TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

# Discrete Mathematics

**Nguyễn Khánh Phương**

**Department of Computer Science**
**School of Information and Communication Technology**
**E-mail: phuongnk@soict.hust.edu.vn**

# PART 1
# COMBINATORIAL THEORY
(Lý thuyết tổ hợp)

# PART 2
# GRAPH THEORY
(Lý thuyết đồ thị)

# Contents of Part 1

# Contents of Part 1: Combinatorial Theory

**Chapter 1. Counting problem**

- This is the problem aiming to answer the question: "How many ways are there that satisfy given conditions?" The counting method is usually based on some basic principles and some results to count simple configurations.
- Counting problems are effectively applied to evaluation tasks such as calculating the probability of an event, calculating the complexity of an algorithm

**Chapter 2. Existence problem**

In the counting problem, configuration existence is obvious; in the existence problem, we need to answer the question: "Is there a combinatorial configuration that satisfies given properties ?"

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

# Chapter 2

# EXISTENCE ROBLEM

NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

# Content

1. **Introduction to existence problems**
2. Basic proof methods
3. Dirichlet principle (pigeonhole principle)

# 1. Introduction to existence problems

- In the "Counting problem" chapter, we focused on counting the combinatorial configurations. In those problems, the existence of the configurations is obvious, and the main object is to count the number of elements that satisfy the given properties.
- However, in many combinatorial problems, it is very difficult to point out the existence of a configuration that satisfies given properties:
  - For example, when a player needs to calculate his moves to answer whether there is a possibility of winning or not?
  - A person needs to search for the key to decipher a secret code that he does not know if this is really the opponent's encrypted message, or just the secret code issued by the opponent to ensure the safety of real telegrams ...
- In combinatorics, besides the counting problem, there is another very important problem is considering the existence of combinatorial configurations satisfying given properties - the problem of existence.

NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

# The 36 officers problem

- This problem is proposed by Euler, it is described as following:

*“You're in command of an army that consists of six regiments, each containing six officers of six different ranks. Can you arrange the officers in a 6x6 square so that each row and each column of the square holds only one officer from each regiment and only one officer from each rank?*

# The 36 officers problem

- Using:
  - A, B, C, D, E, F refer to 6 regiments, respectively
  - 1, 2, 3, 4, 5, 6 refer to 6 ranks of officers, respectively.
- This problem could be generalized by replacing 6 by *n*.
- In the case $n = 4$, a solution to the problem is:

| | | | |
|---|---|---|---|
| A1 | B2 | C3 | D4 |
| B4 | A3 | D2 | C1 |
| C2 | D1 | A4 | B3 |
| D3 | C4 | B1 | A2 |

- In the case $n = 5$, a solution to the problem is:

| | | | | |
|---|---|---|---|---|
| A1 | B2 | C3 | D4 | E5 |
| C4 | D5 | E1 | A2 | B3 |
| E2 | A3 | B4 | C5 | D1 |
| B5 | C1 | D2 | E3 | A4 |
| D3 | E4 | A5 | B1 | C2 |

NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

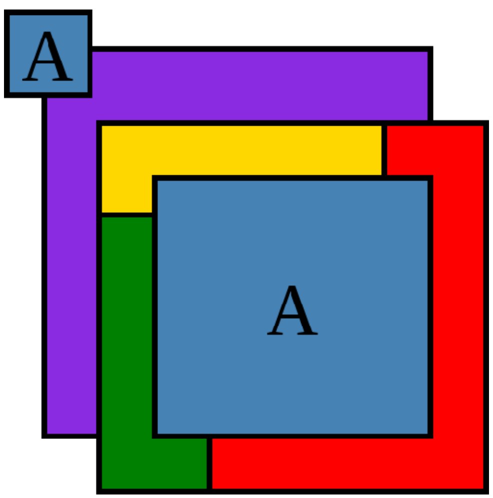
# The 36 officers problem

- As the solution to the problem can be represented by combining two same size squares array of symbols: one with upper-case letter and the other with numbers. The problem is also called as Graeco-Latin square (also called an Euler square)
- Euler struggled to find the solution to the 36 officers problem but was unsuccessful. However, the solution exists when $n$ =4, 5 and 7. Thus, he proposed a general hypothesis: The Graeco-Latin squares are impossible if $n = 4k + 2$.
- Tarri, in 1901, proves the correct hypothesis for $n = 6$, by examining all possible ratings.
- In 1960, three American mathematicians, Boce, Parker, and Srikanda showed a solution with $n = 10$ and then showed a method to construct Graeco-Latin squares for all $n = 4k + 2$, with $k > 1$.

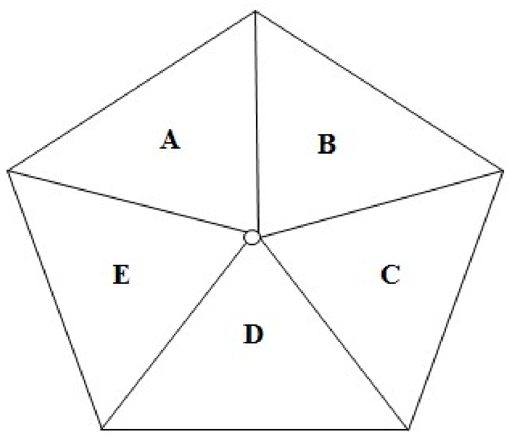
NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

# Four color theorem (Bài toán 4 màu)

- There are problems that its content could be explained to anyone, but its solutions anyone can try to find, but it is difficult to find. The 4-color problem is such a problem.
- The problem can be stated visually as follows: Prove that all maps on the plane could be colored with 4 colors so that no two adjacent regions (neighbor regions) are colored by the same color.
- Note that each country is considered a connected region and the two countries are called neighbors if they share a border of a continuous line.



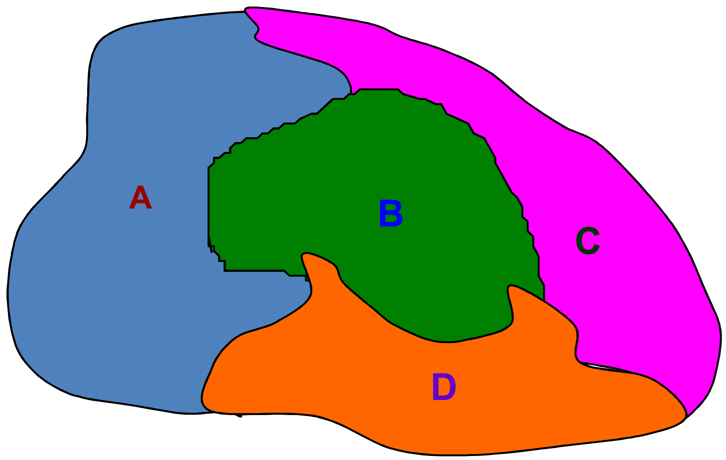

A is not connected region




A and C are not neighbors

# Four color theorem (Bài toán 4 màu)

- The number 4 is not random. It has been shown that all maps are colored with color numbers greater than 4, but with color numbers less than 4 it cannot be colored. For example, the map with 4 countries in the picture below cannot be colored if using less than 4 colors.



# Four color theorem (Bài toán 4 màu)

- This problem was first proposed in 1852 by Francis Guthrie, while trying to color the map of counties of England.
- In 110 years many proofs have been published but have been flawed.
- In 1976, Appel and Haken gave the proof by computer:

K. Appel and W. Hankin, "Every planar map is 4-colorable," Bulletin of the AMS, Volume 82 (1976), 711-712.

# Content

1. Introduction to existence problems
2. **Basic proof methods**
3. Dirichlet principle (pigeonhole principle)

# 2. Basic proof methods

**2.1. Direct Proof (Chứng minh trực tiếp)**

2.2. Proof by Contradiction (Chứng minh bằng phản chứng)

2.3. Proof by Contrapositive (Chứng minh bằng phản đề)

2.4. Proof by Mathematical Induction (Chứng minh bằng qui nạp toán học)

## 2.1. Direct proofs (Chứng minh trực tiếp)

We begin with an example demonstrating the transitivity of divisibility.

