Contrapositive and Contradiction

Proving a statement by way of its negation

Last modified: 2026-11-12 01:18:19 (PST)

Source

Adapted from Kameron Decker Harris's Fall 2026 lecture notes "Contrapositive Proof" and "Proof by Contradiction", which are typed transcriptions of Scott Wehrwein's Spring 2025 handwritten lecture notes. These come from those notes:

- the definition of congruence modulo n, and the point that it is not the mod operator;
- the human and mammal illustration of a contrapositive;
- the example of a product not divisible by 5;
- the truth table showing why a proof by contradiction works;
- the outlines of a proof by contrapositive, a proof by contradiction, and a proof of a conditional by contradiction;
- the definition and examples of a prime number, and the fact that every integer above one has a prime divisor;
- the statement that $\sqrt{2}$ is irrational (the proof here is different);
- Euclid's proof that there are infinitely many primes.

The exercises are new.
The definitions of the contrapositive, proof by contrapositive and proof by contradiction, their example of a proof by contradiction, and the theorem that a conditional is equivalent to its contrapositive, are on the proof writing page, and the definitions of rational and irrational numbers, with their examples, are on the number systems page. The other data science notes link to both pages.

Congruence modulo n

Exercise 1 (Differences divisible by five)**.** For each integer a in the list 23, 38, 50, -7, compute $a - 8$, and decide whether $5 \mid (a - 8)$ (Definition: Divides).

Solution

Solution 1.

- $23 - 8 = 15 = 5 \cdot 3$, so $5 \mid (23 - 8)$.
- $38 - 8 = 30 = 5 \cdot 6$, so $5 \mid (38 - 8)$.
- $50 - 8 = 42$. Since $5 \cdot 8 = 40 < 42 < 45 = 5 \cdot 9$, no integer c has $5c = 42$, so $5 \nmid (50 - 8)$.
- $-7 - 8 = -15 = 5 \cdot (-3)$, so $5 \mid (-7 - 8)$.

Definition 1 (Congruence modulo n)**.** Let a and b be integers, and let n be a positive integer. We say that a is **congruent to** b **modulo** n, written $a \equiv b \pmod{n}$, if n divides $a - b$, written $n \mid (a - b)$, (Wikipedia contributors 2026d). When a is not congruent to b modulo n, we write $a \not\equiv b \pmod{n}$.

Example 1 (Congruences)**.**

- By Solution 1, $23 \equiv 8 \pmod{5}$, $38 \equiv 8 \pmod{5}$ and $-7 \equiv 8 \pmod{5}$, but $50 \not\equiv 8 \pmod{5}$.
- A 24-hour clock that reads 19 shows the same hour as a 12-hour clock that reads 7, and $19 \equiv 7 \pmod{12}$, because $19 - 7 = 12 = 12 \cdot 1$.

Remark 1 (Two meanings of $\equiv$, and the mod operator). The symbol $\equiv$ also means logical equivalence. The "$(\mathrm{mod}\, n)$" after it says which meaning is in use: $23 \equiv 8 \pmod{5}$ is a statement about two integers, and $P \equiv Q$ is a statement about two propositions.
Congruence is related to the mod operator of a programming language, but it is not the same thing. In Racket, `(modulo 23 5)` is the number 3, while $23 \equiv 8 \pmod{5}$ is a proposition (Definition: Proposition, statement), which is true or false.

Proof by contrapositive

Exercise 2 (An odd sum)**.** Let x and y be integers. Prove: if $x + y$ is odd, then $x \neq y$. First try a direct proof (Definition: Direct proof), starting from "Suppose $x + y$ is odd." Then try starting from "Suppose $x = y$."

Solution

Solution 2. The direct start gives $x + y = 2k + 1$ for some integer k (Definition: Odd integer), which says little about whether x and y are equal.
The second start goes further. Suppose $x = y$. Then $x + y = x + x = 2x$, and x is an integer, so $x + y$ is even (Definition: Even integer). No integer is both even and odd (Remark: Facts about integers used without proof), so $x + y$ is not odd.
That proves "if $x = y$, then $x + y$ is not odd". Why proving this proposition proves the one we were asked about is the subject of this section.

