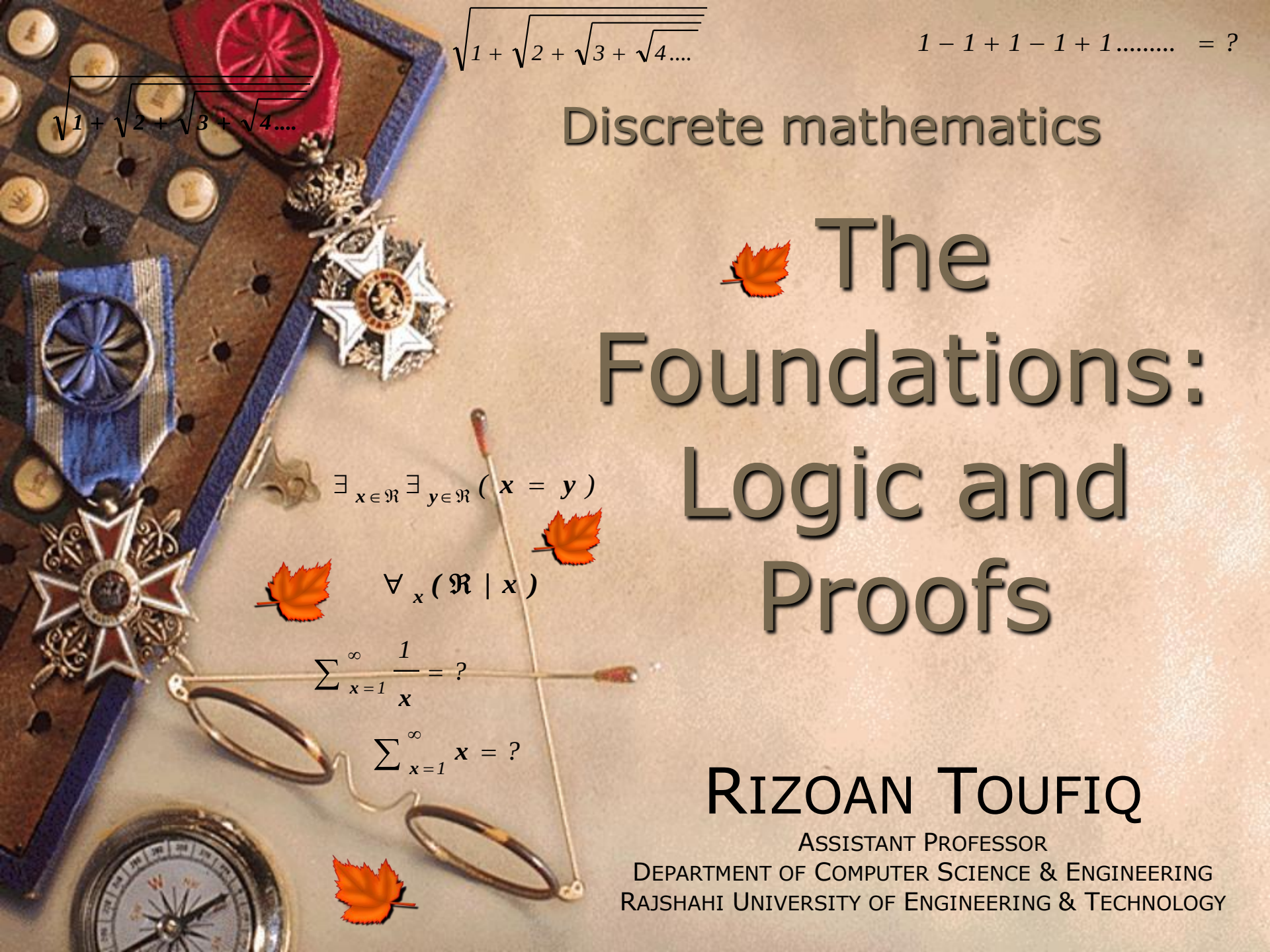