**Theorem. If a divides b and b divides c then a divides c.**

**Prove.** By using the definition of the divisibility, there exist integers $k_1$ and $k_2$ such that

$$a = b\,k_1 \text{ and } b = c\,k_2.$$

Then

$$a = b\,k_2 = c\,k_1\,k_2.$$

Let $k = k_1\,k_2$. We have $k$ as an integer, and a = c$k$, so by the definition of divisibility, a divides c.

NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

## 2.1. Direct proofs (Chứng minh trực tiếp)

# If P, Then Q

- In most theorems, exercises or tests, you need to prove the form "If P, Then Q".
- In this example: "if a divides b and b divides c, then a divides c"
  - "P" is "If a divides b and b divides c" and "Q" is "a divides c".
- This is the standard state of many theorems.
- The direct proof can be conceived as a series of inferences beginning with "P" and ending with "Q":

$$P \Rightarrow \ldots \Rightarrow Q$$

Most of proof is direct. When you have to prove, try starting with direct proof, unless you have a good reason not to.

# Example 1

Theorem: The sum of two odd integers is an even integer;

Proof:

- Let $a$ and $b$ be odd integers.
- Then $a = 2s + 1$ and $b = 2t + 1$ for some integers $s$ and $t$.
- Then $a + b = (2s + 1) + (2t + 1)$

  $= 2(s + t + 1)$.
- Therefore, $a + b$ is an even integer.
- Finish the proof.

# Example 2

- A rational number is a number that equals the quotient of two integers.
- Let $\mathbb{Q}$ denote the set of rational numbers.

Theorem: The sum of two rational numbers is rational.

- Proof:
  - Let $r$ and $s$ be rational numbers.
  - Let $r = a/b$ and $s = c/d$, where $a$, $b$, $c$, $d$ are integers, where $b$, $d > 0$
  - Then $r + s = (ad + bc)/bd$.
    - We know that $ad + bc$ is an integer.
    - We know that $bd$ is an integer.
    - We also know that $bd \neq 0$.
    - Therefore, $r + s$ is a rational number.

# Example 3

- A rational number is a number that equals the quotient of two integers.
- Let $\mathbb{Q}$ denote the set of rational numbers.

Theorem: Between every two distinct rationals, there is a rational.

- Proof:
  - Let $r, s \in \mathbb{Q}$.
  - Without loss of generality, we may assume $r < s$.
  - Let $t = (r + s)/2$.
  - Then $t \in \mathbb{Q}$. (proof?)
  - We must show that $r < t < s$:
    - Since $r < s$, it follows that

$$2r < r + s < 2\mathrm{s}$$

    - Then divide by 2 to get

$$r < (r + s)/2 < \mathrm{s}$$

    - Therefore, $r < t < s$.

# Example 4

- Prove that if $n$ is an integer and $n^3+5$ is odd, then $n$ is even

Proof:

- $n^3+5 = 2k+1$ for some integer $k$ (definition of odd numbers)
- $n^3 = 2k-4$
- $n = \sqrt[3]{2k-4}$

Umm, so direct proof didn't work out.

# 2. Basic proof methods

2.1. Direct Proof (Chứng minh trực tiếp)

**2.2. Proof by Contradiction (Chứng minh bằng phản chứng)**

2.3. Proof by Contrapositive (Chứng minh bằng phản đề)

2.4. Proof by Mathematical Induction (Chứng minh bằng qui nạp toán học)

# 2.2. Proof by Contradiction

Requirement: Proof the statement P

**Proof by contradiction:**

- Assume it is false (Assume ¬P)
- Prove that ¬P cannot occur
  - (it means a contradiction exists: not satisfying the properties given in the problem or come to the absurd such as 1 = 0)

Requirement: Proof "If P, Then Q",

**Proof by contradiction:**

- Assume it is false (Assume that "P and Not Q" are true).
- It thus means a contradiction exists.

# Example 4

- Prove that if $n$ is an integer and $n^3+5$ is odd, then $n$ is even

Proof:

  - $n^3+5 = 2k+1$ for some integer $k$ (definition of odd numbers)
  - $n^3 = 2k-4$
  - $n = \sqrt[3]{2k-4}$

Umm, so direct proof didn't work out.

Requirement: Proof "If P, Then Q",

**Proof by contradiction:**

- Assume it is false (Assume that "P and Not Q" are true).
- It thus means a contradiction exists.

Rephrased: If $n^3+5$ is odd, then $n$ is even

**Proof by contradiction:**

Assume that $n^3+5$ is odd, and $n$ is odd

- $n$ is odd $\rightarrow n=2k+1$ for some integer $k$ (definition of odd numbers)
- $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$ is odd ?!!??
  - As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it must be even
  - Contradiction!

# 2.2. Proof by Contradiction

Example 5. Given 7 segments with length greater than 10 and less than 100. Prove that one can always find 3 segments that can be assembled into a triangle.

Solution:

Note that, the necessary and sufficient condition for 3 segments to be assembled into a triangle is: the sum of the lengths of two smaller segments must be greater than the length of the largest segment.

Ordering the given 7 segments in ascending order of length, we have:

$$10 < a_1 \leq a_2 \leq \ldots \leq a_7 < 100.$$

We need to prove that: from the above ordered sequence, one always can find 3 consecutive segments such that the sum of length of the first 2 segments is greater than that of the last.

Requirement: Proof "If P, Then Q",

**Proof by contradiction:**

- Assume it is false (Assume that "P and Not Q" are true).
- It thus means a contradiction exists.

Proof by contradiction:

Assume this does not happen (not Q: could not find any 3 consecutive segments such that the sum of length of the first 2 segments is greater than that of the last).

# 2.2. Proof by Contradiction

- Proof by contradiction: Assume this does not happen (could not find any 3 consecutive segments such that the sum of length of the first 2 segments is greater than that of the last). Thus, we have equalities:

$$a_1 + a_2 \le a_3,$$
$$a_2 + a_3 \le a_4,$$
$$a_3 + a_4 \le a_5,$$
$$a_4 + a_5 \le a_6,$$
$$a_5 + a_6 \le a_7.$$

- As $a_1$, $a_2$ are greater than 10, we have $a_3 > 20$. As $a_2 > 10$ and $a_3 > 20$, we have $a_4 > 30$, ..., continuing we have $a_5 > 50$, $a_6 > 80$ and $a_7 > 130$.
- The last equalities $a_7 > 130$ is contradiction with the given condition of the problem: all segments has the length less than 100. Thus, the assumption is false.

# 2.2. Proof by Contradiction

**Example 6.** The vertices of a **decagon** (a ten-sided polygon or 10-gon) decimal are arbitrarily numbered by the integers 0, 1, ..., 9. Prove that you can always find three consecutive vertices whose sum of the numbers is greater than 13.

Solution: Let $x_1, x_2, \ldots, x_{10}$ be the numbers assigned to the vertices of 1, 2, ..., 10 of the decagon.

Requirement: Proof "If P, Then Q",

**Proof by contradiction:**

- Assume it is false (Assume that "P and Not Q" are true).
- It thus means a contradiction exists.

Proof by contradiction:

Assume this does not happen (not Q: could not find any three consecutive vertices to satisfy the assertion of the example). Then we have:

$$
\begin{array}{rl}
 & x_1 + x_2 + x_3 \leq 13, \\
 & x_2 + x_3 + x_4 \leq 13, \\
+ & \quad . \;\; . \;\; . \;\; . \;\; . \\
 & x_9 + x_{10} + x_1 \leq 13, \\
 & x_{10} + x_1 + x_2 \leq 13, \\
\hline
 & 3(x_1 + x_2 + \ldots + x_{10}) \leq 130
\end{array}
$$

Summing side by side of all inequalities

# 2.2. Proof by Contradiction

- Summing side by side of all above inequalities, we have

$$3(x_1 + x_2 + \dots + x_{10}) \le 130.$$

- On the other hand, as

$$3(x_1 + x_2 + \dots + x_{10})$$
$$= 3\,(0 + 1 + 2 + \dots + 9)$$
$$= 135,$$

- Therefore:

$$135 = 3(x_1 + x_2 + \dots + x_{10}) \le 130$$

The obtained contradiction proved the claim in the example to be correct. .

