Lecture 8 — Proof by Contradiction

Table of contents

Learning goals . . . 1
Recall . . . 1
When to use contradiction . . . 2
The three methods so far . . . 3
Worked: how to start a proof by contradiction . . . 4
Worked: what type of proof starts this way? . . . 4
Worked: the same statement, both ways . . . 4
Worked: where contradiction earns its keep . . . 5
Worked: if $3n^3 - 2$ is odd then n is odd . . . 6
Worked: without loss of generality . . . 6
See also . . . 7

Pre-work: Video 010 (Proof by Contradiction). Adds a third method to the direct proof and counterexample of 2026-08-10-direct-proof-and-counterexample[1] — see proof-techniques[2] for all four side by side.

Learning goals

- How to write a proof by contradiction.

Recall

The negations this method depends on (see logical-equivalence-laws[3] and quantified-statements[4]):

[1] courses/math1061/2026-08-10-direct-proof-and-counterexample.pdf
[2] courses/math1061/proof-techniques.pdf
[3] courses/math1061/logical-equivalence-laws.pdf
[4] courses/math1061/quantified-statements.pdf

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$
$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim (p \to q) \equiv p \wedge \sim q$$
$$\sim (\exists x \in D \text{ such that } P(x)) \equiv \forall x \in D, \sim P(x)$$
$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D \text{ such that } \sim P(x)$$

The definitions every proof below unfolds

The definitions are written as **biconditionals**, because a proof uses them in both directions — read left-to-right to unpack a hypothesis, right-to-left to establish a conclusion.

- 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 $\leftrightarrow$ $n = 2k - 1$ 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

Both forms of "odd" are usable: $2k + 1$ and $2k - 1$ describe the same set of integers, and some calculations come out tidier with one than the other. The same definitions are tabulated in proof-techniques[5]; the rational one is unpacked in rational-and-irrational-numbers[6] and the divisibility one in divisibility-and-factorisation[7].

Fact: the sum, difference and product of integers is an integer.

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

When to use contradiction

Three questions share one answer: whether proof by contradiction can be used for every proof, whether it only works for universal statements or just works best for them, and which situations suit it over a direct proof. Proof by contradiction is the **most versatile** method, but it requires more set-up, so sometimes a direct proof is easier.

[5] courses/math1061/proof-techniques.pdf
[6] courses/math1061/rational-and-irrational-numbers.pdf
[7] courses/math1061/divisibility-and-factorisation.pdf

Proof by counterexample and proof by contradiction do opposite jobs. Counterexample is a **disproof**; contradiction is a **proof**.

The three methods so far

There are three proof skeletons so far (Figure 1); the fourth arrives next lecture.

Proofs of the statement $\forall x \in D,\ P(x) \to Q(x)$

Direct proof:
Let $x \in D$ and suppose $P(x)$.
...
Hence $Q(x)$. □

Shows the statement is true.

Disproof by counterexample:
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.

Shows the statement is false.

Proof by contradiction:
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 that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$.
This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. □

(⇒⇐)

Shows the statement is true.

Figure 1: Three proof skeletons for the same statement, each with its verdict in red underneath. Only the contradiction box starts by assuming the statement false; the other two start from the statement's own hypothesis. The orange (⇒⇐) in the margin marks the point where the contradiction lands.

For a proof by contradiction we begin by **assuming that the statement is false** — equivalently, that the negation of the statement is true. The negation of $\forall x \in D, P(x) \to Q(x)$ is

$$\exists x \in D \text{ such that } P(x) \wedge \sim Q(x)$$

and we derive from it something that cannot hold — $P(x)$ false, or $Q(x)$ true, or $1 = 0$.

Note what the two moves in that negation are: the $\forall$ becomes an $\exists$ (so you are handed *one* specific x to work with, not an arbitrary one), and $\sim (P \to Q) \equiv P \wedge \sim Q$ turns the implication into a conjunction (so you get to assume the hypothesis **and** the failure of the conclusion at once). Both extra assumptions are why the method is the most versatile one, and why it costs more set-up.

The contradiction mark. ($\Rightarrow\Leftarrow$) — two arrows meeting head-on — is written inline at the point where the contradiction lands. Every proof by contradiction below uses it. It is a marker, not a substitute for saying in words *what* contradicts *what*.

Worked: how to start a proof by contradiction

Claim: $\forall n \in \mathbb{Z}$, if n is odd then $3n + 2$ is odd. An appropriate way to start a proof by contradiction is:

> *Proof:* Suppose that n is an odd integer and that $3n + 2$ is even.

which means **exactly the same thing** as

> Suppose $\exists n \in \mathbb{Z}$ such that n is odd but $3n + 2$ is even.

The second phrasing is the one the negation rule actually produces, so it is the safer one to write while you are learning; the first is the same sentence with the existential left implicit.

Worked: what type of proof starts this way?

Claim: for all integers m and n, if mn is even, then m is even or n is even. Consider the first sentence of a proof:

> *Proof:* Suppose that m and n are integers, mn is even and both m and n are odd.

This is the start of a **proof by contradiction**, not a direct proof and not a disproof by counterexample. It assumes the hypothesis *and* the negation of the conclusion ("m even or n even" negates to "m odd and n odd" by De Morgan).

Worked: the same statement, both ways

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

It can be proved both ways (Figure 2).

