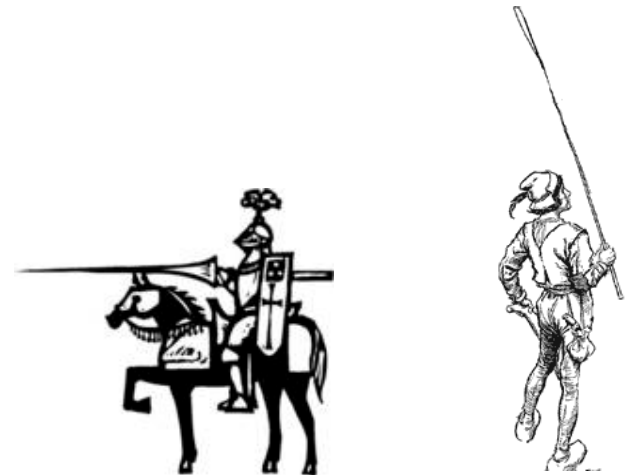


# COMP 1002

## Intro to Logic for Computer Scientists

### Lecture 12



# Admin stuff

- Assignments schedule?
  - Split a2 and a3 in two (A2,3,4,5) , 5% each.
  - A2 due Feb 17<sup>th</sup>.
- Midterm date?
  - March 2<sup>nd</sup>.
- No office hour on Feb 9<sup>th</sup>



# 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?

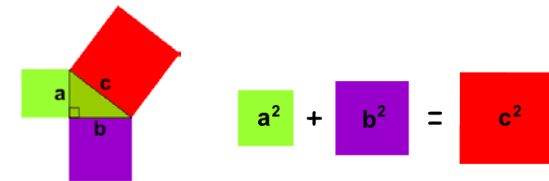


# Theories and theorems



- **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.

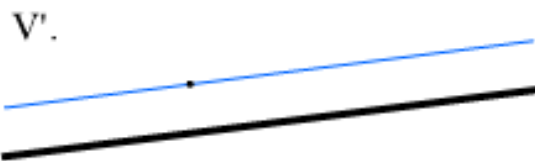
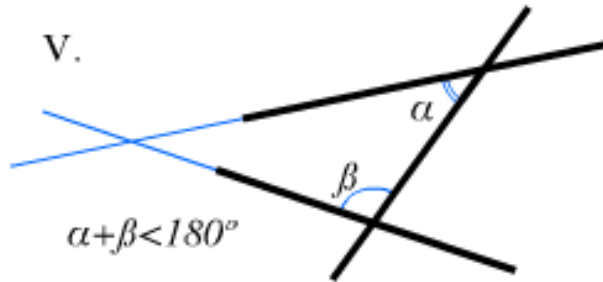
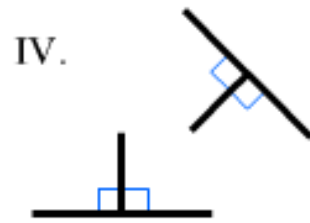
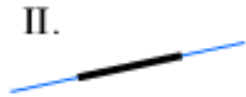
- **Theorem:** a true statement in a theory
  - Proved from axioms (usually, from already proven theorems)



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  $A, B, C$ :
  - $A \vee \neg A \equiv \text{True}$                        $A \wedge \neg A \equiv \text{False}$
  - $\text{True} \vee A \equiv \text{True}$ .                       $\text{True} \wedge A \equiv A$
  - $\text{False} \vee A \equiv A$ .                       $\text{False} \wedge A \equiv \text{False}$
  - $A \vee A \equiv A \wedge A \equiv A$
- Also, like in arithmetic (with  $\vee$  as  $+$ ,  $\wedge$  as  $*$ )
  - $A \vee B \equiv B \vee A$     and     $(A \vee B) \vee C \equiv A \vee (B \vee C)$
  - Same holds for  $\wedge$ .
  - Also,  $(A \vee B) \wedge C \equiv (A \wedge C) \vee (B \wedge C)$
- And unlike arithmetic
  - $(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$

$$x^n + y^n = z^n$$

# Counterexamples

- To disprove a statement, enough to give a counterexample: a scenario where it is false
  - To disprove that  $A \rightarrow B \equiv B \rightarrow A$ 
    - Take  $A = \text{true}, B = \text{false}$ ,
    - Then  $A \rightarrow B$  is false, but  $B \rightarrow A$  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  $(P(0,0) \vee P(1,0)) \wedge (P(0,1) \vee P(1,1))$  is true,
      - But  $(P(0,0) \wedge P(1,0)) \vee (P(0,1) \wedge P(1,1))$  is false.

## Fermat's Last theorem

There are no three positive integers  
 $x, y,$  and  $z$  for which

$$x^n + y^n = z^n$$

for any integer  $n > 2$

# Constructive proofs

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

## Fermat's Last theorem

There are no three positive integers  
 $x$ ,  $y$ , and  $z$  for which

$$x^n + y^n = z^n$$

for any integer  $n > 2$

# Puzzle 11

- Let

$$S = \{x \in \mathbb{N} \mid x \text{ is even}\} \cap \{x \in \mathbb{N} \mid x \text{ is odd}\}$$

- Prove or disprove:

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