# 2.2. Proof by Contradiction

**Example 7. Proof that it is not possible to connect 31 computers into a network such that each computer is connected to exactly 5 other computers.**

Requirement: Proof "If P, Then Q",

**Proof by contradiction:**

- Assume it is false (Assume that "P and Not Q" are true).
- It thus means a contradiction exists.

**Solution:**

Suppose the opposite is finding a way to connect 31 computers so that each computer is connected to exactly 5 other computers. Then the number of connected channels is

$$5 \times 31 / 2 = 75.5 \text{ ?! (not an integer)}$$

The obtained absurdity proves the claim in the example to be true.

# 2. Basic proof methods

2.1. Direct Proof (Chứng minh trực tiếp)

2.2. Proof by Contradiction (Chứng minh bằng phản chứng)

**2.3. Proof by Contrapositive (Chứng minh bằng phản đề)**

2.4. Proof by Mathematical Induction (Chứng minh bằng qui nạp toán học)

# 2.3. Proof by Contrapositive (Chứng minh bằng phản đề)

Proof by contrapositive uses the logically equivalence of two statement "If P then Q" ($P \Rightarrow Q$) and "If not Q then not P ($\neg Q \Rightarrow \neg P$):

$$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$$

Example:

The statement "If this is my car, then its color is red"

is equivalent to

"If its color is not red, then it is not my car".

- Thus, to prove "If P, then Q" by using contrapositive proof, we prove "If not Q then not P").

# Example $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

**Example 1.** If $x$ and $y$ are two integer such that $x+y$ is even, then $x$ and $y$ are either both even or odd.

**Proof.** The contrapositive is

"If $x$ and $y$ are neither both even nor odd, then its sum is odd."

- As $x$ and $y$ are neither both even nor odd. Without loss of generality, we may assume $x$ is even and $y$ is odd. Then we could find integers $k$ and $m$ such that $x = 2k$ and $y = 2m+1$. Now we calculate $x+y = 2k + 2m + 1 = 2(k+m) + 1$, thus $x+y$ is odd.
- Therefore, we have proven the result by contraposition

# Example $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

**Example 2.** If $n$ is a positive integer such that $n$ mod 4 is equal to either 2 or 3, then $n$ is not a perfect square.

**Proof.** The contrapositive is:

"If $n$ is a perfect square then $n$ mod 4 is equal to either 0 or 1"

- Assume $n = k^2$. There are 4 cases:
  - If $k$ mod 4 = 0, then $k = 4q$, where $q$ is positive integer. Thus, $n = k^2 = 16\,q^2 = 4(4\,q^2)$ , so $n$ mod 4 = 0.
  - If $k$ mod 4 = 1, then $k = 4q + 1$, where $q$ is positive integer. Thus, $n = k^2 = 16\,q^2 + 8\,q + 1 = 4(4\,q^2 + 2\,q) + 1$, so $n$ mod 4 = 1.
  - If $k$ mod 4 = 2, then $k = 4q + 2$, where $q$ is positive integer. Thus, $n = k^2 = 16\,q^2 + 16\,q + 4 = 4(4\,q^2 + 4\,q + 1)$, so $n$ mod 4 = 0.
  - If k mod 4 = 3, thì $k = 4q + 3$, where $q$ is positive integer. Thus, $n = k^2 = 16\,q^2 + 24\,q + 9 = 4(4\,q^2 + 6\,q + 2) + 1$, so $n$ mod 4 = 1.

## 2.3. Proof by Contrapositive (Chứng minh bằng phản đề)

The difference between Contrapositive proof and Contradiction proof ?

We are asked to prove a conditional statement, or a statement of the form "If P, Then Q”:

- Contradiction proof (Chứng minh bằng phản chứng): Assume “If P and Not Q is true”, then need to show some sort of fallacy → thus the assumption is false.
- Contrapositive proof (Chứng minh bằng phản đề): We do not prove “If P, then Q” directly, instead, we prove “If not Q, then not P”.

The advantage of contrapositive proof is that your goal is clear: prove not P; while in contradiction proof, your goal is to prove a contradiction (you need to arrive at some sort of fallacy), but it is not always clear what the contradiction is going to be at the start.

# 2. Basic proof methods

2.1. Direct Proof (Chứng minh trực tiếp)

2.2. Proof by Contradiction (Chứng minh bằng phản chứng)

2.3. Proof by Contrapositive (Chứng minh bằng phản đề)

**2.4. Proof by Mathematical Induction (Chứng minh bằng qui nạp toán học)**

# 2.4. Proof by Mathematical Induction

- This is a very useful proof technique when we have to prove that the proposition $P(n)$ is true for all natural numbers $n \geq n_0$.
- Similar to the "domino effect" principle.

**Outline of proof by Induction:**

- Basic step: Prove the first statement $P(n_0)$ is true
- Inductive step: Given any integer $n \geq n_0$ , prove that $P(n) \rightarrow P(n+1)$ (Assuming $P(n)$ is true and showing it forces $P(n+1)$ is true)

---

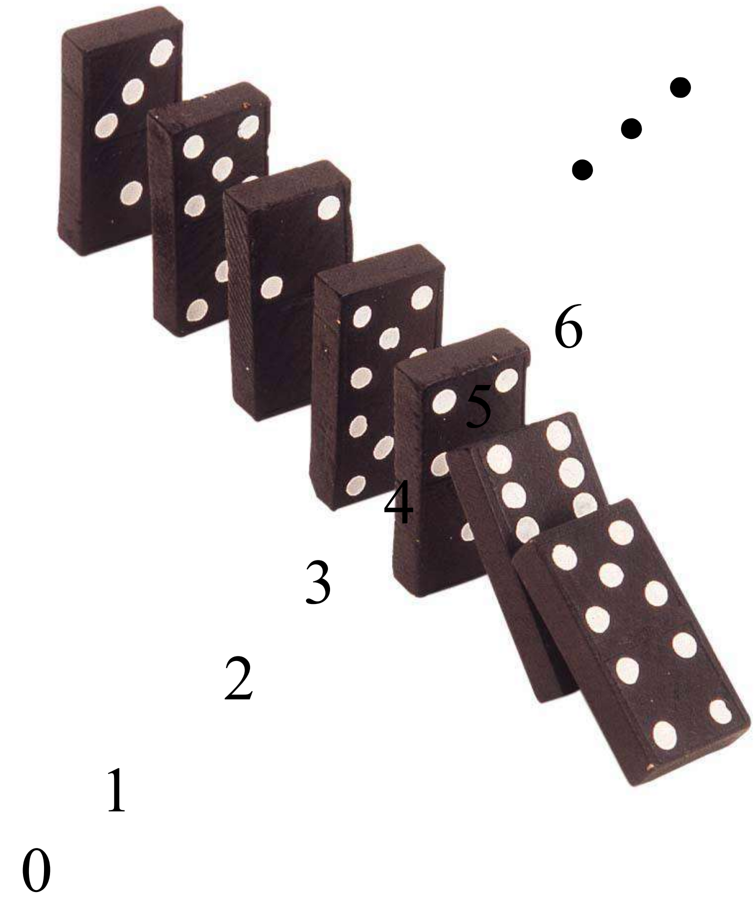
- Conclusion: $P(n)$ is true $\forall n \geq n_0$

(The assumption that $P(n)$ is true is called the inductive hypothesis)

# The "Domino Effect"

- **Step #1:** Domino #0 falls.
- **Step #2:** For all $n \in \mathbf{N}$,
  if domino #$n$ falls, then domino #$n$+1 also falls.
- **Conclusion:** All dominos must fall!

