Proofs.

Proofs in mathematics

In mathematics, a *proof* is a verification of a proposition by a chain of logical deductions from a base set of axioms.

Axioms

An *axiom* is a proposition that is assumed to be true, because you believe it is somehow reasonable.

Examples.

Axiom 1. If $a = b$ and $b = c$, then $a = c$.

Axiom 2. Given a line l and a point p not on l, there is exactly one line through p parallel to l.

Axiom 3. Given a line l and a point p not on l, there are infinitely many lines through p parallel to l.

Axioms

A set of axioms is *consistent* if no proposition can be proved both true and false. This is an absolute must. One would not want to spend years proving a proposition true only to have it proved false the next day! Proofs would become meaningless if axioms were inconsistent.

A set of axioms is *complete* if every proposition can be proved or disproved. Completeness is very desirable; we would like to believe that any proposition could be proved or disproved with sufficient work and insight.

Generally, we'll regard familiar facts from high school as axioms.

Theorems

Important propositions are called *theorems*.

A *lemma* is a preliminary proposition useful for proving later propositions.

A *corollary* is an afterthought, a proposition that follows in just a few logical steps from a theorem.

Conjectures

A *conjecture* is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

Implicit $\forall$

Many theorems assert that a property holds for all elements in the domain of discourse.

If a theorem is stated as follows:

Theorem. $(a+b)^2 = a^2 + 2ab + b^2$.

For all *free* variables, we assume universal quantification:

$$\forall a\ \forall b\ \left((a+b)^2 = a^2 + 2ab + b^2\right)$$

Direct Proof

Consider an example.

Theorem. If n is an odd integer, then n^2 is odd.

Note: Integer n is odd, if there exists another integer k such that $n = 2k + 1$.

Direct Proof

Theorem. If n is an odd integer, then n^2 is odd.

Note: Integer n is odd, if there exists another integer k such that $n = 2k + 1$.

Proof. Let c be an integer. Assume that c is odd. Then, by definition, there exist another an integer d such that $c = 2d + 1$.

$$c^2 = (2d + 1)^2 = 4d^2 + 4d + 1 = 2(2d^2 + 2d) + 1.$$

$2d^2 + 2d$ is an integer, so by definition, $2(2d^2 + 2d) + 1$ is odd. And since it is equal to c^2, c^2 is odd.

Because c was an arbitrary integer, the theorem is true for all integers. $\square$

Direct Proof

To prove a theorem of the form $\forall x\,(P(x) \rightarrow Q(x))$, our goal is to show that $P(c) \rightarrow Q(c)$ is true, where c is an arbitrary element of the domain of discourse.

1. Let varaible c denote an *arbitrary* element from the domain of discourse.
2. Assume that $P(c)$ is true.
3. Prove that $Q(c)$ is true.
4. By the deduction theorem, $P(c) \rightarrow Q(c)$.
5. Because the element c was arbitrary, $\forall x\,(P(x) \rightarrow Q(x))$.

Proof by Contraposition

Consider an example.

Theorem. If n is an integer and $3n+2$ is odd, then n is odd.

Proof by Contraposition

Consider an example.

Theorem. If n is an integer and $3n+2$ is odd, then n is odd.

The theorem states that for every integer n:

$$(3n+2 \text{ is odd}) \rightarrow (n \text{ is odd}).$$

Equivalently, for every integer n:

$$\neg(n \text{ is odd}) \rightarrow \neg(3n+2 \text{ is odd}).$$

Proof by Contraposition

Consider an example.

Theorem. If n is an integer and $3n+2$ is odd, then n is odd.

We have to prove that for every integer n:

$$\neg(n \text{ is odd}) \rightarrow \neg(3n+2 \text{ is odd}),$$

Proof. Assume n is even. Then exists an integer k such that $n = 2k$.

$$3n+2 = 3 \cdot 2k + 2 = 2(3k+1) \text{ is even.}$$

Thus, if n is even, then $3n+2$ is even too.

Therefore, the original statement is also true: If $3n+2$ is odd, then n is odd. $\square$

Proof by Contraposition

To prove a theorem of the form $\forall x\ (P(x) \rightarrow Q(x))$, we can show that $\neg Q(c) \rightarrow \neg P(c)$ for an arbitrary element c.

1. Let varaible c denote an *arbitrary* element from the domain of discourse.
2. Assume that $\neg Q(c)$ is true.
3. Prove that $\neg P(c)$ is true.
4. By the deduction theorem, $\neg Q(c) \rightarrow \neg P(c)$.
5. By equivalence, $P(c) \rightarrow Q(c)$.
6. Because the element c was arbitrary, $\forall x\ (P(x) \rightarrow Q(x))$.

