks the T-F-F row: it is the only row that can make $P(x) \to Q(x)$ false, so it is the only row either method has to deal with. A direct proof shows *no* $x \in D$ can land there; a counterexample exhibits *one* x that does. The two green arrows join that row to the two skeletons.

	Check	Verdict
a. $m = 3, n = 5$	$2(3) + 5 = 11$ odd, but m, n are both odd — so q is **true**	not a counterexample
b. $m = 3, n = 6$	$2(3) + 6 = 12$ even — so p is **false**	not a counterexample
c. $m = 4, n = 5$	$2(4) + 5 = 13$ odd, and m, n are **not** both odd (at least one is even)	**counterexample**
d. $m = 4, n = 6$	$2(4) + 6 = 14$ even — so p is **false**	not a counterexample

For a counterexample to $p \to q$ we require p **true** and q **false**. Options (b) and (d) fail for the opposite reason to (a): they never even engage the statement, because a conditional with a false hypothesis is true and so proves nothing either way.

The wording for (c) matters: not "m and n are both even", but "**not both** m, n are odd — at least one is even". Negating "both odd" gives "at least one is even", not "both even". That is the De Morgan step this question is testing. See 2026-08-06-negation-and-multiple-quantifiers[4].

[4] courses/math1061/2026-08-06-negation-and-multiple-quantifiers.pdf

Example proof

$\forall n \in \mathbb{Z}$, if n is odd then $3n+2$ is odd.

$\forall n \in \mathbb{Z}$, if $\underbrace{n \text{ is odd}}_{P(n)}$ then $\underbrace{3n+2 \text{ is odd.}}_{Q(n)}$

Proof: Let $n \in \mathbb{Z}$ and suppose n is odd. ← hypothesis

Since n is odd, $n = 2k+1$ for some $k \in \mathbb{Z}$. ← the witness for "n is odd"

$$\begin{aligned} \text{Now } 3n+2 &= 3(2k+1)+2 \\ &= 6k+5 \\ &= 2(3k+2)+1 \end{aligned}$$

← the witness for "$3n+2$ is odd"

Since $k \in \mathbb{Z}$, we have $3k+2 \in \mathbb{Z}$.

Hence $3n+2$ is odd. $\square$ ← conclusion

Figure 3: The anatomy of a direct proof. The opening line is boxed, the purple margin labels mark the *hypothesis* and the *conclusion*, and the orange underlines and margin captions mark the two integer witnesses. The blue underlines on the statement pick out its two halves, $P(n)$ and $Q(n)$, which ties the proof back to the skeleton above.

The shape to memorise:

1. **State the hypothesis** in the skeleton's words — `Let n  and suppose n is odd.`
2. **Unfold the definition**, naming a witness: $n = 2k+1$ for some $k \in \mathbb{Z}$.
3. **Do the algebra until the target definition is visible** — $6k+5$ is not obviously odd; $2(3k+2)+1$ is, because it matches the shape $2(\text{integer})+1$ exactly.
4. **Confirm the new witness is an integer**, by the Fact above.
5. **State the conclusion** in the target's own words.

Step 4 is the one most often skipped. $2(3k+2)+1$ only certifies "odd" if $3k+2$ is an integer, and saying so costs one line.

Worked: if $x+6=4y$ then $\frac{x}{2}$ is odd

For any integer x, if $x+6=4y$ for some integer y, then $\frac{x}{2}$ is an odd integer.

Proof. Let $x \in \mathbb{Z}$ and suppose $x+6=4y$ for some $y \in \mathbb{Z}$. Now $x = 4y-6$, so $x = 2(2y-3)$. Hence $\dfrac{x}{2} = \dfrac{2(2y-3)}{2} = 2y-3 = 2(y-1)-1$. Thus, because $y \in \mathbb{Z}$, we have $2y-3 \in \mathbb{Z}$ so $\frac{x}{2} \in \mathbb{Z}$; and $y-1 \in \mathbb{Z}$, so by definition $\frac{x}{2}$ is odd. $\square$

Three things this proof drills:

- **The hypothesis is itself existential.** "$x + 6 = 4y$ for some integer y" hands you a y; the opening line accepts it by name and the rest of the proof uses it.
- **The conclusion is a conjunction, and both halves need discharging.** $\frac{x}{2}$ must be shown to be an *integer* (via $2y - 3 \in \mathbb{Z}$) and to have the *odd* form. Neither half implies the other.
- **Either form of "odd" finishes it.** The proof ends on $2(y-1)-1$, and $2(y-2)+1$ does just as well. This is the $n = 2k - 1$ equivalence from the definitions, cashed in.