**Note:** This happens even when there are infinitely many dominoes!



# Outline of proof by Induction:

We need to prove $P(n)$ is true $\forall n \geq n_0$ .

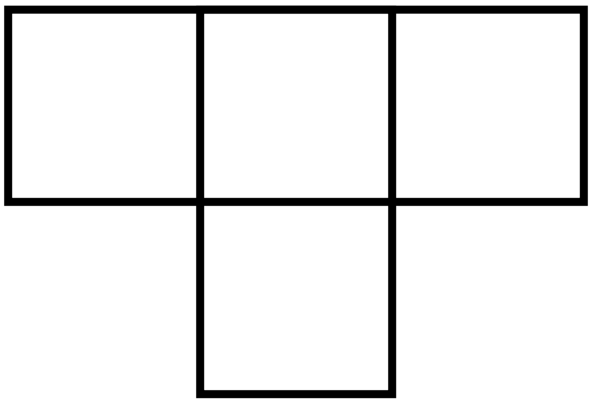
- Basic step (Bước cơ sở): Prove $P(n_0)$ is true.
- Inductive hypothesis (Giả thiết qui nạp): Assume $P(n)$ is true
- Inductive step (Bước chuyển qui nạp): Prove $P(n+1)$ is true.
- Conclusion: It follows by mathematical induction that $P(n)$ is true $\forall n \geq n_0$

*"The First Principle of Mathematical Induction"*

*"Nguyên lý qui nạp toán học thứ nhất"*

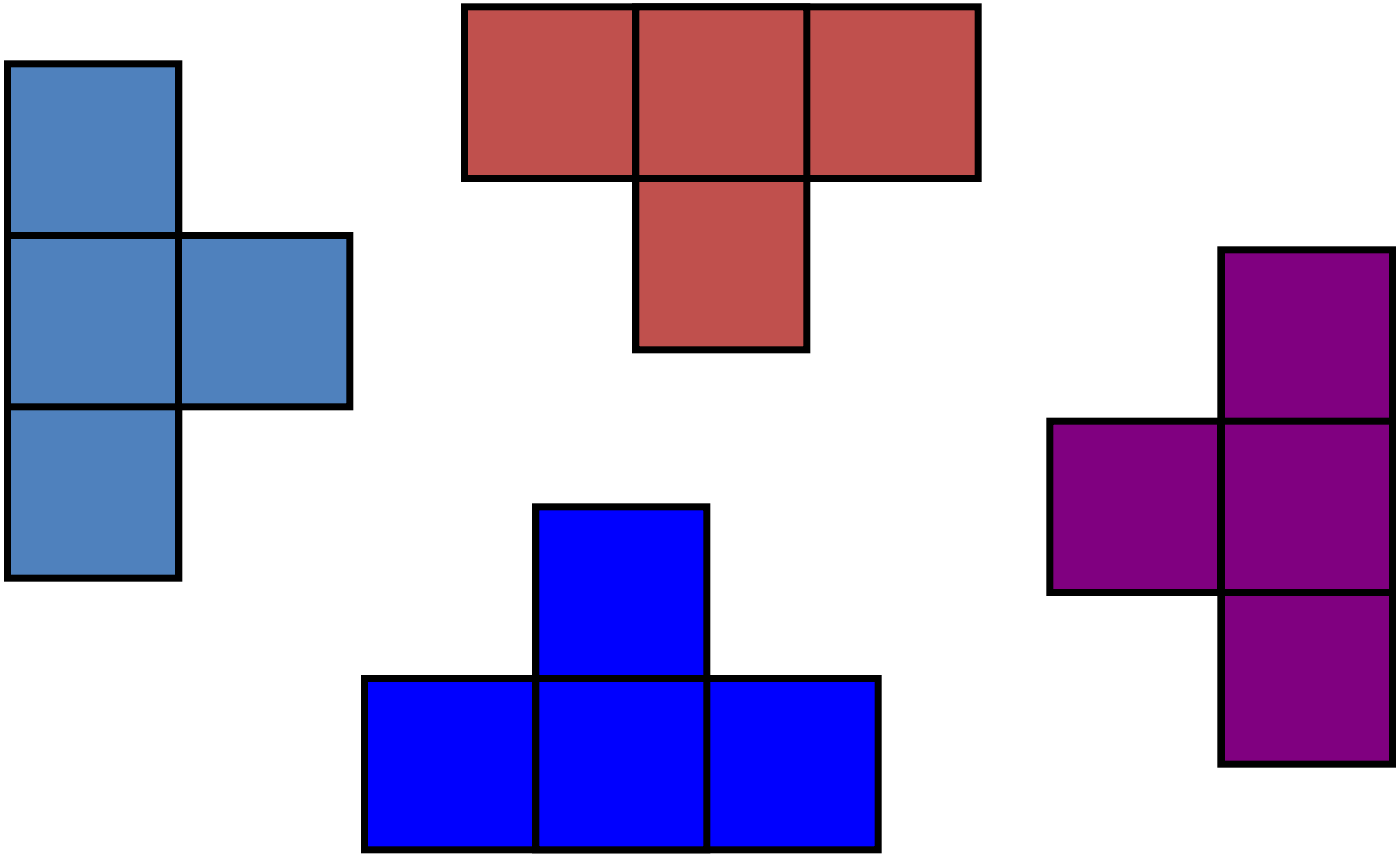
# Example 1

Prove that it is always possible to cover a chessboard of size $2^n \times 2^n$ $(n > 1)$ with T-omino cards.