Definition 2 (Contrapositive)**.** The **contrapositive** (Wikipedia contributors 2026a) of the proposition "if P, then Q" is the proposition "if $\neg Q$, then $\neg P$".

Example 2 (Contrapositives)**.**

- The contrapositive of "if x is a human, then x is a mammal" is "if x is not a mammal, then x is not a human".
- In Exercise 2, P is "$x + y$ is odd" and Q is "$x \neq y$". The negation of Q is "$x = y$" (Definition: Not), so the contrapositive is "if $x = y$, then $x + y$ is not odd", which is what Solution 2 proved.

Theorem 1 (A conditional is equivalent to its contrapositive)**.** *For any propositions P and Q,*

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P).$$

Proof

Proof. By the definition of implies, $P \Rightarrow Q$ is false exactly when P is true and Q is false. By the same definition, $\neg Q \Rightarrow \neg P$ is false exactly when $\neg Q$ is true and $\neg P$ is false, that is, exactly when Q is false and P is true. So the two propositions are false in the same row of a truth table and true in the other three, which is Definition: Logically equivalent. □

Example 3 (A proposition and its contrapositive)**.** Take "if today is Saturday, then today is a weekend day", which is true.
Its contrapositive is "if today is not a weekend day, then today is not Saturday". It is also true, as Theorem 1 says it must be: Monday through Friday are the days that are not weekend days, and none of them is Saturday.

Definition 3 (Proof by contrapositive)**.** A **proof by contrapositive** (Wikipedia contributors 2026a) of a proposition "if P, then Q" is a direct proof of its contrapositive, "if $\neg Q$, then $\neg P$": it assumes that Q is false and reaches the conclusion that P is false. By Theorem 1, proving the contrapositive proves the original proposition.

Example 4 (A product not divisible by 5)**.** Claim: let x and y be integers. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.
A direct proof would start from $5 \nmid xy$, which says only that xy is not 5 times an integer, and gives no equation to work with. By De Morgan's law for a conjunction, the negation of "$5 \nmid x$ and $5 \nmid y$" is "$5 \mid x$ or $5 \mid y$", so the contrapositive (Definition 2) is "if $5 \mid x$ or $5 \mid y$, then $5 \mid xy$". We prove it by cases (Definition: Proof by cases, proof by exhaustion).
Case 1: $5 \mid x$**.** Then $x = 5c$ for some integer c (Definition: Divides), so

$$\begin{aligned} xy &= (5c)y && \text{(substitute } x = 5c\text{)} \\ &= 5(cy), && \text{(regroup the product)} \end{aligned}$$

and cy is an integer (Remark: Facts about integers used without proof), so $5 \mid xy$.
Case 2: $5 \mid y$**.** Then $y = 5d$ for some integer d, so $xy = x(5d) = 5(xd)$, and xd is an integer, so $5 \mid xy$.
In both cases $5 \mid xy$, which proves the contrapositive and so the claim (Theorem 1). For example, $x = 3$ and $y = 7$ give $xy = 21$, which 5 does not divide, and indeed 5 divides neither 3 nor 7.

Remark 2 (The shape of a proof by contrapositive). A proof by contrapositive (Definition 3) of "if P, then Q" has this shape:

> Suppose $\neg Q$.
> ⋮
> Therefore $\neg P$.

Use it when $\neg Q$ gives you more to work with than P does. In Exercise 2, $\neg Q$ was the equation $x = y$, while P said only that $x + y$ is odd.

Exercise 3 (A square not divisible by three)**.** Let n be an integer. Prove: if $3 \nmid n^2$, then $3 \nmid n$.

