Proof Techniques — Direct, Counterexample, Contradiction, Contraposition

Table of contents

The four methods for establishing (or demolishing) a statement of the form $\forall x \in D, P(x) \to Q(x)$, plus the definitions every proof in this course is expected to unfold.

Definitions to prove from

Proofs are written by **demonstrating facts using the definitions** — so these have to be at your fingertips. Each is a biconditional: it can be used in either direction.

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

Two facts used constantly, and worth naming explicitly when you lean on them:

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

Prime vs. not-prime. 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 "n is composite **or** $n \leq 1$" — the integers split into $\mathbb{Z}^{\leq 1}$, $\mathbb{Z}^{\text{prime}}$, and $\mathbb{Z}^{\text{composite}}$, and 1 and everything below it is in none of the latter two. This is why $n = 1$ is the standard counterexample to "every positive integer is prime or composite".

Warning: don't assume something that seems like an "obvious fact" until you have proven it, or can name the lecture or pre-work video it was proved in.

The four methods

All four target $\forall x \in D, P(x) \to Q(x)$. Recall the truth table for $p \to q$ — the only row that makes it false is p true, q false:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Every method below is a different way of attacking that one row.

Direct proof (shows the statement is true)

> Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$. $\square$

Why suppose $P(x)$ is true, when $P(x) \to Q(x)$ holds anyway if $P(x)$ is false? Because the only case that could make the statement false is $P(x)$ true and $Q(x)$ false. Ruling that out is the whole job — the $P(x)$-false rows are true for free.

Disproof by counterexample (shows the statement is false)

> Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true. However, $Q(x)$ is false. So x is a counterexample and the statement is false.

A counterexample to $p \to q$ needs p **true** and q **false** — a value where the hypothesis fails proves nothing.

Proof by contradiction (shows the statement is true)

> Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true. That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false. ... Hence something obviously wrong — $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$. This is a contradiction, and we conclude the original statement is true. □

The set-up comes straight from quantified-statements[1]: the negation of $\forall x \in D, P(x) \to Q(x)$ is $\exists x \in D$ such that $P(x) \wedge \sim Q(x)$.

Useful negations to have ready (see logical-equivalence-laws[2]):

$$\sim (p \vee q) \equiv \sim p \wedge \sim q \qquad \sim (p \wedge q) \equiv \sim p \vee \sim q \qquad \sim (p \to q) \equiv p \wedge \sim q$$

Proof by contraposition (shows the statement is true)

> We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely $\forall x \in D, \sim Q(x) \to \sim P(x)$. Let $x \in D$ and suppose $\sim Q(x)$. ... Hence $\sim P(x)$. □

This is valid because $p \to q \equiv \sim q \to \sim p$ (see conditional-statements[3]).

Choosing a method

- **Contradiction is the most versatile**, but it needs more set-up, so a direct proof is often easier when one is available.
- **Contraposition** is the natural choice when $\sim Q(x)$ gives you something concrete to work with and $P(x)$ doesn't — typically when the conclusion is a negative statement ("r is irrational", "n is odd") whose negation is a definition you can expand.
- **Contradiction vs. contraposition**: a contraposition proof is a contradiction proof that never actually needs the assumption $P(x)$ — you derive $\sim P(x)$ from $\sim Q(x)$ alone. If your "contradiction" proof only ever uses the $\sim Q(x)$ half of the assumption, write it as a contraposition instead.
- **Counterexample vs. contradiction**: counterexample is a **disproof**, contradiction is a **proof**. They are not variants of each other.

Worked comparisons on the same statements live in the lecture notes: 2026-08-13-proof-by-contradiction[4] proves $\forall n \in \mathbb{Z}$, if n is odd then $3n + 2$ is odd both directly and by contradiction,

[1] courses/math1061/quantified-statements.pdf
[2] courses/math1061/logical-equivalence-laws.pdf
[3] courses/math1061/conditional-statements.pdf
[4] courses/math1061/2026-08-13-proof-by-contradiction.pdf

and 2026-08-13-proof-by-contraposition[5] works through statements where one method gets stuck and another doesn't.

Worked examples

Direct proof

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

Let $n \in \mathbb{Z}$ and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Now

$$3n+2 = 3(2k+1)+2 = 6k+5 = 2(3k+2)+1.$$

Since $k \in \mathbb{Z}$, we have $3k+2 \in \mathbb{Z}$, and hence $3n+2$ is odd. $\square$

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

Let $x \in \mathbb{Z}$ and suppose $x+6=4y$ for some $y \in \mathbb{Z}$. Then $x = 4y-6 = 2(2y-3)$, so

$$\frac{x}{2} = \frac{2(2y-3)}{2} = 2y-3 = 2(y-1)-1.$$

Since $y \in \mathbb{Z}$ 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. $\square$

The sum of any pair of even integers is even.

Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence $m+n = 2k+2\ell = 2(k+\ell)$, which is even. $\square$

$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2-5n+2$ is composite.

Suppose $n \in \mathbb{Z}^+$ and $n \geq 4$. Factor $2n^2-5n+2 = (2n-1)(n-2)$. Since $n \geq 4$, we have $2n-1 \geq 7$ and $n-2 \geq 2$, so both factors are integers greater than 1. Hence the expression is composite. $\square$

[5] courses/math1061/2026-08-13-proof-by-contraposition.pdf

Disproof by counterexample

- **For all integers m and n, if $2m+n$ is odd then m and n are both odd.** Counterexample $m=4, n=5$: $2(4)+5=13$ is odd, but m is even. (Not $m=3, n=5$ — there the conclusion holds; not $m=3, n=6$ or $m=4, n=6$ — there the hypothesis fails.)
- **$\forall n \in \mathbb{Z}^{\geq 2}$, n is composite or $n+1$ is composite.** Take $n=2$: both 2 and 3 are prime.
- **For each integer $n \geq 2$, the product of the first n primes minus 1 is prime.** Take $n=4$: $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, composite.
- **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** Take $x=1, y=-2$: $4 > 1$ but $-2 \not> 1$.
- **$\forall x \in \mathbb{R}, \lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** Take $x = \frac{3}{2}$: $\lfloor \frac{9}{4} \rfloor = 2$ but $\lfloor \frac{3}{2} \rfloor^2 = 1$. (See modular-arithmetic[6] for the floor function.)

Disproof by proving the negation

When the statement to disprove is existential, a single counterexample isn't available — you must prove the universal negation.

$\exists n \in \mathbb{Z}^+$ such that n^2+5n+6 is prime. This is false; the negation is $\forall n \in \mathbb{Z}^+$, n^2+5n+6 is composite.

> Let $n \in \mathbb{Z}^+$. Now $n^2+5n+6 = (n+2)(n+3)$. Since $n \geq 1$ we have $n+2 > 1$ and $n+3 > 1$, so n^2+5n+6 is composite. $\square$

(Because $n \geq 1$ forces $n^2+5n+6 \geq 2$, "not prime" here does mean "composite".)

There is an even integer n such that $5n-4$ is prime. False; prove $\forall n \in \mathbb{Z}^{\text{even}}$, $5n-4$ is not prime.

> Suppose n is even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $5n-4 = 10k-4 = 2(5k-2)$, which is even. The only even prime is 2; if $2(5k-2) = 2$ then $k = \frac{3}{5} \notin \mathbb{Z}$. Therefore $5n-4$ is not prime. $\square$

Proof by contradiction

$\forall m, n \in \mathbb{Z}$, if mn is even, then m is even or n is even.

> Suppose $\exists m, n \in \mathbb{Z}$ such that mn is even and both m and n are odd. Since m is odd, $m = 2k+1$ for some $k \in \mathbb{Z}$; since n is odd, $n = 2\ell+1$ for some $\ell \in \mathbb{Z}$ — **a new variable**, since m and n need not be equal. Now
>
> $$mn = (2k+1)(2\ell+1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1.$$

[6] courses/math1061/modular-arithmetic.pdf

Since $k, \ell \in \mathbb{Z}$, $2k\ell + k + \ell \in \mathbb{Z}$, so mn is odd. It is impossible for mn to be both even and odd, a contradiction. Therefore the original statement is true. $\square$

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

Suppose the statement is false: $\exists n \in \mathbb{Z}$ such that $3n^3 - 2$ is odd and n is even. Since n is even, $n = 2a$ for some $a \in \mathbb{Z}$. Then

$$3n^3 - 2 = 3(2a)^3 - 2 = 24a^3 - 2 = 2(12a^3 - 1).$$

Since $a \in \mathbb{Z}$, $12a^3 - 1 \in \mathbb{Z}$, so $3n^3 - 2$ is even — a contradiction. Therefore the original statement is true. $\square$

$\forall m, n \in \mathbb{Z}$, if $m + n$ is even, then m and n are both even or both odd.

Suppose the statement is false. Then $\exists m, n \in \mathbb{Z}$ such that $m + n$ is even but exactly one of m, n is even. **Without loss of generality**, assume m is even and n is odd — the other case (m odd, n even) follows because $m + n = n + m$. Thus $m = 2a$ for some $a \in \mathbb{Z}$ and $n = 2b + 1$ for some $b \in \mathbb{Z}$. Now $m + n = 2a + 2b + 1 = 2(a + b) + 1$, and $a + b \in \mathbb{Z}$, so $m + n$ is odd. This contradicts the assumption that $m + n$ is even. Therefore the original statement is true. $\square$

For integers a and b, if $6a + 3b$ is odd, then b is odd.