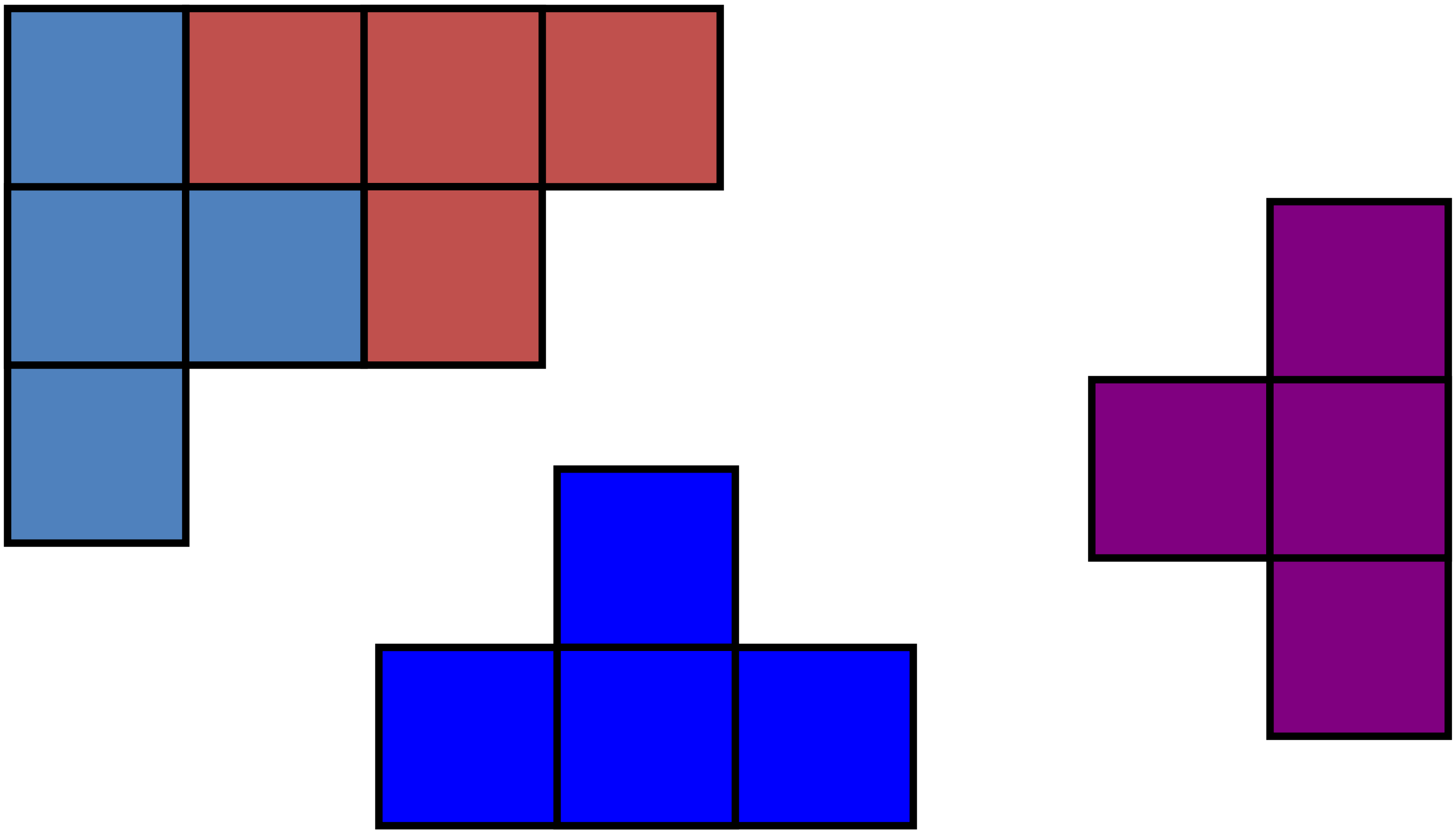


- Basic step: Prove that it is true when $n = 2$

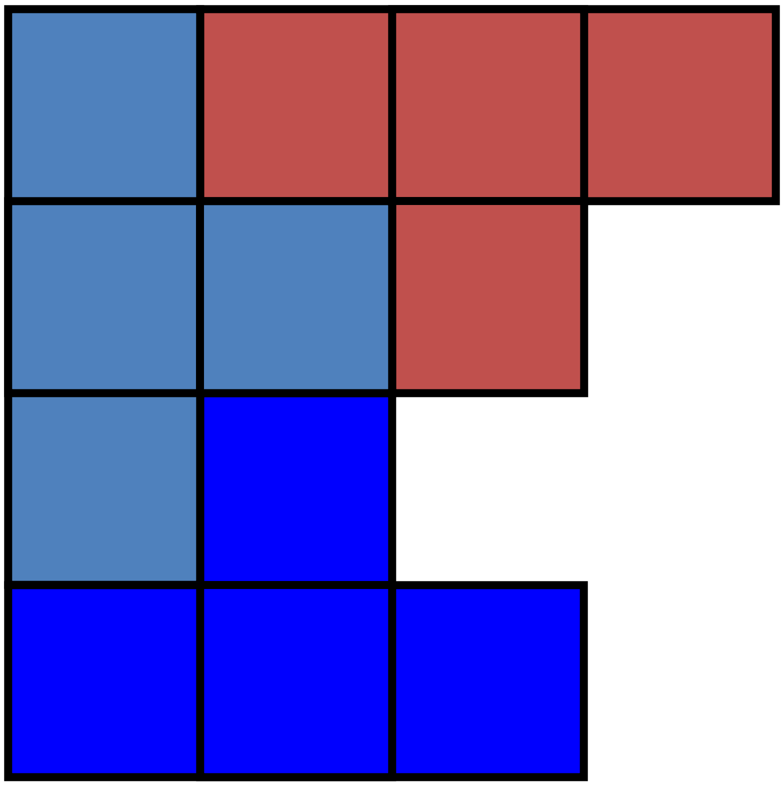
# Basic step: Chessboard $2^2$ x $2^2$

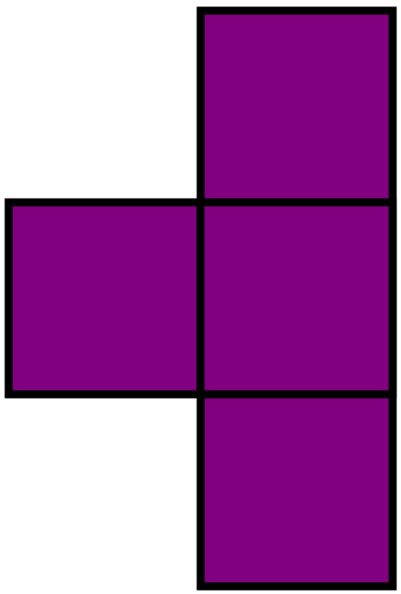


# Basic step: Chessboard $2^2 \times 2^2$

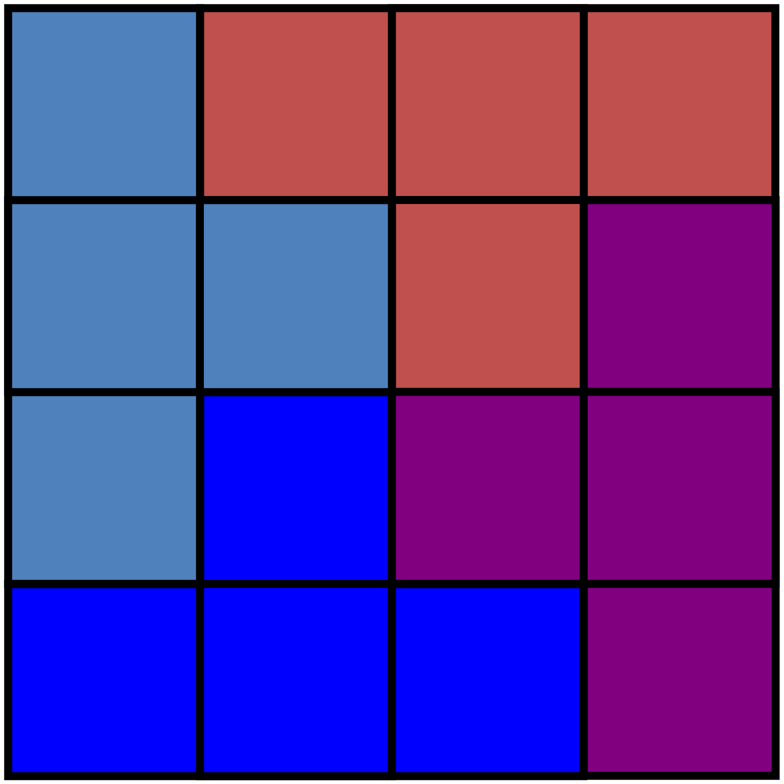


# Basic step: Chessboard $2^2$ x $2^2$





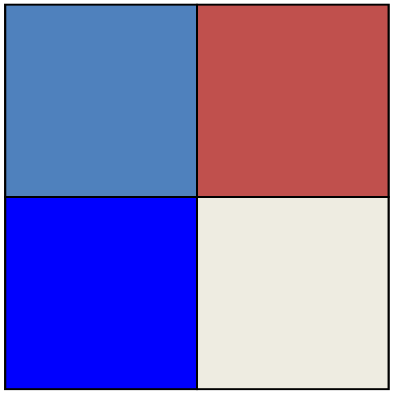
# Basic step: Chessboard $2^2$ x $2^2$



# Inductive step

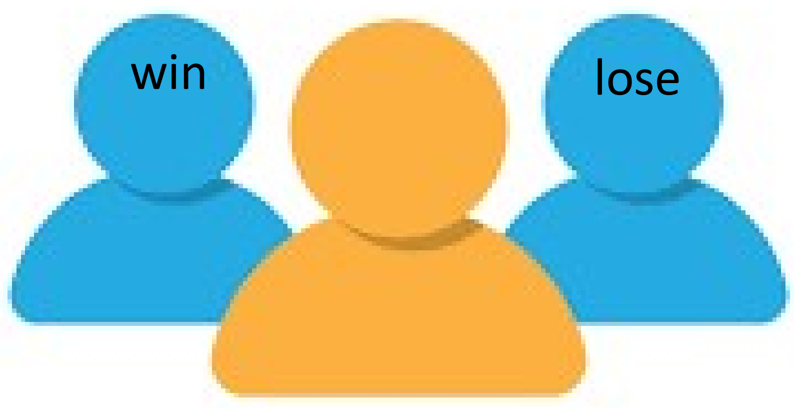
Assume we can cover chessboard of size $2^n \times 2^n$. We need to prove also can cover chessboard of size $2^{n+1} \times 2^{n+1}$.