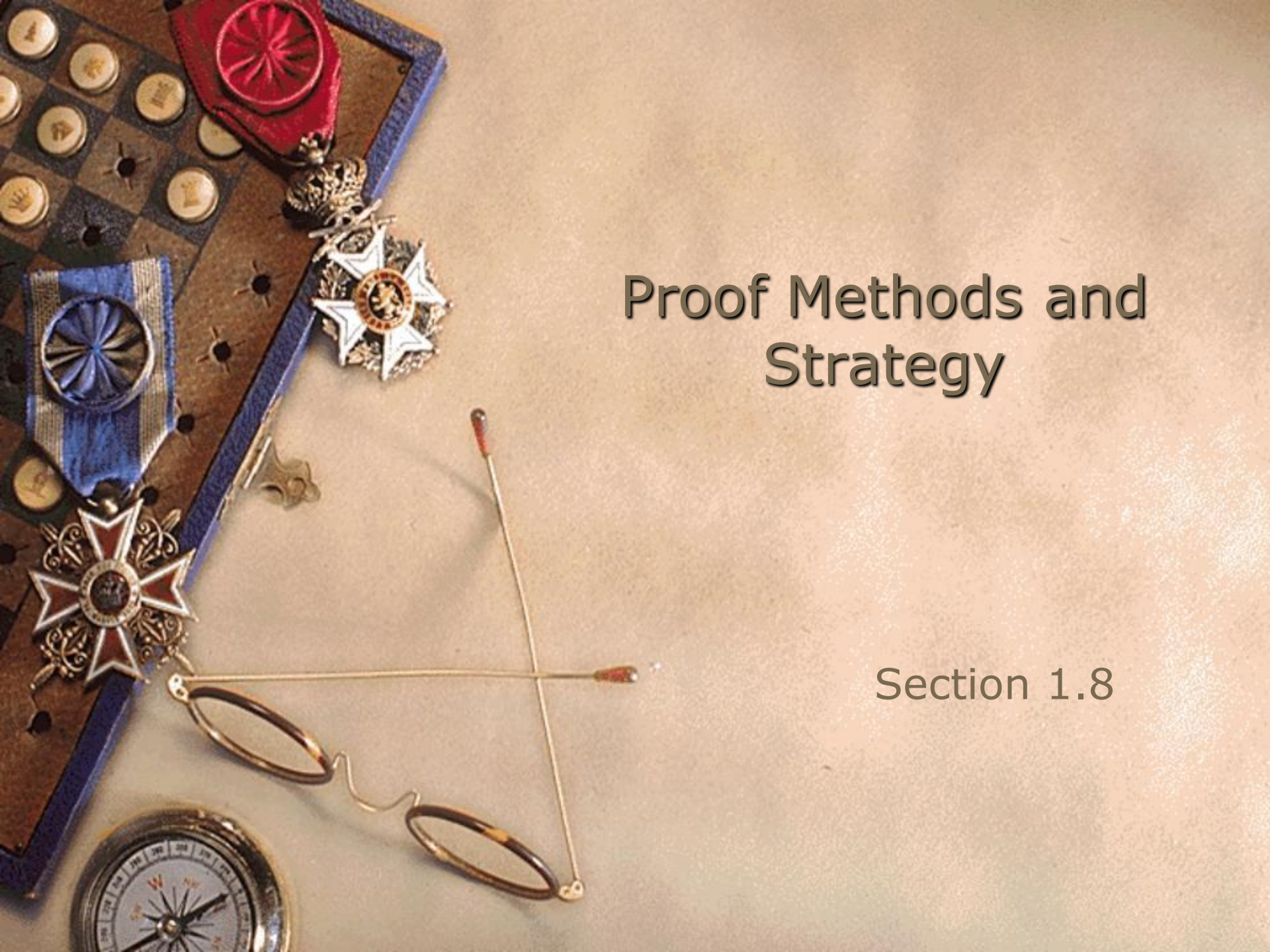


