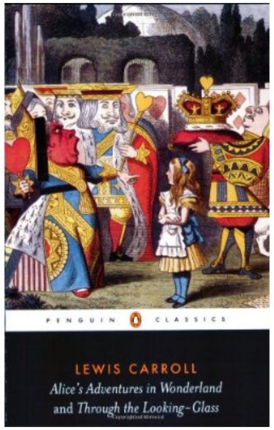
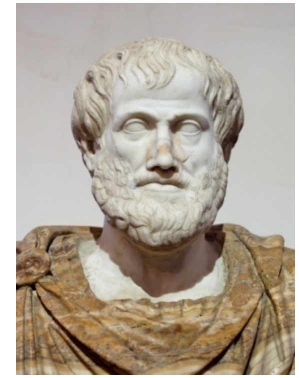
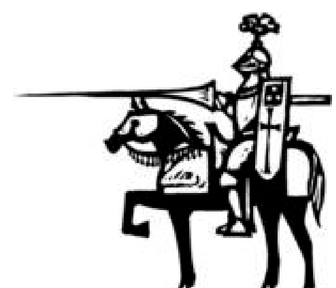




COMP 1002

Intro to Logic for Computer Scientists

Lecture 12



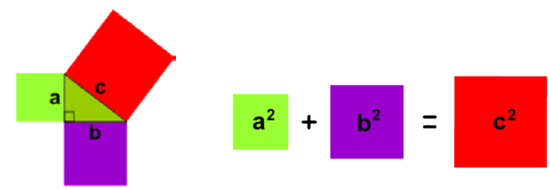
Proofs

- What is a theorem?
  - Lemma, claim, etc
- What is a proof?
  - Where do we start?
  - Where do we stop?
  - What steps do we take?
  - How much detail is needed?

Theories and theorems

- **Theory:** axioms + everything derived from them using rules of inference
  - Euclidean geometry, set theory, theory of reals, theory of integers, Boolean algebra…
  - In verification: theory of arrays.

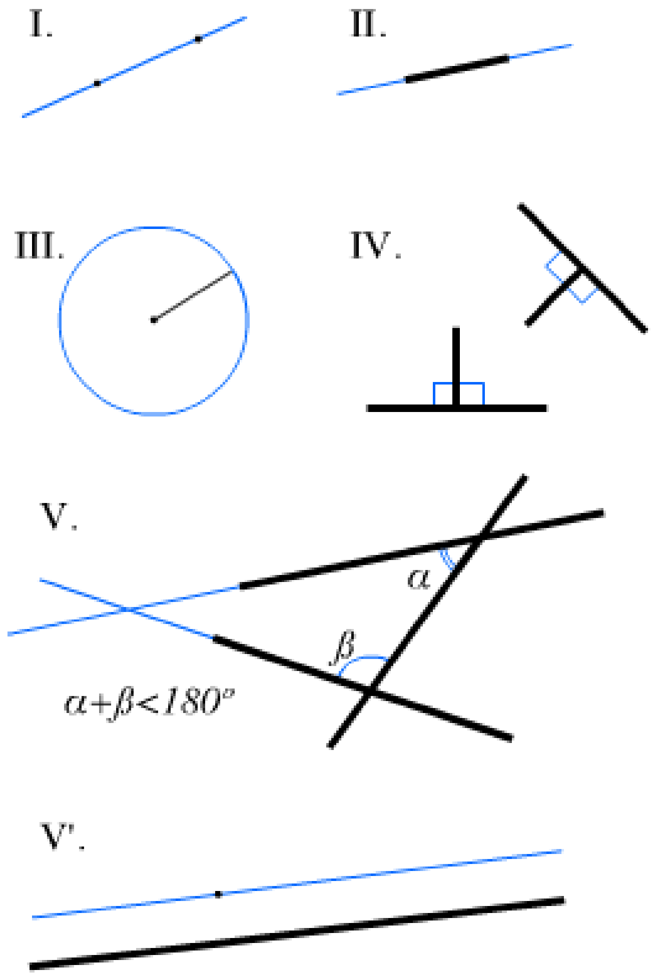
- **Theorem:** a true statement in a theory
  - Proved from axioms (usually, from already proven theorems)



Pythagorean theorem

- A statement can be a theorem in one theory and false in another!
  - Between any two numbers there is another number.
    - A theorem for real numbers. False for integers!

