Proofs

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

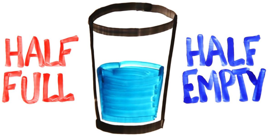
Imdad ullah Khan

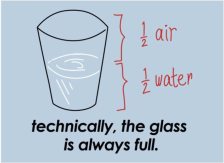
Proofs

An argument that convincingly demonstrates the truth of a statement

Proofs in Computer Science

- Prove that an algorithm is correct
- Prove that an algorithm has a particular runtime
- Data structure proofs often lead to efficient and simpler algorithms
- Develops useful habits in thinking: e.g.
  - working with precise notations and definitions
  - exactly and unambiguously formulating statements
  - paying attention to all possibilities





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

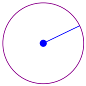
Terminology

- **Axiom:** A basic assumption about mathematical structure that is accepted to be true. e.g.
  - *There is a straight line between any two points*
  - $2 > 1$
- **Theorem:** Important proposition that has a proof
- **Lemma:** Proposition that serves as an intermediate step in proof of a theorem
- **Corollary:** Proposition that follows directly (easily) from a theorem
  - Essentially a special case of the general statement of the theorem
- **Rules of Inference:** The justification for the steps in the chain of deductions in a proof
- **Fallacy:** An incorrect reasoning or deduction

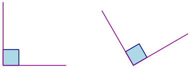
Axioms of Euclidean Geometry

Any two points can be joined by exactly one line segment

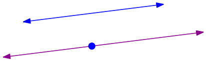
Any line segmented can be extended into a line



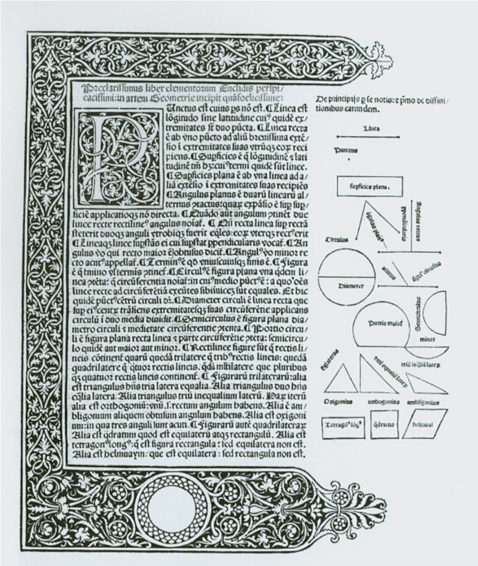
Given a point p and a length r, there is a circle of radius r with center p



Any two right angles are congruent

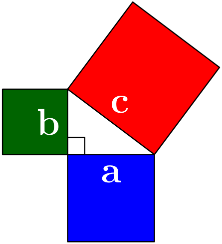


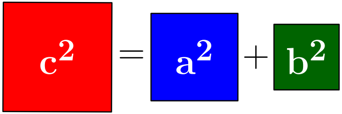
Given a line ℓ and a point p not on ℓ, there is exactly one line through p parallel to ℓ

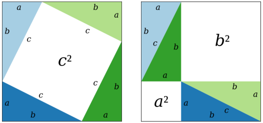


The first page of the first printed edition of Euclid's Elements, published in 1482.

The Pythogorus theorem

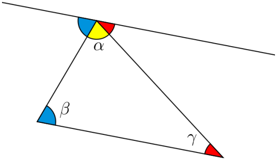






$c^2 = a^2 + b^2$

The Triangle Angles Sum theorem



Rules of Inference

modus ponens

Suppose we know (have a proof) that

1. P is true and
2. $P \to Q$ is true

Then Q must be true

$$\frac{P, \quad P \to Q}{Q}$$

P and $P \to Q$ are two hypotheses and Q is the conclusion in this case

$\because$ the following is a tautology

$$P \wedge (P \to Q) \to Q$$

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

modus tollens

Suppose we know (have a proof) that

1. Q is false and
2. $P \to Q$ is true

Then P must be false

$$\frac{\neg Q,\quad P \to Q}{\neg P}$$

$\neg Q$ and $P \to Q$ are two hypotheses and $\neg P$ is the conclusion in this case

$\because$ the following is a tautology

$$\neg Q \wedge (P \to Q) \to \neg P$$

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

hypothetical syllogism

Suppose we know (have a proof) that

1. $P \rightarrow Q$ is true $\because$ and
2. $Q \rightarrow R$ is true

Then $P \rightarrow R$ must be true

$$\frac{P \rightarrow Q, \quad Q \rightarrow R}{P \rightarrow R}$$

Fallacies

Theorem

$2 = 1 \quad ^{?}$

Proof:

Let	$a = b$	▷ Assumption
$\implies$	$a^2 = ab$	▷ multiply by a
$\implies$	$a^2 + a^2 - 2ab = ab + a^2 - 2ab$	▷ add $a^2 - 2ab$
$\implies$	$2(a^2 - ab) = a^2 - ab$	
$\implies$	$2 = 1$	▷ divide by $a^2 - ab$

Proof

A proof is an argument that can withstand all criticisms from a highly caffeinated adversary (your TA).