Solution

Solution 3. We prove the contrapositive (Definition 3): if $3 \mid n$, then $3 \mid n^2$.
Suppose $3 \mid n$. Then $n = 3c$ for some integer c (Definition: Divides), so

$$\begin{aligned} n^2 &= (3c)^2 && \text{(substitute } n = 3c\text{)} \\ &= 9c^2 && \text{(square each factor)} \\ &= 3(3c^2), && \text{(write } 9 = 3 \cdot 3\text{)} \end{aligned}$$

and $3c^2$ is an integer (Remark: Facts about integers used without proof), so $3 \mid n^2$. By Theorem 1, this proves the original proposition.

Proof by contradiction

Exercise 4 (No solution in integers)**.** Show that there are no integers m and n with $6m + 9n = 1$.
Hint: suppose there were. What would $6m + 9n = 1$ say about 3 and 1?

Solution

Solution 4. Suppose there are integers m and n with $6m + 9n = 1$. Then

$$\begin{aligned} 1 &= 6m + 9n && \text{(the assumption, read from right to left)} \\ &= 3(2m + 3n), && \text{(distributive law, read from right to left)} \end{aligned}$$

and $2m + 3n$ is an integer (Remark: Facts about integers used without proof), so $3 \mid 1$ (Definition: Divides).
But $3 \nmid 1$: since $3 \cdot 0 = 0 < 1 < 3 = 3 \cdot 1$, no integer c has $3c = 1$. So $3 \mid 1$ and $3 \nmid 1$, which is impossible. The assumption must be false, so there are no integers m and n with $6m + 9n = 1$.

Definition 4 (Proof by contradiction)**.** A **proof by contradiction** (Wikipedia contributors 2026f) of a proposition P assumes that P is false, and derives from that assumption a proposition that is known to be false.

Example 5 (No integer is both even and odd)**.** Suppose, for contradiction, that some integer n is both even and odd (definition). Then $n = 2j$ and $n = 2k+1$ for some integers j and k, and

$$\begin{aligned} 2j &= 2k + 1 && \text{(both equal } n\text{)} \\ 2j - 2k &= 1 && \text{(subtract } 2k \text{ from both sides)} \\ 2(j - k) &= 1 && \text{(distributive law)} \\ j - k &= \tfrac{1}{2} && \text{(divide both sides by 2)} \end{aligned}$$

The third line uses the distributive law. But $j - k$ is an integer, and $\frac{1}{2}$ is not, so the last line is false. So no integer is both even and odd. For example, $6 = 2 \cdot 3$ is even, and $6 = 2k + 1$ would need $k = 2.5$, which is not an integer.

Theorem 2 (Why a proof by contradiction works)**.** *For propositions P and C,*

$$P \equiv (\neg P \Rightarrow (C \wedge \neg C)).$$

Proof

Proof. By the definitions of and and not, $C \wedge \neg C$ is false in every row, so it is a contradiction. So, by the definition of implies, $\neg P \Rightarrow (C \wedge \neg C)$ is true exactly in the rows where $\neg P$ is false, which are the rows where P is true:

P	C	$\neg P$	$C \wedge \neg C$	$\neg P \Rightarrow (C \wedge \neg C)$
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

The first and last columns match in every row, so the two are logically equivalent. □

Example 6 (The six and nine proof, read through the theorem)**.** In Solution 4, P is "there are no integers m and n with $6m+9n = 1$", and C is "$3 \mid 1$". The solution assumed $\neg P$, that such integers exist, and derived both C and $\neg C$. That proves $\neg P \Rightarrow (C \wedge \neg C)$, so, by Theorem 2, it proves P.

Remark 3 (The shape of a proof by contradiction). A proof by contradiction (Definition 4) of a proposition P has this shape:

> Suppose $\neg P$.
> ⋮
> Therefore C and $\neg C$.

Two things differ from a proof by contrapositive (Remark 2). P need not be a conditional. And the proof does not know C in advance: any proposition C for which the argument derives both C and $\neg C$ will do.