How to prove "if and only if"?

$$p \longleftrightarrow q?$$

How to prove “if and only if”?

$$p \longleftrightarrow q$$
$$\equiv (p \longrightarrow q) \wedge (q \longrightarrow p)$$

You have to prove that p implies q, and q implies p.

Proof by Contradiction

Theorem. There are infinitely many prime numbers.

Proof by Contradiction

Theorem. There are infinitely many prime numbers.

Assume to the contrary that there are only finitely many prime numbers: p_1, p_2, p_3, $\ldots p_n$. Consider a number

$$q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1.$$

Clearly, $q \neq p_i$ for all p_i. The number q is either prime or composite. If a number is composite, it is a product of at least two prime numbers (so it must have at least two divisors among primes).

For all p_i, q cannot be divided evenly by p_i, there is always a remainder of 1. Thus q cannot be composite, so it must be a prime number, not among the primes listed above. We find that q is a new prime, contradicting to the assumption that all of them were listed already. Thus the assumption was wrong: There is infinitely many primes.

Proof by Contradiction

To prove a proposition p by contradiction:

1. Assume that $\neg p$ is true.
2. Derive a contradiction.
3. Therefore, the assumption was incorrect, and p must be true instead!

Proving backwards does not work

Erroneous technique: You start with what we want to prove and then reason until you reach a statement that is surely true.

Theorem (Arithmetic Geometric Mean Inequality). For all non-negative real numbers a and b,

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Wrong proof:

$$\frac{a+b}{2} \stackrel{?}{\geq} \sqrt{ab}$$

$$a+b \stackrel{?}{\geq} 2\sqrt{ab}$$

$$a^2+2ab+b^2 \stackrel{?}{\geq} 4ab$$

$$a^2-2ab+b^2 \stackrel{?}{\geq} 0$$

$$(a-b)^2 \geq 0.$$

Proving backwards does not work

What are we doing wrong?

We have to prove p.

But in fact we assume p, and derive a tautology, so we prove that

$$p \rightarrow T$$

But this statement is always true: either p is false, or T is true.

Proving backwards does not work

What are we doing wrong?

$p \to T$ is always true: either p is false, or T is true.

Example. Prove that $1 = 0$.

Assume

$$1 = 0.$$

Then,

$$0 \cdot 1 = 0 \cdot 0$$

$$0 = 0.$$

The last statement is true. But, obviously, $1 \neq 0$.

So, assuming p and deducing a true statement is not a sufficient argument for proving p.

Proof by cases

Theorem. if n is an integer, then $n^2 \geq n$.

Proof by cases

Theorem. if n is an integer, then $n^2 \geq n$.

- when $n = 0$, there only one value to check: $0^2 = 0$ is true.
- when $n < 0$, then $n^2 \geq 0 > n$, so $n^2 \geq n$.
- when $n > 0$, that is, if it is equal to 1, 2, 3, etc.:

$$n \geq 1$$

$$n \cdot n \geq 1 \cdot n$$
$$n^2 \geq n$$

Proof by cases

We want to prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

We have to go through all the cases $p_1, \ldots p_n$ and prove that each of them implies q.

Generally, look for a proof by cases when there is no obvious way to begin a proof, but when extra information in each case helps move the proof forward.

Remember: The cases must be exhaustive!

Existence Proofs

To prove $\exists x\ P(x)$, we usually make a *constructive* proof, providing an example (witness) x such that $P(x)$ is true.

However, sometimes it's possible to make a *non-constructive* proof, when you show that it's impossible that an example does not exist.

Theorem. There exist irrational numbers x and y such that x^y is rational.

Existence Proofs

Theorem. There exist irrational numbers x and y such that x^y is rational.

Number $\sqrt{2}$ is irrational (it cannot be expressed as the ratio of two integers).

If $\sqrt{2}^{\sqrt{2}}$ is rational, then the theorem is true ($x = \sqrt{2}$, $y = \sqrt{2}$).

Alternatively, if $\sqrt{2}^{\sqrt{2}}$ is irrational, then: $x = \sqrt{2}^{\sqrt{2}}$, and $y = \sqrt{2}$.

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2.$$

In either case, there exists a pair of irrational numbers with the desired property, but we do not know which of these two pairs works.

Uniqueness Proofs

To prove that there *exists one and only one* x such that $P(x)$.

