CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

Today

- Some revision missing exercise
- Definitions and facts about numbers
- Direct proof

Revision exercises

Exercise: 2021 midterm-1

Problem 3. [10 points]

Give negations of the following statements. Reasoning is not required.

(a) [1 point] $p \wedge q$

(b) [1 point] $p \vee q$

(c) [1 point] $p \oplus q$

(d) [1 point] $p \to q$

(e) [1 point] $p \leftrightarrow q$

Exercise: 2021 midterm-1

Problem 3. [10 points]

Give negations of the following statements. Reasoning is not required.

(f) [1 point] $\forall x, \forall y$ **such that** $p(x, y)$

(g) [1 point] $\forall x, \exists y$ **such that** $p(x, y)$

(h) [1 point] $\exists x, \forall y$ **such that** $p(x, y)$

(i) [1 point] $\exists x, \exists y$ **such that** $p(x, y)$

(j) [1 point] $\exists x, \forall y, \exists z$ **such that** $p(x, y, z)$

Final 2021

Problem 6. [5 points]

Prove that if $n^2 + 8n + 20$ is odd, then n is odd for natural numbers n.

- Express the propositions we need to prove here

Final 2021

Problem 5. [5 points]

Prove using contradiction that the cube root of an irrational number is irrational.

- Express the propositions we need to prove here

Definitions and facts about numbers

Symbols

- Integers Z
- Natural numbers N
- Real numbers R
- $| x |$
- sum Σ
- $a \mid b$
- b mod a

Formal definitions

- Even/Odd numbers
- Rational/Irrational numbers
- Prime/Composite numbers

Even/odd numbers

We say an integer n is even if: $\exists k \in \mathbf{Z}$ such that $n = 2k$

How can you define an odd number?

Rational/Irrational numbers

We say a real number r is rational if $\exists m, n \in \mathbf{Z}$ such that $r = n/m$

(and n and m have no common divisor).

Prime/Composite numbers

We say a natural number n is prime if $n > 1$, and

$$\forall r, s \in \mathbf{N}, n = rs \to (r = 1 \lor s = 1)$$

d | n

We say a non-zero integer d divides an integer n, if

$$\exists k \in \mathbf{Z}, \text{ such that } n = k * d.$$

Direct proof

Methods of mathematical proof

Statements	Method of proof
Proving existential statements (Disproving universal statements)	Constructive proof Non-constructive proof
Proving universal statements (Disproving existential statements)	Direct proof Proof by mathematical induction Well-ordering principle Proof by exhaustion Proof by cases Proof by contradiction

- Prove: If p is an even number, then p^2 is an even number
- Proof.
    - Assume p is an even integer. By definition of an even number, $p = 2k$ for some integer k
    - squaring both sides of “$p=2k$”, we get $p^2 = 4k^2$
    - Thus $p^2 = 2(2k^2)$ which is twice an integer
    - Thus p^2 is even

Skill: Writing a proof

- Writing a proof that is clear, concise, and rigorous is a skill that can be honed with practice and a deep understanding of the subject matter.

How to hone your proof writing skill

- Understand the statement
- Choose a proof method
- Struct your proof
  - Starts with Proof.
  - State assumptions clearly
  - Proceed Step-by-Step: Each step should follow logically from the previous one. Every claim you make should either be self-evident, previously proven, or proven within your proof.
  - End with QED.
- Read again your proof. Make it read like an essay.

Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

- Proof.
  - Suppose n is an even number, and m is an odd number, we need to show n+m is odd
  - since n is an even number, n = 2k for some integer k
  - since m is an odd number, m = 2k’+1 for some integer k’
  - Thus n+m = 2(k+k’)+1 which shows n+m is odd.
- QED.

n is odd $\Rightarrow n^2$ is odd

Proposition

- The square of an odd integer is odd.

- Proof.
    - Suppose n is an odd number. We want to show that n^2 is an odd number.
    - Since n is odd, $n = 2k+1$ for some integer k
    - $n^2 = 4k^2+4k+1= 2(2k^2+2k) + 1$
    - Thus n^2 is odd
- QED.

If $a|b$ and $b|c$, then $a|c$

Proposition

- (Transitivity) For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

- Proof.
    - Suppose a, b, c are three integers and $a|b$, $b|c$.
    - Since $a|b$, we have $b = ak$ for some integer k
    - Since $b|c$, we have $c = bk'$ for some integer k'
    - Thus, $c = a (k*k')$
    - Thus $a|c$.
- QED.

Summary

- Proof techniques — direct proof. **Commonly used for proving “for all x, P(x) -> Q(x)”.**

- A proof is an essay of rigorous arguments. Practice your proof-writing skill.