Lecture 8 — Proof by Contradiction

Table of contents

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

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

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

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

$$\sim (\exists x \in D \text{ such that } P(x)) \equiv \forall x \in D, \sim P(x)$$

$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D \text{ such that } \sim P(x)$$

Plus the definitions of even, odd, prime, composite, rational and divides, tabulated in proof-techniques[5].

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.

Student questions and comments

Can proof by contradiction be used for every proof? / Does this type of proof only work for universal statements, or does it just work best for them? / What situations are best for proof by contradiction vs the direct proof?

Proof by contradiction is the **most versatile** method, but it requires more set-up, so sometimes a direct proof is easier.

What is the difference between proof by counterexample and proof by contradiction? Counterexample is a **disproof**; contradiction is a **proof**. They do opposite jobs.

The three methods so far

Method	Shape	Shows
Direct proof	Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$.	statement is **true**
Disproof by counterexample	Let $x = \cdots$. Then $x \in D$, $P(x)$ true, $Q(x)$ false.	statement is **false**
Proof by contradiction	Suppose $\exists x \in D$ such that $P(x)$ true, $Q(x)$ false. ... Hence something obviously wrong.	statement is **true**

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

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 $1 = 0$.

Q1 from the pre-class questions

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.

Q2 from the pre-class questions

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 of what type?

(a) A direct proof. (b) A disproof by counterexample. **(c) A proof by contradiction.**

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).

Activity 1 — the same statement, both ways

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

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

> 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. $\square$

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.

Activity 2 — 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 — a contradiction. 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[6].

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

Activity 3

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 — a contradiction. Therefore the original statement is true. □

Activity 4 — completing a started proof

$\forall m, n \in \mathbb{Z}$, 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, 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

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

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. Therefore the original statement is true. □

"Without loss of generality" is only legitimate when the omitted case really is the stated one relabelled — say why, as above.

See also

- proof-techniques[7] · quantified-statements[8] · logical-equivalence-laws[9]
- 2026-08-13-proof-by-contraposition[10] — Lecture 9
- practice-problems[11] — §10 Proof by Contradiction, with full worked solutions

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