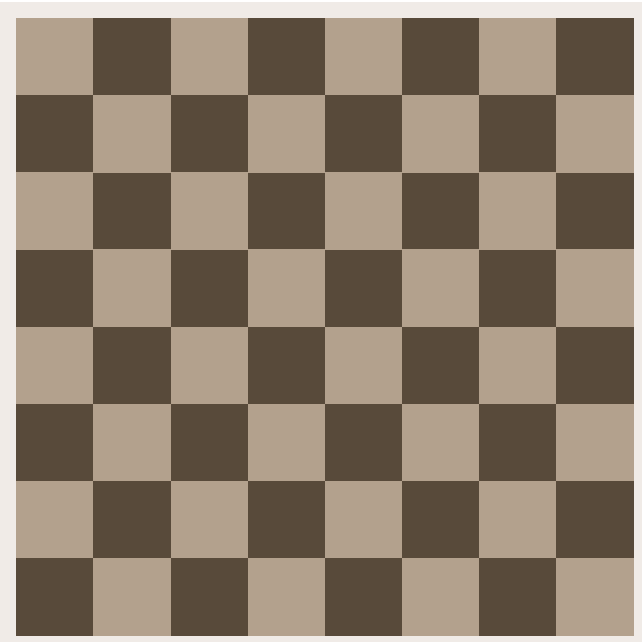
Proof in two stages:

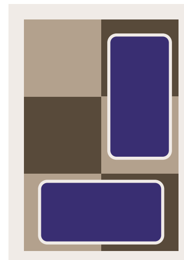
1. *Existence:* Show that an element x with the desired property exists.
2. *Uniqueness:* Show that if $y \neq x$, then y does not have the desired property.

Equivalently:

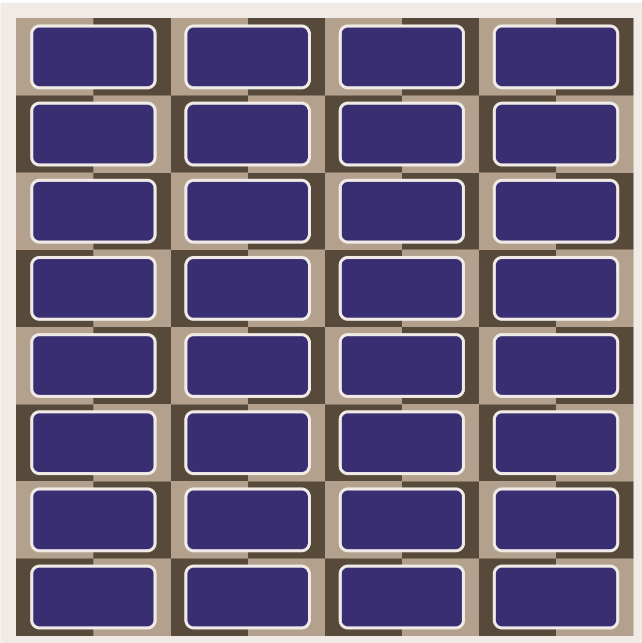
$$\exists x \, \big(P(x) \wedge \forall y \, (y \neq x \rightarrow \neg P(y))\big)$$

Tiling a chessboard with dominos

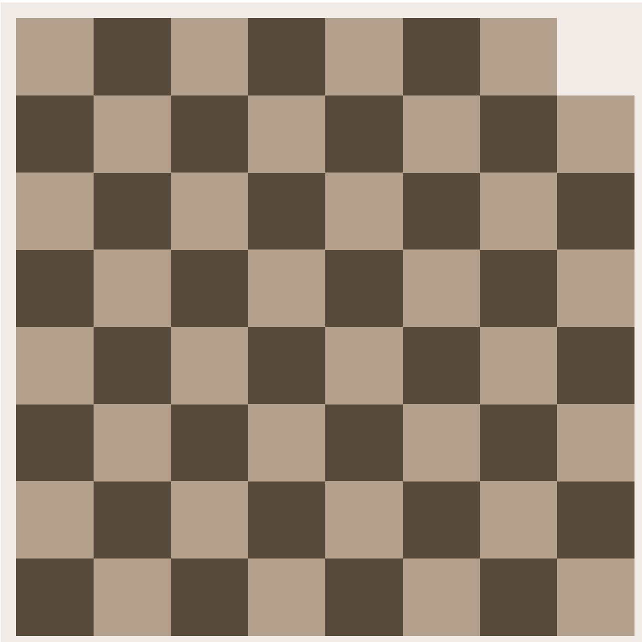




Tiling a chessboard with dominos



Tiling a chessboard with dominos



Tiling a chessboard with dominos