Suppose there exist integers a, b with $6a + 3b$ odd and b even. Then $b = 2k$ for some $k \in \mathbb{Z}$, so $6a + 3b = 6a + 6k = 2(3a + 3k)$, which is even — contradicting that $6a + 3b$ is odd. $\square$

For all positive integers x and y, $x^2 - y^2 \neq 1$.

Suppose $x, y \in \mathbb{Z}^+$ with $x^2 - y^2 = 1$. Factoring, $1 = (x - y)(x + y)$. Since x, y are positive integers we must have $x - y = 1$ and $x + y = 1$, so $2x = 2$ and $x = 1$; then $y = 0$, which is not a positive integer — a contradiction. $\square$

Proof by contraposition

$\forall r \in \mathbb{R}$, if r^2 is irrational, then r is irrational.

We prove the contrapositive: $\forall r \in \mathbb{R}$, if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$. Suppose $r \in \mathbb{R}$ with $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Now $r^2 = \frac{a^2}{b^2}$. Since $a, b \in \mathbb{Z}$ we have $a^2, b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ since $b \neq 0$. So $r^2 \in \mathbb{Q}$. $\square$

$\forall m, n \in \mathbb{Z}$, if mn is odd, then m and n are both odd.

We prove the contrapositive: $\forall m, n \in \mathbb{Z}$, if at least one of m, n is even then mn is even. Without loss of generality, assume m is even, so $m = 2k$ for some $k \in \mathbb{Z}$. Now $mn = (2k)n = 2(kn)$, and $kn \in \mathbb{Z}$, so mn is even. $\square$

For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.

Contrapositive: if a is even or b is even, then $(ab)^2$ is even. WLOG suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ and $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even. $\square$

For all integers x and y, if $x^2(y^2 - 2y)$ is odd then x and y are odd.

Contrapositive: if x is even or y is even, then $x^2(y^2 - 2y)$ is even. Here the two cases need separate treatment.

Case 1: x even. $x = 2k$ for some $k \in \mathbb{Z}$, so $x^2(y^2 - 2y) = 4k^2(y^2 - 2y) = 2(2k^2(y^2 - 2y))$, and $2k^2(y^2 - 2y) \in \mathbb{Z}$.

Case 2: y even. $y = 2\ell$ for some $\ell \in \mathbb{Z}$, so $x^2(y^2 - 2y) = x^2(4\ell^2 - 4\ell) = 2(x^2(2\ell^2 - 2\ell))$, and $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$.

In both cases $x^2(y^2 - 2y)$ is even. $\square$

For any integer n, n^2 is odd if and only if n is odd. A biconditional needs both directions, and they want different methods:

($\Leftarrow$, direct) Suppose n is odd, so $n = 2k+1$. Then $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ is odd.

($\Rightarrow$, contraposition) The contrapositive is: if n is even then n^2 is even. Suppose $n = 2k$. Then $n^2 = 4k^2 = 2(2k^2)$ is even. $\square$

This lemma — **for all integers n, if n^2 is even then n is even** — is used in the proof that $\sqrt{2}$ is irrational (see rational-and-irrational-numbers[7]).

Common proof errors

The course explicitly tests spotting these:

- **Arguing from examples** — a single example never establishes a universal statement. ("$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy = 1$. Proof: if $x = 10$ take $y = \frac{1}{10}$." Not a proof — and the statement is false, since $x = 0$ has no such y.)
- **Using the same variable to mean two different things** — "let $m = 2k + 1$ and $n = 2k$" only proves the case $m = n + 1$. Use a fresh variable for each quantity.

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

- **Assuming what is to be proved** — starting from "$4a + 2b = 2\ell$" and manipulating both sides assumes the conclusion. Derive the conclusion; don't begin with it.
- **Jumping to the conclusion** — writing down the definition you need to satisfy and then asserting it holds, without exhibiting the witnesses.
- **Forgetting to state assumptions**, or forgetting to say where a variable lives ("for some $r, s \in \mathbb{Z}$").
- **Confusion between what is known and what is to be shown.**
- **Use of the word *any* instead of *some***, and **misuse of the word *if***.

See also

- quantified-statements[8] — the negations these proofs are built on
- conditional-statements[9] · logical-equivalence-laws[10]
- rational-and-irrational-numbers[11] · divisibility-and-factorisation[12]
- practice-problems[13] — §9 Direct Proofs and Counterexamples, with full worked solutions
- practice-problems[14] — §10 Proof by Contradiction, with full worked solutions
- practice-problems[15] — §11 Proof by Contraposition, with full worked solutions

[8] courses/math1061/quantified-statements.pdf
[9] courses/math1061/conditional-statements.pdf
[10] courses/math1061/logical-equivalence-laws.pdf
[11] courses/math1061/rational-and-irrational-numbers.pdf
[12] courses/math1061/divisibility-and-factorisation.pdf
[13] courses/math1061/practice-problems.pdf
[14] courses/math1061/practice-problems.pdf
[15] courses/math1061/practice-problems.pdf