RIZOAN TOUFIQ

ASSISTANT PROFESSOR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

RAJSHAHI UNIVERSITY OF ENGINEERING & TECHNOLOGY



Proof Methods and Strategy

Section 1.8

Section Summary

- Proof by Cases
- Existence Proofs
  - Constructive
  - Non-constructive
- Uniqueness Proofs
- Proof Strategies
- Looking For Counterexample
- Proof Strategy in Action
- Proving Universally Quantified Assertions
- Open Problems

Exhaustive Proof and Proof by Cases

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$$

- Use the tautology

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

- Each of the implications $\mathbf{p_i \rightarrow q}$, i = 1, 2,...,n is a *case*.

Exhaustive Proof

- Some theorems can be proved by examining a relatively small number of examples.
- An exhaustive proof is a **special type of proof by cases** where **each case** involves checking a **single example.**
- **Example:** Prove that $(n + 1)^3 \geq 3n$ if n is a positive integer with $n \leq 4$.
- **Proof:**
  - We use a proof by exhaustion.
  - We only need verify the inequality $(n + 1)^3 \geq 3^n$ when n = 1,2,3 and 4
  - n=1, $(n + 1)^3 = 8$, $3^n = 3$
  - n=2, $(n + 1)^3 = 27$, $3^n = 9$
  - n=3, $(n + 1)^3 = 64$, $3^n = 27$
  - n=4, $(n + 1)^3 = 125$, $3^n = 81$
- We have used the method of **exhaustion** to prove that $(n + 1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$

Proof by Cases

- A proof by cases must cover **all possible cases** that arise in a theorem.

Example: Let $a @ b = \max\{a, b\} = a$ if $a \geq b$, otherwise $a @ b = \max\{a, b\} = b$. Show that for all real numbers a, b, c

$$(a @ b) @ c = a @ (b @ c)$$

(This means the operation @ is associative.)

Proof: Let a, b, and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1.	$a \geq b \geq c$	4.	$b \geq c \geq a$
2.	$a \geq c \geq b$	5.	$c \geq a \geq b$
3.	$b \geq a \geq c$	6.	$c \geq b \geq a$

Case 1: $a \geq b \geq c$, so $(a @ b) = a$, $a @ c = a$, $b @ c = b$

Left Side: $\mathbf{(a @ b)} @ c = \mathbf{a @ c} = a$

Right Side: $a @ \mathbf{(b @ c)} = \mathbf{a @ b} = a$

Hence $(a @ b) @ c = a = a @ (b @ c)$

Therefore the equality holds for the first case.

Note: A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.

Without Loss of Generality

Example: Show that if x and y are integers and both $x \cdot y$ *and* $x+y$ are even, then both x and y are even.

Proof: Use a proof by **contraposition**. Suppose x and y are not both even. Then, one or both are odd. Without loss of generality, assume that x is odd. Then $x = 2m + 1$ for some integer m.

Case 1: y is even. Then $y = 2n$ for some integer n, so $x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.

Case 2: y is odd. Then $y = 2n + 1$ for some integer n, so $x \cdot y = (2m + 1)(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd.

◀

✓We only **cover** the case where ***x* is odd** because the case where y is odd is similar.
✓The use phrase **without loss of generality (WLOG)** indicates this.

Common Errors With Exhaustive Proof And Proof By Cases

- What is wrong with this "proof?"
  - "Theorem:" If x is a real number, then x2 is a positive real number.
  - "Proof:" Let
    - p_1: "x is positive,"
    - p_2:"x is negative," and
    - q:"x^2 is positive."
  - To show that $p_1 \rightarrow q$ is true,
    - note that when x is positive, x^2 is positive because it is the productof two positive numbers, x and x.
  - To show that $p_2 \rightarrow q$,
    - note that when x is negative, x^2 is positive because it is the product of two negative numbers, x and x.
  - **This completes the proof.**

Solution: The problem with this "proof" is that we missed the case of x = 0. When x = 0, $x^2 = 0$ is not **positive**, so the supposed theorem is false.

Existence Proofs

- Proof of theorems of the form $\exists_x P(x)$.
- **Constructive** existence proof:
  - Find an explicit value of *a*, for which *P(a)* is true.
  - Then $\exists_x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

◀

Nonconstructive Existence Proofs

- We do not find an element a such that P(a) is true, .