Worked: prove or disprove

The primes begin $2, 3, 5, 7, 11, ...$

(a) There are distinct integers m and n such that $\frac{1}{m} + \frac{1}{n}$ is an integer.

True. Take $m = 1$ and $n = -1$. Then $\frac{1}{m} + \frac{1}{n} = 1 + (-1) = 0 \in \mathbb{Z}$.

The statement is existential, so one witness *is* the proof — the opposite of the situation with $n^2 + 5n + 6$ below. The word **distinct** matters: it rules out the easy $m = n = 1$, so the witness uses a negative integer instead.

(b) $\forall n \in \mathbb{Z}^{\geq 2}$, n is composite or $n + 1$ is composite.

False. Take $n = 2$: then $n = 2$ and $n + 1 = 3$, which are both prime.

This one is a universal statement that is *not* a conditional — the predicate is a disjunction. So the counterexample has to falsify the disjunction outright, i.e. make **both** disjuncts false, which here means finding two consecutive primes. $n = 2$ is the *only* value that works, because for $n \geq 3$ one of n, $n + 1$ is even and bigger than 2, hence composite.

(c) For each integer $n \geq 2$, the product of the first n prime numbers minus 1 is prime.

False. Try $n = 2, 3, 4, ...$ in turn. Take $n = 4$:

$$2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19 \quad \text{— composite.}$$

The two values before it: $n = 2$ gives $2 \cdot 3 - 1 = 5$, prime; $n = 3$ gives $2 \cdot 3 \cdot 5 - 1 = 29$, prime. So the first two cases both hold and the claim only breaks at the third. That is why "arguing from examples" is on the list of common proof errors in proof-techniques[5]. A pattern surviving two checks is not evidence of anything.

[5] courses/math1061/proof-techniques.pdf

Worked: disprove by proving the negation

Show that $\exists n \in \mathbb{Z}^+$ such that n^2+5n+6 is prime is false, by proving the negation.

The statement is existential, so a counterexample won't do — one bad n says nothing about whether some *other* n works. Negating it turns it into a universal, and that has to be proved outright:

> Negation: $\forall n \in \mathbb{Z}^+$, n^2+5n+6 is composite.
>
> *Proof of the negation.* Let $n \in \mathbb{Z}^+$. Now $n^2+5n+6 = (n+2)(n+3)$. Since $n \geq 1$ we have $n+2 > 1$ and $n+3 > 1$. Thus n^2+5n+6 is composite. $\square$

The original statement is false (**F**) and its negation is true (**T**). The step from "not prime" to "composite" needs a justification: because $n \geq 1$ we have $n^2+5n+6 \geq 2$, so "not prime" is "composite". The value sits in $\mathbb{Z}^{\geq 2}$, the region of Figure 1 where the two really do coincide. Without that check the negation of "prime" would also have to admit values ≤ 1.

One small gap to close: the proof gives only the two "> 1" halves, but the definition of composite asks for factors with $1 < r < n$ **and** $1 < s < n$. Here each factor is also strictly less than the product, since the other factor exceeds 1 — so $n+2 < (n+2)(n+3)$ and $n+3 < (n+2)(n+3)$, and the definition is met in full.

The general move — **to disprove $\exists x \in D$ such that $P(x)$, prove $\forall x \in D, \sim P(x)$** — is the quantifier negation rule from 2026-08-06-negation-and-multiple-quantifiers[6] used as a proof strategy. It generalises: a universal falls to one counterexample, an existential needs a universal proof.

See also

- proof-techniques[7] · quantified-statements[8] · conditional-statements[9]
- rational-and-irrational-numbers[10] · divisibility-and-factorisation[11] — the two definitions from the table that get their own notes
- 2026-08-13-proof-by-contradiction[12] — Lecture 8, which adds a third skeleton to the two above
- 2026-08-13-proof-by-contraposition[13] — Lecture 9, which adds the fourth

[6] courses/math1061/2026-08-06-negation-and-multiple-quantifiers.pdf
[7] courses/math1061/proof-techniques.pdf
[8] courses/math1061/quantified-statements.pdf
[9] courses/math1061/conditional-statements.pdf
[10] courses/math1061/rational-and-irrational-numbers.pdf
[11] courses/math1061/divisibility-and-factorisation.pdf
[12] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[13] courses/math1061/2026-08-13-proof-by-contraposition.pdf

- math1061-diagram-notation[14] — the house conventions the figures above follow
- practice-problems[15] — §9 Direct Proofs and Counterexamples, with full worked solutions

[14] courses/math1061/math1061-diagram-notation.pdf
[15] courses/math1061/practice-problems.pdf