Axioms example: Euclid’s postulates

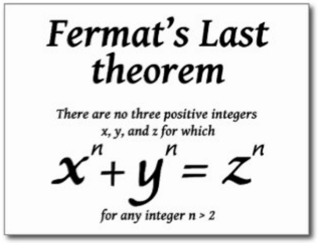


I. Through 2 points a line segment can be drawn
II. A line segment can be extended to a straight line indefinitely
III. Given a line segment, a circle can be drawn with it as a radius and one endpoint as a centre
IV. All right angles are congruent
V. Parallel postulate

Some axioms for propositional logic

- For any formulas A, B, C:
  - A $\lor \neg A \equiv True$ $\qquad A \land \neg A \equiv False$
  - $True \lor A \equiv True$. $\qquad True \land A \equiv A$
  - $False \lor A \equiv A$. $\qquad False \land A \equiv False$
  - A$\lor A \equiv A \land A \equiv A$
- Also, like in arithmetic (with ∨ as +, ∧ as *)
  - $A \lor B \equiv B \lor A \quad and \ \ (A \lor B) \lor C \equiv A \lor (B \lor C)$
  - Same holds for ∧.
  - Also, $(A \lor B) \land C \equiv (A \land C) \lor (B \land C)$
- And unlike arithmetic
  - $(A \land B\ ) \lor C \equiv \ \ (A \lor C) \land (B \lor C)$

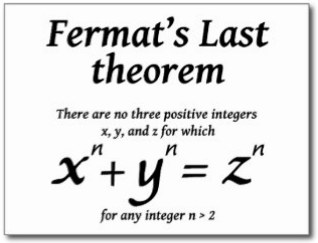
Counterexamples



- To disprove a statement, enough to give a counterexample: a scenario where it is false
  - To disprove that $A \to B \equiv B \to A$
    - Take $A = true, B = false$,
    - Then $A \to B$ is false, but $\mathrm{B} \to A$ is true.

  - To disprove that if $\forall x \, \exists \, y \; P(x, y)$, then $\exists y \, \forall x \; P(x, y)$,
    - Set the domain of x and y to be {0,1}
    - Set P(0,0) and P(1,1) to true, and P(0,1), P(1,0) to false.
    - Then $\forall x \, \exists \, y \; P(x, y)$ is true, but $\exists y \, \forall x \; P(x, y)$ is false.
      - Because $\big(P(0,0) \vee P(1,0)\big) \wedge \big(P(0,1) \vee P(1,1)\big)$ is true,
      - But $(P(0,0) \wedge P(1,0)) \vee (P(0,1) \wedge P(1,1))$ is false.

Constructive proofs

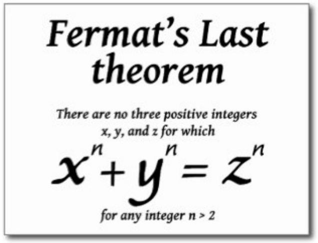


- To prove a statement of the form $\exists x$, sometimes can just find that x
  - $\exists x \in \mathbb{N}\ Even(x) \wedge Prime(x)$
    - Set x=2.
    - Even(x) holds.
    - Prime(x) holds.
    - Therefore, $Even(x) \wedge Prime(x)$ holds.
    - Done.
  - This proof is **constructive**, because we constructed an x which makes the formula $Even(x) \wedge Prime(x)$ true.

Proof

- To prove that something of the form $\forall x\ F(x)$:
  - Make sure it holds in every scenario (method of exhaustion)
    - For all possible values of A and B, $\neg B \rightarrow \neg A$ is equivalent to $A \rightarrow B$, by checking the truth table.
  - But there can be too many scenarios!
    - For any integer, there is a larger integer which is a prime.
    - For any two reals, there is a real between them.
  - Instead, use axioms and rules of inference to derive it.

    $\neg B \rightarrow \neg A \equiv \neg\neg B \vee \neg A \equiv B \vee \neg A \equiv \neg A \vee B \equiv A \rightarrow B$
    - So $(\neg B \rightarrow \neg A) \leftrightarrow (A \rightarrow B)$ is a tautology.
    - And, therefore, $\forall A, B \in \{True, False\}$, $\neg B \rightarrow \neg A \equiv A \rightarrow B$



Puzzle 11

- Let $S = \{x \in \mathbb{N} \mid x\ is\ even \wedge\ x\ is\ odd\}$

- Prove or disprove:

$$\forall x \in S, \qquad x\ does\ not\ divide\ x^2$$