Example: Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$.

On the other hand if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\,\sqrt{2})} = \sqrt{2}^{2} = 2$.

This proof is an example of a nonconstructive existence proof because we have not found irrational numbers x and y such that xy is rational. Rather, we have shown that either the pair $x = \sqrt{2}$, $y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, **but we do not know which of these two pairs works!**

Uniqueness Proofs

- Some theorems asset the existence of a unique element with a particular property, $\exists! x\, P(x)$. The two parts of a *uniqueness proof* are
  - *Existence*: We show that an element x with the property exists.
  - *Uniqueness*: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- Uniqueness: Suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$.

Proof Strategies

- Choose a method.
  1. First try a direct method of proof.
  2. If this does not work, try an indirect method (e.g., try to prove the contrapositive).
- For whichever method you are trying, choose a strategy.
  1. First try *forward reasoning.* Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q, or start with $\neg q$ and prove $\neg p$.
  2. If this doesn't work, try *backward reasoning*. When trying to prove q, find a statement p that we can prove with the property $p \rightarrow q$.

Backward Reasoning

Example: Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Proof: Let *n* be the last step of the game.

Step n: $Player_1$ can win if the pile contains 1,2, or 3 stones.

Step n-1: $Player_2$ will have to leave such a pile if the pile that he/she is faced with has 4 stones.

Step n-2: $Player_1$ can leave 4 stones when there are 5,6, or 7 stones left at the beginning of his/her turn.

Step n-3: $Player_2$ must leave such a pile, if there are 8 stones .

Step n-4: $Player_1$ has to have a pile with 9,10, or 11 stones to ensure that there are 8 left.

Step n-5: $Player_2$ needs to be faced with 12 stones to be forced to leave 9,10, or 11.

Step n-6: $Player_1$ can leave 12 stones by removing 3 stones.

Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.

Looking for Counterexamples

- Recall $\exists_x \neg P(x) \equiv \neg \forall_x P(x)$. .
- To establish that $\neg \forall_x P(x)$ is true (or $\forall_x P(x)$ is false) find a c such that $\neg P(c)$ is true or $P(c)$ is false.
- In this case c is called a counterexample to the assertion $\forall_x P(x)$.

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

Universally Quantified Assertions

- To prove theorems of the form $\forall_x P(x)$, assume x is an arbitrary member of the domain and show that $P(x)$ must be true. Using UG it follows that $\forall_x P(x)$.

Example: An integer x is even if and only if x^2 is even.

Solution: The quantified assertion is

$\forall x\,[x \text{ is even} \leftrightarrow x^2 \text{ is even}]$

We assume x is arbitrary.

Recall that $p \leftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

So, we have two cases to consider. These are considered in turn.

Universally Quantified Assertions

Case 1.

We show that if x is even then x^2 *is* even using a direct proof (the *only if* part or *necessity*).

$x = 2k$ for some integer k.

Hence $x^2 = 4k^2 = 2(2k^2)$ which is even since it is an integer divisible by 2.

This completes the proof of case 1.

Case 2.

We show that if x^2 is even then x must be even (the *if* part or *sufficiency*). We use a proof by contraposition.

Assume x is not even and then show that x^2 is not even. If x is not even then it must be odd. So, $x = 2k + 1$ for some k.

Then $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ which is odd and hence not even.

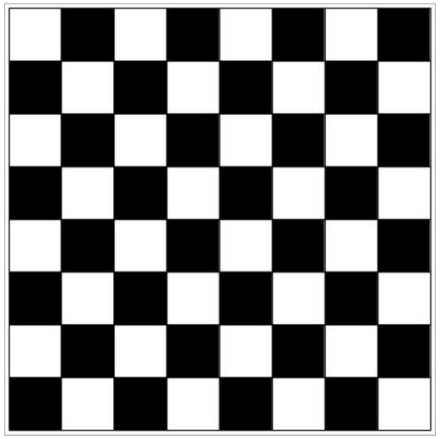
This completes the proof of case 2.