Actually, divide the chessboard of size $2^{n+1} \times 2^{n+1}$ into 4 parts, each of size $2^n \times 2^n$. According to the inductive hypothesis (giả thiết qui nạp), each of these parts could be covered by T-ominos. Putting them on the chessboard of size $2^{n+1} \times 2^{n+1}$, we then get the answer for the problem.



# Example 2

- At the end of a volleyball championship consisting of $n$ participating teams, in which teams take a round trip, the captains of teams are invited to stand in a row to take pictures.
- P($n$): It is always possible to place $n$ captains in a row so that except for two captains standing at the leftmost and rightmost, each of them is always next to the captain of the team that won his team and the captain of the team that lost his team in the tournament.

# Example 2

**Proof.** We prove by induction

- Basic step: P(1) is always true.
- Assume P($n$-1) is true, we need to prove P($n$) is true.
  - First, we rank $n$-1 captains of teams 1, 2,..., $n$-1. According to the inductive hypothesis, it is possible to arrange them in the row that satisfies the given condition of the problem. Without loss of generality, we may assume this row is:

$$1 \rightarrow 2 \rightarrow \ldots \rightarrow n\text{-}1$$

(1 wins 2, 2 wins 3, … $n$-2 wins $n$-1)

# Example 2

– Now we find the position to place the captain of the $n^{th}$ team. There are 3 cases:

- If team $n$ won team 1, then the row is:

  $$n \to 1 \to 2 \to \ldots \to n\text{-}1.$$

- If team $n$ lost team $n$-1, then the row is:

  $$1 \to 2 \to \ldots \to n\text{-}1 \to n\ .$$

- If team $n$ lost team 1 and won team $n$-1:
  - Let $k$ be the smallest index such that team $n$ won team $k$.
  - Obviously, such $k$ exists.
  - The row obtained from the row of $n$-1 teams is by inserting the captain of the $n^{th}$ team between the captains of team $k$-1 and team $k$.

$$1 \to 2 \to \ldots \to n\text{-}1$$

(1 wins 2, 2 wins 3, … $n$-2 wins $n$-1)

# Example 2

$$1 \to 2 \to \ldots \to k\text{-}1 \to k \to k+1 \to \ldots \to n\text{-}1$$

The row: $1 \to \ldots \to k\text{-}1 \to n \to k \to k+1 \to \ldots \to n\text{-}1$

# Second Principle of Induction – Strong Induction

Occasionally it happens in induction proof that it is difficult to show that P($n$) forces P($n$+1) to be true. Instead, you may find that you need to use the fact that some "lower" statements P($k$) (with $k < n$) force P($n$+1) to be true. For these situations, you can use a slight variant of induction called **strong induction**. Strong induction works just like regular induction, except that in Inductive step, instead of assuming P($n$) is true and showing this forces P(n+1) to be true, we assume that all the statements P($n_0$), P($n_0$+1),..,P($n$) are true and show this forces P($n$+1) to be true. The idea is that if it always happens that the first $n$ dominoes falling makes the ($n$ +1)th domino fall, then all the dominoes must fall. Here is the outline:

We need to prove $P(n)$ is true $\forall n \geq n_0$ .

- Basic step (Bước cơ sở): Prove $P(n_0)$ is true or the first several P($n$).
- Inductive hypothesis (Giả thiết qui nạp): Assume any integer $k$:

$$\forall\ n_0 \leq k \leq n \quad P(k) \text{ is true}$$

- Inductive step (Bước chuyển qui nạp): Prove $P(n+1)$ is true.
- Conclusion: It follows by mathematical induction that $P(n)$ is true $\forall n \geq n_0$

# Second Principle of Induction – Strong Induction

## Outline of proof by strong Induction:

- $P(n_0)$
  $\forall n \geq n_0 : \overbrace{(\forall\ n_0 \leq k \leq n \ \ P(k))}^{\text{Assume } P \text{ is true for all previous cases } n_0 \text{ to } n} \rightarrow P(n+1)$
  Conclusion $\forall n \geq n_0 : P(n)$

- The difference with 1st principle of induction:
  - Inductive step use stronger assumption: $P(k)$ is true for all $k \leq n$, not just the case $k=n$ as in the 1st principle of induction.

# Outline of proof by strong Induction

We need to prove $P(n)$ is true $\forall n \geq n_0$.

- **Basic step:** Prove that $P(n_0)$ is true.
- **Inductive hypothesis :** Assume $P(k)$ is true $\forall\ n_0 \leq k \leq n$.
- **Inductive step :** Prove $P(n+1)$ is true.
- **Conclusion:** It follows by mathematical induction that $P(n)$ is true $\forall n \geq n_0$.

# Example 3

**Prove that when natural $n \geq 1$, we have $12 \mid n^4 - n^2$**

We need to prove $P(n)$ is true $\forall n \geq n_0$ .

- Basic step (Bước cơ sở): Prove $P(n_0)$ is true.
- Inductive hypothesis (Giả thiết qui nạp): Assume $P(n)$ is true
- Inductive step (Bước chuyển qui nạp): Prove $P(n+1)$ is true.
- Conclusion: It follows by mathematical induction that $P(n)$ is true $\forall n \geq n_0$

First look at how 1st principle of induction would be problematic:

- Basic step: Need to show $12 \mid n^4 - n^2$ is true for $n = 1$. This part is easy because it reduces to $12|0$, which is clearly true.
- Inductive step: Assume that $12 \mid n^4 - n^2$ and show this implies $12 \mid (n+1)^4 - (n+1)^2$
  - Now $12 \mid n^4 - n^2$ means $n^4 - n^2 = 12a$ for some $a \in \mathbb{Z}$.
  - Thus, we need to use this to try showing that $(n+1)^4 - (n+1)^2 = 12b$ for some $b \in \mathbb{Z}$

$$(n+1)^4 - (n+1)^2 = (n^4+4n^3+6n^2+4n+1)-(n^2+2n+1)$$
$$= (n^4-n^2) + 4n^3+6n^2+6n$$
$$= 12a + 4n^3+6n^2+6n$$

At this point, we are stuck because we can't factor out of 12. Now let's see how strong induction can get us out of this bind.

# Example 3: **Prove that when natural $n \geq 1$, we have $12 \mid n^4 - n^2$**

Strong induction involves assuming each of statements $P(n_0) = S_1$ , $P(n_0+1) = S_2$ ,...,$P(n)= S_n$ , is true, and showing that this forces $P(n+1) = S_{n+1}$ , to be true.

In particular, if $S_1$ through $S_n$ are true, then certainly $S_{n-5}$ is true, provided that $1 \leq n-5 < n$.

The idea is then to show $S_{n-5} \Rightarrow S_{n+1}$ instead of $S_n \Rightarrow S_{n+1}$

For this to make sense, our basic step must involve checking that $S_1, S_2, S_3, S_4, S_5, S_6$ are all true. Once this is established, $S_{n-5} \Rightarrow S_{n+1}$ will imply that the other $S_n$ are all true.

For example, if $n = 6$, then $S_{n-5} \Rightarrow S_{n+1}$ is $S_1 \Rightarrow S_7$, so $S_7$ is true;

for $n = 7$, then $S_{n-5} \Rightarrow S_{n+1}$ is $S_2 \Rightarrow S_8$, so $S_8$ is true, etc.

We need to prove $P(n)$ is true $\forall n \geq n_0$.

- **Basic step:** Prove that $P(n_0)$ is true.
- **Inductive hypothesis :** Assume $P(k)$ is true $\forall\ n_0 \leq k \leq n$.
- **Inductive step :** Prove $P(n+1)$ is true.
- **Conclusion:** It follows by mathematical induction that $P(n)$ is true $\forall n \geq n_0$.

