$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4\ldots}}}}$$

$$1-1+1-1+1\ldots\ldots = ?$$

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4\ldots}}}}$$

Discrete mathematics

# The Foundations: Logic and Proofs

$$\exists_{x\in\Re}\exists_{y\in\Re}(x=y)$$

$$\forall_{x}(\Re \mid x)$$

$$\sum_{x=1}^{\infty}\frac{1}{x}=?$$

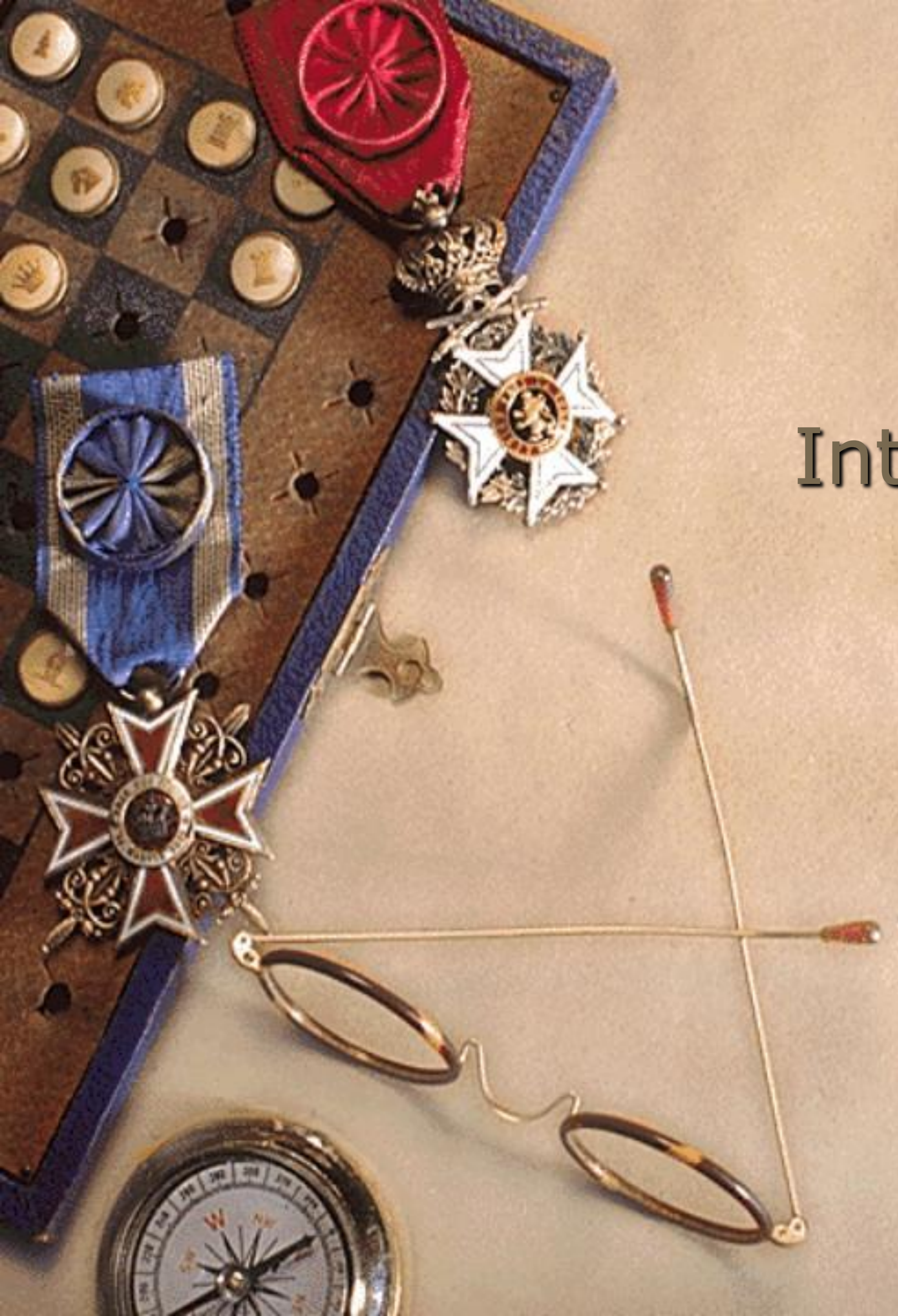
$$\sum_{x=1}^{\infty}x=?$$


RIZOAN TOUFIQ

ASSISTANT PROFESSOR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

RAJSHAHI UNIVERSITY OF ENGINEERING & TECHNOLOGY



# Introduction to Proofs

Section 1.7

# Section Summary

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
  - Proof of the Contrapositive
  - Proof by Contradiction