Remark 4 (Proving a conditional by contradiction). To prove "if P, then Q" by contradiction, suppose its negation, which is "P and $\neg Q$" (Theorem: Negating a conditional):

> Suppose P and $\neg Q$.
> $\vdots$
> Therefore C and $\neg C$.

A proof by contrapositive (Remark 2) assumes only $\neg Q$, and has the fixed goal $\neg P$. A proof by contradiction assumes both P and $\neg Q$, and any contradiction will do.

Example 7 (A number plus its reciprocal)**.** Claim: let x be a real number. If $x > 0$, then $x + \frac{1}{x} \geq 2$.
Suppose, for contradiction, that $x > 0$ and $x + \frac{1}{x} < 2$. Since $x > 0$, multiplying both sides by x keeps the inequality, so

$$\begin{aligned} x^2 + 1 &< 2x && \text{(multiply both sides by } x > 0\text{)} \\ x^2 - 2x + 1 &< 0 && \text{(subtract } 2x \text{ from both sides)} \\ (x-1)^2 &< 0. && \text{(square of a difference)} \end{aligned}$$

Let C be "$(x-1)^2 \geq 0$". C is true, because a square of a real number is never negative, and the last line says $\neg C$. That is a contradiction, so the claim holds. The proof used $x > 0$ in the first step, and the contradiction it reached is not $x \leq 0$. For example, $x = 4$ gives $4 + \frac{1}{4} = 4.25 \geq 2$.

Exercise 5 (Squares one apart)**.** Prove that there are no positive integers x and y with $x^2 - y^2 = 1$.

Solution

Solution 5. Suppose, for contradiction, that x and y are positive integers with $x^2 - y^2 = 1$. Then

$$\begin{aligned} 1 &= x^2 - y^2 && \text{(the assumption, read from right to left)} \\ &= (x-y)(x+y). && \text{(difference of squares)} \end{aligned}$$

Since $x \geq 1$ and $y \geq 1$, $x + y \geq 2$. Dividing both sides by $x + y$ gives $x - y = \frac{1}{x+y}$, and $0 < \frac{1}{x+y} \leq \frac{1}{2}$, so $x - y$ is strictly between 0 and 1 and is not an integer. But $x - y$ is an integer (Remark: Facts about integers used without proof). That is a contradiction, so there are no such x and y.

Irrational numbers

Exercise 6 (Bounds on a fraction for $\sqrt{2}$)**.** Suppose a and b are positive integers with $\frac{a}{b} = \sqrt{2}$. Use $1 < 2 < 4$ to show that $b < a < 2b$.

Solution

Solution 6. Square roots keep the order of positive numbers, so $1 < 2 < 4$ gives $1 < \sqrt{2} < 2$, that is, $1 < \frac{a}{b} < 2$. Multiplying each part by b, which is positive, keeps the order, and gives $b < a < 2b$.

Definition 5 (Rational numbers)**.** A **rational number** (Wikipedia contributors 2026h) is a number that can be written as a fraction $\frac{a}{b}$, where a and b are integers (Definition: Integers) and $b \neq 0$. The set of rational numbers is written $\mathbb{Q}$:

$$\mathbb{Q} \stackrel{\text{def}}{=} \left\{ \frac{a}{b} : a \in \mathbb{Z},\ b \in \mathbb{Z},\ b \neq 0 \right\}$$

Example 8 (Rational numbers)**.**

- $\frac{3}{4}$ is rational, with $a = 3$ and $b = 4$.
- 0.75 is rational, because $0.75 = \frac{3}{4}$.
- Every integer is rational: for example, $-5 = \frac{-5}{1}$.
- $0.333\ldots$, with the 3s repeating forever, is rational, because $0.333\ldots = \frac{1}{3}$.

Definition 6 (Irrational numbers)**.** An **irrational number** (Wikipedia contributors 2026c) is a real number (Definition: Real numbers) that is not rational (Definition 5).

