

1. Direct proof.

The implication $p \rightarrow q$ can be proved by showing that if p is true then q must also be true. A proof of this kind is called a *direct proof*.

2. Indirect Proof.

Proof by contraposition: Since the implication $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$, the implication $p \rightarrow q$ can be proved by showing that $\neg q \rightarrow \neg p$ is true. This related implication is usually proved directly. An argument of this type is called an *indirect proof*.

Example: Prove “If $3n + 2$ is odd, then n is odd”.

A **vacuous proof** is established by showing $\neg p$.

A **trivial proof** is established by showing q is true.

3. Proof by contradiction.

(a) *For proposition p :* Assume $\neg p$ is true and show this leads to both r and $\neg r$ for some independent proposition r ; in other words $\neg p \rightarrow (r \wedge \neg r)$.

(b) *For implication $p \rightarrow q$:* By assuming that the hypothesis p is true and that the conclusion q is false, then using p and $\neg q$ as well as other axioms, definitions, and previously derived theorems, derives a contradiction. Proofs are based on noting that

$$((p \rightarrow q) \wedge p) \wedge \neg q \equiv (q \wedge \neg q) \quad \text{likewise} \quad (p \wedge (\neg q \rightarrow \neg p)) \equiv (p \wedge \neg p).$$

Exmpl (a): Prove that $\sqrt{2}$ is irrational.

Exmpl (b): Prove that for all real numbers x and y , if $x + y \geq 2$, then either $x \geq 1$ or $y \geq 1$.

4. Equivalence proof (or “if-and-only-if proof”, “necessary-and-sufficient proof”).

To prove a theorem that is an equivalence, i.e., $p \leftrightarrow q$, the tautology

$$(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$$

can be used. That is, the proposition “ p if and only if q ” can be proved if both the implication “if p then q ” and “if q then p ” are proved.

Example: Prove the theorem: The integer n is odd if and only if n^2 is odd”.

5. Exhaustive proof / proof by cases

Exhaustive proof: Proof by showing it holds for all possible x in U (e.g. a truth table).

Proof by cases: Proof by showing it holds for all possible cases. (Useful when direct proof not simple but the extra information in the cases let's you move forward.)

Example: Prove that if n is an integer, then $n^2 \geq n$. (Three cases, $n < 0$, $n = 0$, $n > 0$.)

Without loss of generality (WLOG): Same proof holds for all cases. Quite useful but gets one into trouble (a common mistake in a proof).

6. Constructive existence proof: of statement of the form $\exists x P(x)$. Just find one value of x in U for which $P(x)$ is true. (Hence “constructive”)

Example: Prove there exists a positive integer n that is the sum of cubes of positive integers in two ways: $\exists n : n = i^3 + j^3 = k^3 + l^3$.

7. Nonconstructive existence proof. Don't pinpoint the exact values that satisfy, just show they must exist.

Example: Show there exist irrational numbers x and y such that x^y is rational. In propositional language $\exists x, y ((\text{Irrational}(x) \wedge \text{Irrational}(y)) \rightarrow \text{Rational}(x^y))$.

Example: Prove there are infinitely many primes; $\forall n \exists p > n$ where p is prime.

8. Proof by counterexample.

The goal of such a proof is to show $\forall x P(x)$ is false.

(Note: Showing $\exists x P(x)$ is false is counterexample for $\forall x P(x)$, but this is not a counterexample for the conjecture $\exists x P(x)$.)

Example: Show that the assertion “All primes are odd” is false.

9. Mistakes in proofs.

False premises

Circular reasoning

Not considering all cases (e.g. missing $x = 0$ case).

Showing \exists a satisfying value to prove \forall statements.

Assuming \exists means that all instances satisfy.

Example: What is wrong with the famous supposed “proof” that $1 = 2$?