---

quote from 15-251@CMU

A mathematical proof should resemble a simple and clear-cut constellation, not a scattered cluster in the Milky Way.

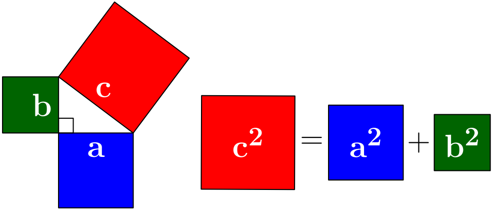
G.H. Hardy, A Mathematician's Apology

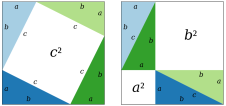
The mathematician's patterns, like the painter's or the poet's must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics.

G. H. Hardy

Pythagoras's Theorem ($\sim$ 500 BC)

$a^2 + b^2 = c^2$ has solutions where a, b, and c are positive integers





$c^2 = a^2 + b^2$

This statement is TRUE,

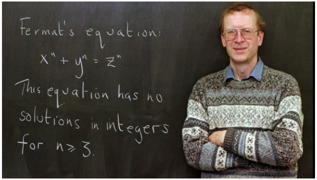
e.g. $a = 3$, $b = 4$, and $c = 5$

Proving Statements

Fermat's Last Theorem (1637)

$a^3 + b^3 = c^3$ has no solution where a, b, c are positive integers

Andrew Wiles (1994) proved this statement to be TRUE



- Wiles announced "proof" on 23 June 1993
- In September 1993 error was found in the proof
- On 19 September 1994, Wiles corrected the proof
- The corrected proof was published in 1995

Proving Statements

Euler Conjecture (1769)

$a^4 + b^4 + c^4 = d^4$ has no solutions where a, b, c, d are positive integers

Noam Elkies (1987) proved this statement FALSE

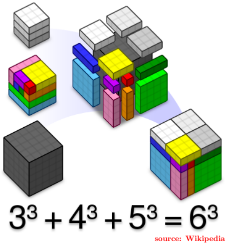
$a = 2682440$,

$b = 15365639$,

$c = 18796760$,

$d = 20615673$,

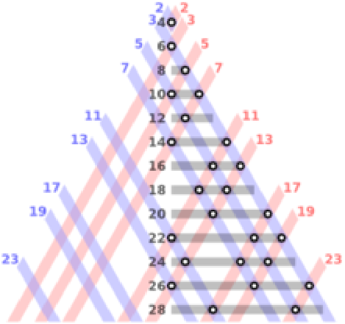
is a solution



Proving Statements

Goldbach Conjecture (1742)

Every even integer > 2 is the sum of two primes



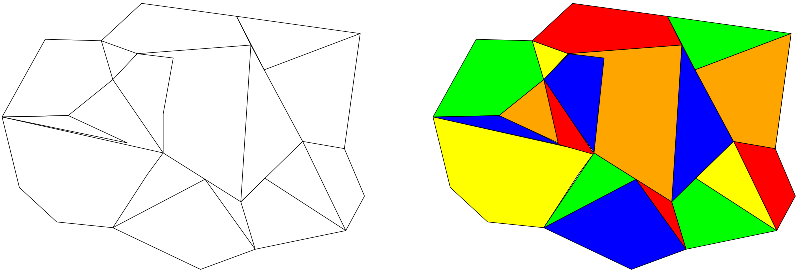
Sum of two primes at intersection of two lines. (source: Wikipedia)

- No one yet knows the truth value of this statement
- Every even integer ever checked is a sum of two primes
- Just one counter-example will disprove the claim
- Homework!

Proving Statements

Conjecture (1852)

Regions of any 2-d map can be colored with 4 colors so that no neighboring regions have the same color.



Graphs Applications: Coloring

- Kempe (1879) announced a proof
- Tait (1880) announced an alternative proof
- Heawood (1890) found a flaw in Kempe's proof
- Petersen (1881) found a flaw in Tait's proof
- Heesch (1969) reduced the statement to checking a large number of cases
- Appel & Haken (1976) gave a "proof", that involved a computer program to check 1936 cases (1200 hours of computer time)
- Robertson et.al. (1997) gave another simpler "proof" but still involved computer program

- No human can check all the cases
- What if the program has a bug
- What if the compiler/system hardware has a bug