Example 9 (Irrational numbers)**.**

- $\sqrt{2} = 1.41421\ldots$, the square root of 2, is irrational: no fraction of integers $\frac{a}{b}$ squares to 2 (Wikipedia contributors 2026i).
- $\pi = 3.14159\ldots$ is irrational (Wikipedia contributors 2026g).
- 1.5 is not irrational, because $1.5 = \frac{3}{2}$ is rational.

Remark 5 (Smallest elements). These notes use one more fact about the integers without proving it (Wikipedia contributors 2026j):

- every set of positive integers that has at least one element has a smallest element.

For example, the set of positive integers b for which $\frac{3}{4}b$ is an integer has the elements 4, 8, 12 and so on, and its smallest element is 4.

Theorem 3 ($\sqrt{2}$ is irrational)**.** *The square root of* 2 *is irrational (Definition 6) (Wikipedia contributors 2026i).*

Proof

Proof. Suppose, for contradiction, that $\sqrt{2}$ is rational (Definition 5). Then $\sqrt{2} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Since $\sqrt{2} > 0$, we can take a and b positive (if $b < 0$, replace a and b with $-a$ and $-b$). So the set of positive integers b for which $\sqrt{2}\,b$ is an integer has an element, and by Remark 5 it has a smallest element. Let b be that smallest element, and let $a = \sqrt{2}\,b$, a positive integer.
By Solution 6, $b < a < 2b$, so $b' = a - b$ is an integer with $0 < b' < b$. Let $a' = 2b - a$, also an integer. Then

$$\begin{aligned}
\sqrt{2}\,b' &= \sqrt{2}\,(a-b) && \text{(definition of } b'\text{)} \\
&= \sqrt{2}\,a - \sqrt{2}\,b && \text{(distributive law)} \\
&= \sqrt{2}\,\sqrt{2}\,b - a && \text{(substitute } a = \sqrt{2}\,b \text{ in the first term, and } \sqrt{2}\,b = a \text{ in the second)} \\
&= 2b - a && (\sqrt{2}\,\sqrt{2} = 2) \\
&= a'. && \text{(definition of } a'\text{)}
\end{aligned}$$

So b' is a positive integer for which $\sqrt{2}\,b'$ is an integer, and $b' < b$. That contradicts the choice of b as the smallest such integer. So $\sqrt{2}$ is not rational. □

Example 10 (The step in the proof, on a fraction near $\sqrt{2}$)**.** The proof of Theorem 3 turns a fraction $\frac{a}{b}$ into $\frac{2b-a}{a-b}$. Applied to $\frac{7}{5} = 1.4$, whose square is $\frac{49}{25} = 1.96$, it gives $\frac{10-7}{7-5} = \frac{3}{2} = 1.5$, whose square is $\frac{9}{4} = 2.25$. Neither fraction is exactly $\sqrt{2}$, and the step moved from denominator 5 to the smaller denominator 2. If some fraction were exactly $\sqrt{2}$, the step would give another fraction exactly equal to $\sqrt{2}$, with a smaller positive denominator, and a smallest positive denominator could not exist.

Infinitely many primes

Exercise 7 (Which are prime?)**.** Which of 51, 53 and 57 have no positive divisors other than 1 and themselves? Hint: try dividing by 2, 3, 5 and 7.

Solution

Solution 7.

- $51 = 3 \cdot 17$, so 3 divides 51 (Definition: Divides).
- $57 = 3 \cdot 19$, so 3 divides 57.
- 53 is not divisible by 2, 3, 5 or 7, because it lies strictly between two multiples of each: $2 \cdot 26 = 52 < 53 < 54 = 2 \cdot 27$, $3 \cdot 17 = 51 < 53 < 54 = 3 \cdot 18$, $5 \cdot 10 = 50 < 53 < 55 = 5 \cdot 11$, and $7 \cdot 7 = 49 < 53 < 56 = 7 \cdot 8$. A divisor d of 53 with $1 < d < 53$ would pair with $\frac{53}{d}$, and one of the two would be at most 7, because $8 \cdot 8 = 64 > 53$. It would be one of $2, \ldots, 7$, and 4 or 6 would make 2 a divisor too, since 2 divides both (Exercise: Divisors of divisors). So 53 has no positive divisors other than 1 and 53.