# Example 3: **Prove that when natural $n \geq 1$, we have $12 | n^4 - n^2$**

- Basic step: Need to show $12 | n^4 - n^2$ is true for $n = 1,2,3,4,5,6$
  - If $n = 1$, 12 divides $n^4 - n^2 = 1^4 - 1^2 = 0$.
  - If $n = 2$, 12 divides $n^4 - n^2 = 2^4 - 2^2 = 12$.
  - If $n = 3$, 12 divides $n^4 - n^2 = 3^4 - 3^2 = 72$.
  - If $n = 4$, 12 divides $n^4 - n^2 = 4^4 - 4^2 = 240$.
  - If $n = 5$, 12 divides $n^4 - n^2 = 5^4 - 5^2 = 600$.
  - If $n = 6$, 12 divides $n^4 - n^2 = 6^4 - 6^2 = 1260$.
- Inductive step: Let $n \geq 6$ and assume that $12 | k^4 - k^2$ for $1 \leq k \leq n$ (that is, assume statements P(1), P(2),..,P($n$) are all true), and show this implies $12 | (n+1)^4 - (n+1)^2$ (that is, we must show that P($n$+1) is true)
  - Since P($n$-5) is true, we have $12 | (n-5)^4 - (n-5)^2$ . For simplicity, let's set $m = n-5$, so we know $12 | m^4 - m^2$ means $m^4 - m^2 = 12a$ for some $a \in \mathbb{Z}$.
  - Thus, we need to use this to try showing that $(n+1)^4 - (n+1)^2 = 12b$ for some $b \in \mathbb{Z}$

$$\begin{aligned}
(n+1)^4 - (n+1)^2 &= (m+6)^4 - (m+6)^2 \\
&= (m^4+24m^3+216m^2+865m+1296) - (m^2+12m+36) \\
&= (m^4-m^2) + 24m^3+216m^2+852m + 1260 \\
&= 12a \quad + 24m^3+216m^2+852m + 1260 \\
&= 12(a + 2m^3+18m^2+71m + 105)
\end{aligned}$$

As $(a + 2m^3+18m^2+71m + 105)$ is integer, we get $12 | (n+1)^4 - (n+1)^2$

This shows by strong induction that $12 | n^4 - n^2$ for all natural $\boldsymbol{n \geq 1}$

# Example 4

**For all naturals $n \geq 0$, we have $10 | n^5 - n$**

Proof: using strong induction

- **Basic step:** Prove $P(0)$ is true.

When $n = 0$: we have $0^5$-0=0 và 10|0 → statement is true for $n = 0$

- **Inductive hypothesis:** Assume $P(k)$ is true $\forall\ 0 \leq k \leq n$.

Assume $k \geq 0$, and $10 \mid k^5 - k$ is true for $0 \leq k \leq n$

As $0 \leq n\text{-}1 \leq n$, inductive hypothesis implies that P($n$-1) is true, so

$(n\text{-}1)^5 - (n\text{-}1) = 10c$ for $c \in \mathbb{Z}$

- **Inductive step: Prove $P(n+1)$ is true**

$$10 \mid (n+1)^5 - (n+1)$$

# Example 4

$$(n+1)^5 - (n+1)$$
$$= [(n-1)+2]^5 - [(n-1)+2]$$
$$= (n-1)^5 + 10(n-1)^4+40(n-1)^3+80(n-1)^2+80(n-1)+32$$
$$-(n-1) \qquad\qquad -2$$
$$= \underbrace{\boxed{[(n-1)^5 - (n-1)]}}_{10c} + 10[(n-1)^4 + 4(n-1)^3 +8(n-1)^2+8(n-1)+3]$$
$$= 10\,[\underbrace{c + (n-1)^4 + 4(n-1)^3 +8(n-1)^2+8(n-1)+3}_{\text{integer}}]$$

$\rightarrow$ $10 \mid (n+1)^5 - (n+1)$

# Example 4

**For all naturals $n \geq 0$, we have $10 | n^5 - n$**

Proof: using strong induction

- **Basic step:** Prove $P(0)$ is true.

When $n = 0$: we have $0^5$-0=0 and 10|0 → statement is true for $n = 0$

When $n = 1$: we have $1^5$-1=0 and 10|0 → statement is true for $n = 1$

- **Inductive hypothesis:** Assume $P(k)$ is true $\forall\ 0 \leq k \leq n$.

Asume $k \geq 0$, and $10 \mid k^5 - k$ is true for với $0 \leq k \leq n$

As $\boxed{0 \leq n\text{-}1 \leq n}$, inductive hypothesis implies that P($n$-1) is true, so

$(n\text{-}1)^5 - (n\text{-}1) = 10c$ for $c \in \mathbb{Z}$

- **Inductive step: Prove $P(n+1)$ is true**

$$10 \mid (n+1)^5 - (n+1)$$

# Content

1. Introduction to existence problems
2. Basic proof methods
3. **Dirichlet principle (pigeonhole principle)**

# 3. Dirichlet principle

**3.1. Principle statement**

3.2. Application examples

NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

# 3.1. Dirichlet principle

***If putting more than n objects into n boxes then at least one box has at least 2 objects ( $\geq$ 2 ).***

- 7 objects
- 6 boxes

**Proof.** (Contradiction).

The reverse assumption is that one could not find a box containing $\geq$ **2** objects.

➔ That means that each box contains $\leq$ **1** object.

➔ The total number of objects put in $n$ boxes $\leq$ $\boldsymbol{n}$

Contrary to the given condition of problem that more than $n$ objects are put in them.

# 3.1. Dirichlet principle

The above principle has been successfully applied by the German mathematician Dirichlet to solving many existence problems in combinatorics.

It is also presented in the language of pigeons:

"*If one put more than n pigeons into n pigeonholes, then at least one hole has more than one pigeon* **(≥ 2)**."

So the principle is also known as " **Pigeonhole principle** ".

# Example

***If putting more than n objects into n boxes then at least one box has at least 2 objects* ( ≥ 2 ).**

**Example 1.** Among 13 people, there are always 2 people born in the same month as there are only 12 months.

**Example 2.** In the exam, the test score is assessed by an integer between 0 and 100. Then at least how many students must take the test so that it is certainly to exist 2 students get same result ?

Solution. There are 101 different results

➔ Using Dirichlet principle, the number of students is 102

# Generalized Pigeonhole Principle (Nguyên lý Dirichlet tổng quát)

***Dirichlet principle: If putting more than n objects into n boxes then at least one box has ≥ 2 objects.***

When the number of objects putting into $k$ boxes is much larger than the $k$, it is obviously that the claim in the principle about the existence of a box containing at least two objects is too small. In such a case, we use the following generalized Dirichlet principle:

"If putting $n$ objects into $k$ boxes, one could always find at least one box containing $\geq \lceil n/k \rceil$ objects".

Here the symbol $\lceil \alpha \rceil$ is the least integer greater than or equal to $\alpha$.

e.g.: $\lceil 3.14 \rceil = 4$

NGUYỄN KHÁNH PHƯƠNG
Bộ môn KHMT – ĐHBK HN

# Generalized Pigeonhole Principle

"If putting $n$ objects into $k$ boxes, one could always find at least one box containing $\geq \lceil n/k \rceil$ objects".

Proof by contradiction.

Assume the claim in principle is not true.

➔ Each box contains $\leq \lceil n/k \rceil - 1 < [(n/k)+1] - 1 = n/k$ objects

There are $k$ boxes

➔ There are $< k(n/k) = n$ objects

The obtained contradiction has proved the principle.

# Example

***Dirichlet principle:*** "If putting $n$ objects into $k$ boxes, one could always find at least one box containing $\geq \lceil n/k \rceil$ objects".

