Proofs

- Proofs: Terminology and Rules of Inference
- Direct Proof
- Proof by Contrapositive
- Proof by Contradiction
- Proofs using Case Analysis

Imdad ullah Khan

Proof

An argument that convincingly demonstrates the truth of a statement

In mathematics,

A proof is a chain of logical deductions that demonstrates the truth of a proposition assuming the truth of some known axioms

- Direct proof to prove $P \to Q$
  - Assume P is true, with a chain of logical deductions conclude that Q is true
- Proof by contrapositive to prove $P \to Q$
  - Give a direct proof of $\neg Q \to \neg P$

Proof by Contradiction

Suppose we want to prove some statement P to be true

In proof by contradiction we argue that

if P is not true, then some contradiction must occur

1. Assume that P is false
2. Show that from this ($\neg P$) we can logically deduce some contradiction

The contradiction can be to

- the assumption $\neg P$
  - implying both P and $\neg P$ are simultaneously true, a contradiction
- or to some known true statement S
  - implying S is false, meaning both S and $\neg S$ are simultaneously true

Proof by Contradiction

Prove that Square of an even integer is even

Implication Form

Prove that If x is an even integer, then x^2 is even

Proof:

Assume that for an even x, x^2 is odd ▷ negation of given implication

Let $x^2 = 2k + 1 \implies x^2 - 1 = 2k$ ▷ definition of odd integers

$\implies (x+1)(x-1) = 2k$

$(x-1)$ and $(x+1)$ are either both odd or both even

They have to be even for their product to be even

so x must be odd, a contradiction to our assumption, that x is even □

Proof by Contradiction

Prove that If $a + b > 7$, then $a > 3$ or $b > 4$

Proof:

Let $a + b > 7$

We want to show that either $a > 3$ or $b > 4$

Assume the contrary, $a \leq 3 \wedge b \leq 4$ ▷ negation of the implication

Add these two inequalities we get

$a + b \leq 3 + 4 = 7$

This contradicts our assumption that $a + b > 7$ $\square$

Proofs by Contradiction

$\boxed{\textbf{ICP 8-8}}$ Prove that there exist no integers a and b for which $21a + 30b = 1$ pause

Proof:

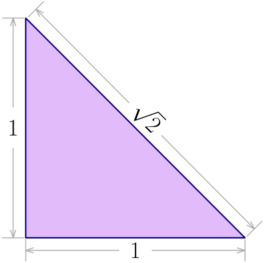
Suppose there exists $a, b \in \mathbb{Z}$ such that

$$21a + 30b = 1 \implies 3(7a + 10b) = 1$$

$$7a + 10b \in \mathbb{Z} \qquad \implies 3|1$$

Proof by Contradiction

Prove that $\sqrt{2}$ is irrational



We will need one of the following two results

Lemma 1

If n is even, then n^2 is also even

Lemma 2

If n is odd, then n^2 is also odd

Proof by Contradiction

Prove that $\sqrt{2}$ is irrational

Proof: Assume that $\sqrt{2}$ is rational ▷ for the sake of contradiction

$$\text{i.e.} \quad \sqrt{2} = {}^{p}\!/_{q} \quad p, q \in \mathbb{Z}, \quad q \neq 0$$

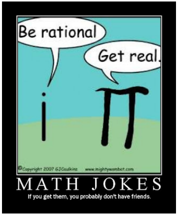
Suppose p and q have no common factors ▷ e.g. cancel any common factors

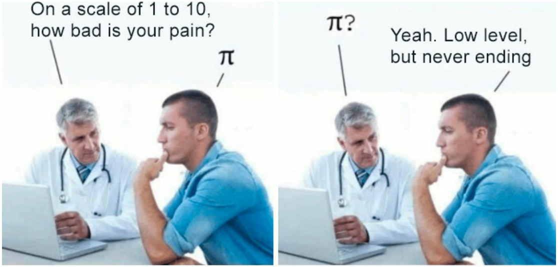
$$2 = {}^{p^2}\!/_{q^2} \implies p^2 = 2q^2$$ ▷ square both sides

- So p^2 is even and p is even ▷ **ICP 8-6** By Lemma ?
- Let $p = 2k$, then $p^2 = 4k^2 = 2q^2 \implies 2k^2 = q^2$
- Hence q^2 is even, so q is even

p and q have 2 as a common factor ▷ A contradiction! □

Irrational Numbers





credit: https://www.boredpanda.com/

Proofs by Contradiction

ICP 8-7 Prove that the sum of any rational number and any irrational number is an irrational number

Proof:

Assume not

Suppose some rational number p/q and an irrational number r adds up to a rational number a/b

$$r + \frac{p}{q} = \frac{a}{b}$$

What can we say about r?

$\triangleright$ Recall the theorem on sum of two rational numbers.

Proof by Contradiction

Prove that There are infinitely many prime numbers

Give a try to proving it using Direct Proof! or a Proof by Contrapositive!

We use the following two lemmas for proving this theorem

Lemma 1

If $x \geq 2$ and x divides y, then x does not divide $y + 1$

Proof by contradiction; it implies that x divides 1

Lemma 2

Every number x has a prime divisor

Proof by Induction next week

Proof by Contradiction

Prove that There are infinitely many prime numbers

Proof: Assume (the contrary) that there are finitely many primes, say

$$p_1, p_2, \ldots, p_n$$

- Let $S = (p_1 p_2 \ldots p_n) + 1$ ▷ product of 'ALL' primes plus 1
- S is larger than all primes, hence can't be prime
- By Lemma 2, S has a prime divisor p
- This p must be (in the list)
- By construction, p divides $S - 1$

Thus, p divides both S and $S - 1$, a contradiction to Lemma 1!

Proof by Contradiction

> Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game
>
> G.H. Hardy, A Mathematician's Apology