Definition 7 (Prime number)**.** An integer $n \geq 2$ is **prime** if no positive integer other than 1 and n divides it (Wikipedia contributors 2026e).

Example 11 (Prime and not prime)**.**

- 2, 3, 5, 7, 11 and 13 are prime.
- 9 is not prime, because $3 \mid 9$, and 3 is neither 1 nor 9.
- 1 is not prime, because Definition 7 applies only to integers $n \geq 2$.

Remark 6 (Every integer above one has a prime divisor). These notes use one more fact without proving it:

- every integer $n \geq 2$ is divisible by at least one prime (Definition 7).

For example, 91 is divisible by the primes 7 and 13, since $91 = 7 \cdot 13$.

Theorem 4 (There are infinitely many primes)**.** *There are infinitely many prime numbers (Definition 7) (Wikipedia contributors 2026b).*

Proof

Proof. Suppose, for contradiction, that there are only finitely many primes, and list them all as $p_1, p_2, \ldots, p_k$. The list is not empty, because 2 is prime. Let

$$N = p_1 p_2 \cdots p_k + 1.$$

Each $p_i \geq 2$, so $N \geq 3$, and by Remark 6 some prime p divides N: $N = ps$ for some integer s. The list holds every prime, so p is one of $p_1, \ldots, p_k$, and so p also divides their product: $p_1 p_2 \cdots p_k = pt$ for some integer t. Then

$$\begin{aligned} 1 &= N - p_1 p_2 \cdots p_k && \text{(definition of } N\text{)} \\ &= ps - pt && \text{(substitute both products)} \\ &= p(s - t). && \text{(distributive law, read from right to left)} \end{aligned}$$

Since $s - t$ is an integer (Remark: Facts about integers used without proof), $p \mid 1$. But $p \geq 2$, and $p \cdot 0 = 0 < 1 < p = p \cdot 1$, so no integer c has $pc = 1$, and $p \nmid 1$. That is a contradiction, so there are infinitely many primes. □

Example 12 (The number N in the proof)**.** The proof of Theorem 4 does not claim that N is prime.

- From the list $2, 3, 5$, $N = 2 \cdot 3 \cdot 5 + 1 = 31$, which is prime.
- From the list $2, 3, 5, 7, 11, 13$, $N = 30030 + 1 = 30031 = 59 \cdot 509$, which is not prime. Its prime divisors 59 and 509 are not in the list, which is what the proof needs: every list of primes misses some prime.

Choosing a method

Remark 7 (Which method to try).

- Try a direct proof (Definition: Direct proof) first.
- Try the contrapositive (Definition 3) when $\neg Q$ is the easier assumption (Remark 2).
- Try contradiction (Definition 4) when the proposition says that something does not exist or is not true, as in "no integers satisfy", "is irrational" or "infinitely many": its negation hands you an object to work with.

References

Wikipedia contributors. 2026a. *Contraposition — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Contraposition.

Wikipedia contributors. 2026b. *Euclid's Theorem — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Euclid%27s_theorem.

Wikipedia contributors. 2026c. *Irrational Number — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Irrational_number.

Wikipedia contributors. 2026d. *Modular Arithmetic — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Modular_arithmetic.

Wikipedia contributors. 2026e. *Prime Number — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Prime_number.

Wikipedia contributors. 2026f. *Proof by Contradiction — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Proof_by_contradiction.

Wikipedia contributors. 2026g. *Proof That Pi Is Irrational — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Proof_that_%CF%80_is_irrational.

Wikipedia contributors. 2026h. *Rational Number — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Rational_number.

Wikipedia contributors. 2026i. *Square Root of 2 — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Square_root_of_2.

Wikipedia contributors. 2026j. *Well-Ordering Principle — Wikipedia, the Free Encyclopedia*. https://en.wikipedia.org/wiki/Well-ordering_principle.