# Proofs of Mathematical Statements

- A *proof* is a valid argument that establishes the truth of a statement.
- In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - Easier for to understand and to explain to people.
  - But it is also easier to introduce errors.
- Proofs have many practical applications:
  - verification that **computer programs** are **correct**
  - establishing that **operating systems** are **secure**
  - enabling programs to make inferences in **artificial intelligence**
  - showing that **system specifications** are consistent

# Some Terminology

- A **theorem** is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - *axioms* (statements which are given as true)
  - rules of inference
- A **lemma** is a 'helping theorem' or a result which is needed to prove a theorem.
- A **corollary** is a result which follows directly from a theorem.
- Less important theorems are sometimes called **propositions**.
- A **conjecture** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

# Understanding How Theorems Are Stated

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

"If $x > y$, where $x$ and $y$ are positive real numbers, then $x^2 > y^2$ "

really means

"For all positive real numbers $x$ and $y$, if $x > y$, then $x^2 > y^2$ ."

# Methods of Proving Theorems

- Many theorems have the form:
$$\forall x(P(x) \rightarrow Q(x))$$
- To prove them, we show that where $c$ is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$

# Even and Odd Integers

**Definition**: The integer $n$ is **even** if there exists an integer $k$ such that $n = 2k$, and $n$ is **odd** if there exists an integer $k$, such that $n = 2k + 1$. Note that every integer is either even or odd and no integer is both even and odd.

# Direct Proof

## (Proving Conditional Statements: $p \to q$)

- **Direct Proof:** Assume that $p$ is true. Use rules of inference, axioms, and logical equivalences to show that $q$ must also be true.

**Example**: Give a direct proof of the theorem "If $n$ is an odd integer, then $n^2$ is odd."

**Solution**: Assume that $n$ is odd. Then $n = 2k + 1$ for an integer $k$. Squaring both sides of the equation, we get:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

We have proved that if n is an odd integer, then $n^2$ is an odd integer.

◀

(◀ marks the end of the proof. Sometimes **QED** is used instead. )

# Direct Proof

## (Proving Conditional Statements: $p \to q$)

**Definition:** The real number $r$ is *rational* if there exist integers $p$ and $q$ where $q \neq 0$ such that $r = p/q$

**Example:** Prove that the sum of two rational numbers is rational.

**Solution:** Assume $r$ and $s$ are two rational numbers. Then there must be integers $p, q$ and also $t, u$ such that

$$r = p/q, \quad s = t/u, \quad u \neq 0, \; q \neq 0$$

Thus the sum is rational.

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu+qt}{qu} = \frac{v}{w}$$

where $v = pu + qt$
$w = qu \neq 0$

◀

# Direct Proof

## (Proving Conditional Statements: $p \rightarrow q$)

**Example**: Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

(An integer a is a perfect square if there is an integer b such that $a = b^2$.)

**Solution**:

Home Task

# Proof by Contraposition

## (Proving Conditional Statements: $p \to q$)

- **Proof by Contraposition**: Assume $\neg q$ and show $\neg p$ is true also. This is sometimes called an *indirect proof* method. If we give a direct proof of $\neg q \to \neg p$ then we have a proof of $p \to$ q.

**Example**: Prove that if $n$ is an integer and $3n + 2$ is odd, then $n$ is odd.

**Solution**: Assume $n$ is even. So, $n = 2k$ for some integer $k$. Thus

$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) = 2j$ for $j = 3k + 1$

Therefore $3n + 2$ is even. Since we have shown $\neg q \to \neg p$, $p \to q$ must hold as well. If $n$ is an integer and $3n + 2$ is odd (not even), then $n$ is odd (not even).

# Proof by Contraposition

**(Proving Conditional Statements: $p \rightarrow q$)**

**Example**: Prove that for an integer $n$, if $n^2$ is odd, then $n$ is odd.

**Solution**: Use proof by **contraposition**. Assume $n$ is even (i.e., not odd). Therefore, there exists an integer $k$ such that $n = 2k$. Hence,

$$n^2 = 4k^2 = 2(2k^2)$$

and $n^2$ is even(i.e., not odd).

We have shown that if $n$ is an even integer, then $n^2$ is even. Therefore by contraposition, for an integer $n$, if $n^2$ is odd, then $n$ is odd.