Direct proof

> Let $n \in \mathbb{Z}$ and suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$ (by definition). Now
>
> $$3n + 2 = 3(2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1.$$
>
> Since $k \in \mathbb{Z}$, we know $3k + 2 \in \mathbb{Z}$, and hence $3n + 2$ is odd (by definition). $\square$

Proof by contradiction

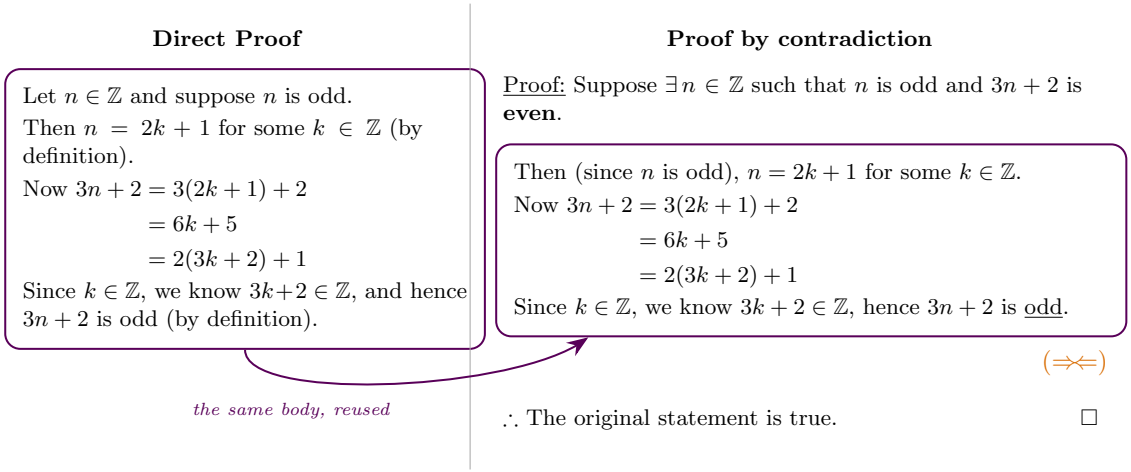

Figure 2: The same statement proved both ways — direct proof left, proof by contradiction right. The purple outline marks the body the two proofs share, and the arrow carries it across: it is character-for-character the same algebra. Contradiction only adds an assumption line on top and the (⇒⇐) plus conclusion at the bottom. That extra wrapper is the 'more set-up' that contradiction costs.

> Suppose $\exists n \in \mathbb{Z}$ such that n is odd and $3n + 2$ is **even**. Then (since n is odd), $n = 2k + 1$ 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 know $3k + 2 \in \mathbb{Z}$, hence $3n + 2$ is **odd** (⇒⇐) — contradicting the assumption that it is even. Therefore the original statement is true. □

The body of the two proofs is identical; contradiction just wraps it in an extra assumption and an extra closing line. That's the "more set-up" cost — and here the direct proof is the better choice.

Worked: where contradiction earns its keep

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

Direct proof — suppose $m, n \in \mathbb{Z}$ and mn is even. We can write $mn = 2k$ for some $k \in \mathbb{Z}$ … and now there's no way forward: knowing $mn = 2k$ tells you nothing about m and n individually.

Proof by contradiction

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 $\ell \in \mathbb{Z}$ — **use a new variable**; m and n need not be equal. Now

$$mn = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1.$$

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 ($\Rightarrow\Leftarrow$). Therefore the original statement is true. $\square$

Reusing k for both m and n is one of the standard proof errors listed in proof-techniques[8]. Note also where the contradiction lands here: not on a stray arithmetic absurdity but on the *hypothesis itself* — the assumed-even mn turns out to be odd. That is one of the three landing points listed above ("$P(x)$ is false").

Worked: if $3n^3 - 2$ is odd then n is odd

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

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

$$3n^3 - 2 = 3(2a)^3 - 2 = 3 \cdot 8a^3 - 2 = 24a^3 - 2 = 2(12a^3 - 1).$$

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

The negation is worth reading slowly: "if $3n^3 - 2$ is odd then n is odd" negates to "$3n^3 - 2$ is odd **and** n is even". The even hypothesis is the one that gives you something to substitute, so that is where the work starts.

Worked: without loss of generality

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

Proof. Suppose the statement is false. Thus $\exists m, n \in \mathbb{Z}$ such that $m + n$ is even but exactly one of m, n is even (and the other is odd).

Without loss of generality (WLOG), assume m is even and n is odd. (The two cases are (1) m even, n odd and (2) m odd, n even; since $m + n = n + m$, the second is the first with the names swapped, so proving one proves both.)

Thus $m = 2a$ for some $a \in \mathbb{Z}$, and $n = 2b + 1$ for some $b \in \mathbb{Z}$. Now

$$m + n = (2a) + (2b + 1) = 2(a + b) + 1.$$

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

We know $a + b \in \mathbb{Z}$ because $a, b \in \mathbb{Z}$, so $m + n$ is odd. This contradicts the assumption that $m + n$ is even ($\Rightarrow\Leftarrow$). Therefore the original statement is true. $\square$

"Without loss of generality" is only legitimate when the omitted case really is the stated one relabelled — say why, as above. The phrase abbreviates to **WLOG**.

See also

- proof-techniques[9] · quantified-statements[10] · logical-equivalence-laws[11]
- 2026-08-13-proof-by-contraposition[12] — Lecture 9
- practice-problems[13] — §10 Proof by Contradiction, with full worked solutions

[9] courses/math1061/proof-techniques.pdf
[10] courses/math1061/quantified-statements.pdf
[11] courses/math1061/logical-equivalence-laws.pdf
[12] courses/math1061/2026-08-13-proof-by-contraposition.pdf
[13] courses/math1061/practice-problems.pdf