# CSE215
# Foundations of Computer Science

**Instructor: Zhoulai Fu**

**State University of New York, Korea**

# Today

- A missing exercise
- Definitions and facts about numbers
- Direct proof

* Exercise 5

Determine if the following argument is valid:

p ↔ q
q ⊕ r
————
∴ p \/ r

# Solution

- It is valid.
- Assume the premises are true.
- Namely,  p<->q is true and q xor r is true.
- Since  p <->q is true, we know p and q must be the same truth value.
- Since q xor r is true, we know q and r must be different truth values.
- Thus, p and r must be different truth values.
- Thus p and r can be either (true and false), or (false and true)
- Thus $q \vee r$, namely, the conclusion, is true.

# Definitions and facts about numbers

# Symbols

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

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

# 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<br>(Disproving universal statements) | Constructive proof<br>Non-constructive proof |
| Proving universal statements<br>(Disproving existential statements) | Direct proof<br>Proof by mathematical induction<br>Well-ordering principle<br>Proof by exhaustion<br>Proof by cases<br>Proof by contradiction |

# 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.

# Odd = difference of squares

**Proposition**

- Every odd integer is equal to the difference between the squares of two integers

**Workout**

- Write a formal statement.
  $\forall$ integer $k$, $\exists$ integers $m, n$ such that $(2k+1) = m^2 - n^2$.
- Try out a few examples.

$$\begin{aligned} 1 &= 1^2 - 0^2 & -1 &= 0^2 - (-1)^2 \\ 3 &= 2^2 - 1^2 & -3 &= (-1)^2 - (-2)^2 \\ 5 &= 3^2 - 2^2 & -5 &= (-2)^2 - (-3)^2 \\ 7 &= 4^2 - 3^2 & -7 &= (-3)^2 - (-4)^2 \end{aligned}$$

- Find a pattern.
  $(k+1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 =$ odd

- Proof.
  - Suppose $x$ is an odd number, we need to show:
    - There exists two integers $m$ and $n$ such that $x = m^2 - n^2$
  - Since $x$ is odd, we can write $x = 2k+1$ for some integer $k$
  - Let $m = k+1$, and $n = k$. Then, we have $m^2 - n^2 = 2k+1 = x$
- 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.

## Summation

**Proposition**

- $1 + 2 + 3 + \cdots + n = n(n+1)/2.$

## Proof

- Formal statement. $\forall$ natural number $n$, prove that $1 + 2 + 3 + \cdots + n = n(n+1)/2$.
- $S = 1 + 2 + 3 + \cdots + n$

$$\implies S = n + (n-1) + (n-2) + \cdots + 1$$

(addition on integers is commutative)

$$\implies 2S = \underbrace{(n+1) + (n+1) + (n+1) + \cdots + (n+1)}_{n \text{ terms}}$$

(adding the previous two equations)

$$\implies 2S = n(n+1) \qquad \text{(simplifying)}$$

$$\implies S = n(n+1)/2 \qquad \text{(divide both sides by 2)}$$

Break

Exercises

**Problem 4. [5 points]**

Prove that the sum of the squares of any two consecutive odd integers is even.

- Proof.
  - We need to prove the following:
    - for any integer n, $(2n+1)^2 + (2n+3)^2$ is even
  - We know $(2n+1)^2 + (2n+3)^2 = 8n^2 + 20n + 2 = 2(4n^2 + 10n+1)$
  - Thus, $(2n+1)^2 + (2n+3)^2$ is even
- QED.

**Problem 5. [5 points]**

Suppose that $x$ and $y$ are real numbers. Prove that $x = y$ if and only if $xy = (x + y)^2/4$.

- Proof.
  - Suppose that x and y are real numbers.
  - We need to prove (1) $x = y \to xy = (x+y)^2/4$ and (2) $xy = (x+y)^2/4 \to xy$
  - #1 is clearly true
  - To show #2, we assume $xy=(x+y)^2/4$. Thus $x^2 - 2xy + y^2 = 0$. Thus, $(x-y)^2=0$. Thus $x=y$
- QED

# Problem 5. Direct proof (points = 5)

Suppose a, b and c are integers. If $a^2|b$ and $b^3|c$, then $a^6|c$.

# Problem 5. Direct proof (points = 5)

Suppose a, b and c are integers. If $a^2|b$ and $b^3|c$, then $a^6|c$.

- Proof.
  - Assume a^2 | b and b^3 | c
  - We have b = k a^2 for some integer k, and c = k' b^3 for some integer k'.
  - Thus, c = (k' k^3) a^6
- QED

# That is all for today

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

*Thank you!*