◀

# Vacuous And Trivial Proofs

## Proving Conditional Statements: $p \rightarrow q$

- **Trivial Proof:** If we know $q$ is true, the $p \rightarrow q$ is true as well.

  "If it is raining then 1=1."

- **Vacuous Proof:** If we know $p$ is false then $p \rightarrow q$ is true as well.

  "If I am both rich and poor then $2 + 2 = 5$."

[Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction, as we will see in Chapter 5) ]

# Proof by Contradiction

**(Proving Conditional Statements: $p \rightarrow q$)**

- **Proof by Contradiction:**
  - ✓ To prove $p$
  - ✓ Assume $\neg p$
  - ✓ Derive a contradiction such as $p \land \neg p$. (an indirect form of proof).

Since we have shown that $\neg p \rightarrow \mathbf{F}$ is true ,

it follows that the contrapositive $\mathbf{T} \rightarrow p$ also holds.

# Proof by Contradiction

## (Proving Conditional Statements: $p \rightarrow q$)

- **Example**: Use a proof by contradiction to give a proof that $\sqrt{2}$ is irrational.

**Solution:** Suppose $\sqrt{2}$ is rational. Then there exists integers $a$ and $b$ with $\sqrt{2} = a/b$, where $b \neq 0$ and $a$ and $b$ have no common factors (see Chapter 4). Then

$$2 = \frac{a^2}{b^2} \qquad 2b^2 = a^2$$

Therefore $a^2$ must be even. If $a^2$ is even then $a$ must be even (an exercise). Since $a$ is even, $a = 2c$ for some integer $c$. Thus,

$$2b^2 = 4c^2 \qquad b^2 = 2c^2$$

Therefore $b^2$ is even. Again then $b$ must be even as well.

But then 2 must divide both $a$ and $b$. This contradicts our assumption that $a$ and $b$ have no common factors. We have proved by contradiction that our initial assumption must be false and therefore $\sqrt{2}$ is irrational .

◀

# Proofs Of Equivalence

- To prove a theorem that is a **biconditional** statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

**Example**: Prove the theorem: "If $n$ is an integer, then $n$ is odd if and only if $n^2$ is odd."

**Solution:** We have already shown (previous slides) that both $p \rightarrow q$ and $q \rightarrow p$. Therefore we can conclude $p \leftrightarrow q$.

Sometimes *iff* is used as an abbreviation for "if an only if," as in

"If $n$ is an integer, then $n$ is odd iif $n^2$ is odd."

# Counterexamples

- **$\forall_x P(x)$ is false**, we need only find a counterexample.
- **Example**: x for which P(x) is false

**Example**: Show that the statement “Every positive integer is the sum of the squares of two integers” is false.

**Solution:** there is no way to get 3 as the sum of two terms each of which is 0 or 1.

$$2^2 = 4$$

$$\{0, 1\},$$

$$0 + 1 = 1 \neq 3$$

# Mistakes in Proofs

"Proof" that $1 = 2$

| **Step** | **Reason** |
|---|---|
| 1. $a = b$ | Premise |
| 2. $a^2 = a \times b$ | Multiply both sides of (1) by a |
| 3. $a^2 - b^2 = a \times b - b^2$ | Subtract $b^2$ from both sides of (2) |
| 4. $(a-b)(a+b) = b(a-b)$ | Algebra on (3) |
| 5. $a + b = b$ | Divide both sides by $a - b$ |
| 6. $2b = b$ | Replace a by b in (5) because $a = b$ |
| 7. $2 = 1$ | Divide both sides of (6) by b |

**Solution**: Step 5. a - b = 0 by the premise and division by 0 is undefined.

# Query???

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4\ldots.}}}}$$

$$\exists_{x\in\Re}\exists_{y\in\Re}\,(\,x = y\,) = ?$$

$$\sum_{x=1}^{\infty} x = ?$$

$$\sum_{x=1}^{\infty}\frac{1}{x} = ?$$

$$\forall_{x}\,(\,\Re \mid x\,) = ?$$

$$\exists_{x\in\Re}\exists_{y\in\Re}\,(\,x = y\,) = ?$$

$$\sqrt{1+\sqrt{2+\sqrt{3+\sqrt{4\ldots.}}}} = ?$$

$$1-1+1-1+1\ldots\ldots\ldots = ?$$

$$\sum_{x=1}^{\infty}\frac{1}{x} = ?$$