Since x was arbitrary, the result follows by UG. Therefore we have shown that x is even if and only if x^2 is even.

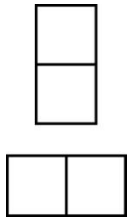
Proof and Disproof: Tilings

Example 1: Can we tile the standard checkerboard using dominos?

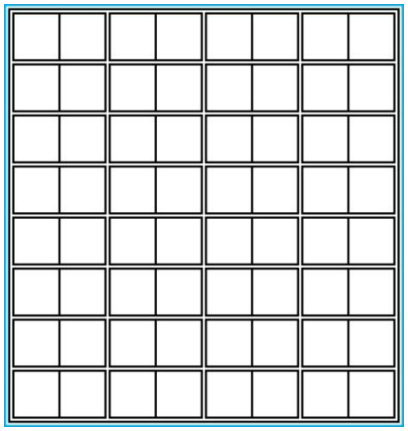
Solution: Yes! One example provides a constructive existence proof.



The Standard Checkerboard



Two Dominoes



One Possible Solution

Tilings

Example 2: Can we tile a checkerboard obtained by removing one of the four corner squares of a standard checkerboard?

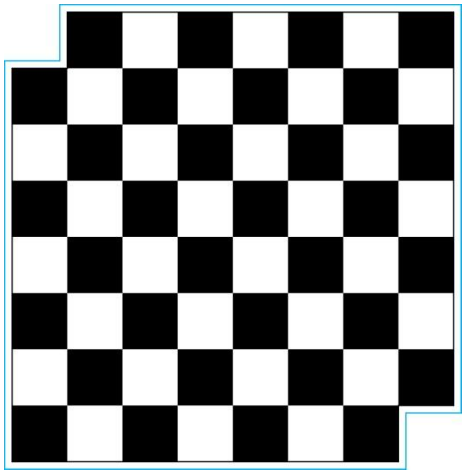
Solution:

- Our checkerboard has $64 - 1 = 63$ squares.
- Since each domino has two squares, a board with a tiling must have an even number of squares.
- The number 63 is not even.
- We have a contradiction.

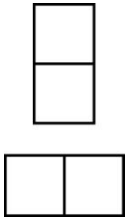
◀

Tilings

Example 3: Can we tile a board obtained by removing both the upper left and the lower right squares of a standard checkerboard?



Nonstandard Checkerboard



Dominoes

Tilings

Solution:

- There are 62 squares in this board.
- To tile it we need 31 dominos.
- ***Key fact***: Each domino covers one black and one white square.
- Therefore the tiling covers 31 black squares and 31 white squares.
- Our board has either 30 black squares and 32 white squares or 32 black squares and 30 white squares.
- Contradiction!

The Role of Open Problems

- Unsolved problems have motivated much work in mathematics. Fermat's Last Theorem was conjectured more than 300 years ago. **It has only recently been finally solved**.
- **Fermat's Last Theorem**: The equation $x^n + y^n = z^n$ has no solutions in integers x, y, and z, with $xyz \neq 0$ whenever n is an integer with $n > 2$.

A proof was found by Andrew Wiles in the 1990s.

An Open Problem

- **The $3x + 1$ Conjecture**: Let T be the transformation that sends an even integer x to $x/2$ and an odd integer x to $3x + 1$. For all positive integers x, when we repeatedly apply the transformation T, we will eventually reach the integer 1.
- For example, starting with $x = 13$:
  - $T(13) = 3 \cdot 13 + 1 = 40$, $T(40) = 40/2 = 20$,
  - $T(20) = 20/2 = 10$, $T(10) = 10/2 = 5$,
  - $T(5) = 3 \cdot 5 + 1 = 16$, $T(16) = 16/2 = 8$,
  - $T(8) = 8/2 = 4$, $T(4) = 4/2 = 2$, $T(2) = 2/2 = 1$

The conjecture has been verified using computers up to $5.6 \cdot 10^{13}$.

Query???

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

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

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

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

$$\forall_x(\Re\mid x)=?$$

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

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

$$1-1+1-1+1.....=?$$

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