**Example 3.** In a group of 100 people, what is the minimum number of people that were born in the same month ?.

**Solution**: Putting people born in the same month into one group. There are 12 months. Therefore, according to the Dirichlet principle, there exists at least one group consisting $\geq \lceil 100/12 \rceil = 9$ people

**Example 4.** There are 5 different types of scholarships. What is the minimum number of students so that there are at least 6 students getting the same type of scholarship?

Solution. The minimum number of students needed to ensure that 6 students getting the same scholarship is the smallest integer $n$ such that $\lceil n/5 \rceil = 6$. The smallest integer is $n = 5 \times 5 + 1 = 26$.

Thus, 26 is the smallest number of student needed to ensure that there are 6 students getting the same type of scholarship

# Example

**Example 5**. What is the minimum number of area codes so that 25 millions cellphones, each assigned to a unique 10-digit number of the form NXX-NXX-XXXX where the first 3 numbers is the area code, N representing the numbers through 2 to 9, and X representing number through 0 to 9

**Solution**: The number of phone numbers in the form NXX-XXXX is:

8 millions.

According to Dirichlet principle, among 25 millions cellphones, there are always at least $\lceil 25/8 \rceil = 4$ cellphones with the same number. Therefore, we need at least 4 area codes to ensure that 25 millions cellphones do not have the same number.

# Example

***Dirichlet principle:*** "If putting $n$ objects into $k$ boxes, one could always find at least one box containing $\geq \lceil n/k \rceil$ objects".

**Example 6.**

There are 50 baskets. Every basket contains apples, but not more than 24apples. Prove that there are at least 3 baskets containing the $\boxed{\text{same amount of apples.}}$

**Solution**:

Number of Objects ~ Number of baskets → 50 baskets

Number of Boxes ~ Number of apples in each basket → 24 boxes

$\boxed{1}$ $\boxed{2}$ $\boxed{3}$ $\boxed{24}$

We put each basket in one of 24 boxes depending on the number of apples in the basket.

Dirichlet principle: at least one box contains $\lceil 50/24 \rceil = 3$ baskets

➔ There is at least 3 baskets in the same box (same amount of apples)

# Example

**Example 7**. Prove that among 4 arbitrary natural numbers, there are always 2 numbers with difference is divisible by 3.

**Solution**: When diving a natural number by 3, there could be 3 remainders (0, 1 or 2). There are 4 numbers, so according to Dirichlet principle, there are 2 numbers of them have the same remainders when divided by 3, so we can write:

$n_1 = 3k_1 + r$

$n_2 = 3k_2 + r$

where $r$ is the remainder when divided by 3. Then, their difference is

$n_1 - n_2 = (3k_1+r) - (3k_2+r) = 3(k_1-k_2)$

→ $n_1 - n_2$ is divisible by 3

# Example

**Example 8**. 15 students write a report together. Lan takes 13 mistakes, each of remaining students takes less than 13 mistakes. Prove that there are always 2 students taking the same number of mistakes.

*Proof:*

# Example

**Example 9**. Set S consists of 6 integers from 1 to 12. Prove that there exists always 2 nonempty subsets of S such that the sum of elements in these subsets are equal.

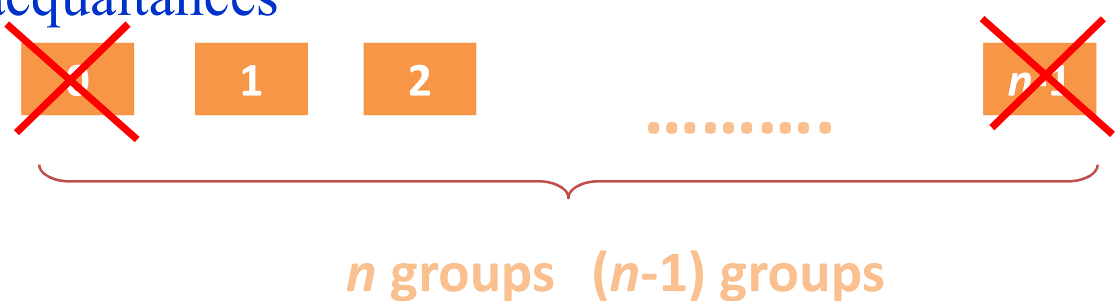
# Example

**Example 10**. In a meeting room, there are always 2 people whom are acquainted with the same number of people present at the meeting.

**Solution.** Let the number of people in the meeting be $n$, then the number of acquaitance of any people in the meeting could only be 0 to $n$-1.

Obviously, in the room, it could not exists a people having number of acquaitances is 0 (means do not know anybody) and a people having number of acquaitances is $n$-1 (means know everybody in the room). Therefore, dividing people based on the numeber of acquaitances, one could only divide $n$ people into $n$-1 groups.

According to Dirichlet principle, there are at least one group containing at least 2 people, it means one could always find at least 2 people with the same number of acquaitances



# Example

**Example 11.** In a month of 30 days, a volleyball team plays at least 1 match per day, but does not play more than 45 matches. Prove that it always could find a period consisting of a certain number of consecutive days in the month so that the team plays exactly 14 matches during that period.

**Solution**: Let $a_j$ be the total number of matches played until day $j$ of the team. Then

$$a_1, a_2, \ldots, a_{30}$$

is the increasing sequence of positive integer numbers and $1 \le a_j \le 45$. Therefore, the sequence

$$a_1+14, a_2+14, \ldots, a_{30}+14$$

is also the increasing sequence of positive integer numbers and $15 \le a_j + 14 \le 59$.

- There are 60 positive integer numbers

$$a_1, a_2, \ldots, a_{30}, a_1+14, a_2+14, \ldots, a_{30}+14,$$

where all elements are less than or equal to 59

- Therefore, according to Dirichlet principle, two of these elements are equal. As the numbers $a_1, \ldots, a_{30}$ are thirty distinct positive integer numbers and numbers $a_1+14, \ldots, a_{30}+14$ are thirty distinct positive integer numbers, thus we could find index $i$ and $j$ such that $a_i = a_j+14$. It means there are exactly 14 matches in the period from day $j+1$ to day $i$.

# Example

**Example 12**. Prove that, among $n+1$ positive integer numbers, each not larger than $2n$, one could always find two numbers, such that one number is divisible by the other

**Solution:** Let the given numbers be

$$a_1, a_2, \ldots, a_{n+1}.$$

Write each number $a_j$ of $n+1$ above numbers in the form:

$$a_j = 2^{k(j)}q_j, \; j = 1, 2, \ldots, n+1$$

where $k(j)$ is a non-negative integer, $q_j$ is odd.

- Numbers $q_1, q_2, \ldots, q_{n+1}$ are odd integers, each number is not greater than $2n$.
- Integers from 1 to $2n$, there are only $n$ odd numbers, so according Dirichlet principle we have: two numbers of $(n+1)$ numbers $q_1, q_2, \ldots, q_{n+1}$ are equal, it means we could find two indices $i$ and $j$ such that $q_i = q_j = q$.
- Then

$$a_i = 2^{k(i)}q, \; a_j = 2^{k(j)}q.$$

So if $k(i) < k(j)$ then $a_j$ is divisible by $a_i$, and if $k(i) \geq k(j)$ then $a_i$ is divisible by $a_j$.

# Example

**Example 13.** On the plane, let's consider 5 points with integer coordinates $M_i(x_i, y_i)$, $i$=1, 2, ..., 5. Prove that there are always two points such that the segment connecting them, excluding the two ends, passes through another point having integer coordinates.

Middle point

**Solution.** We prove that: always could find 2 points such that the segment connecting these two points has the middle point with integer coordinates. According to the parity of two coordinates, given 5 points could be divided into at most 4 groups:

(Even, Even), (Even, Odd), (Odd, Even), (Odd, Odd).

# Example

- Therefore, according Dirichlet principle, one must find a group of at least 2 points, such as $M_i$, $M_j$. The middle point $G_{ij}$ of the segment connecting $M_i$ and $M_j$ has the coordinates

$$G_{ij} = ((x_i+x_j)/2, (y_i+y_j)/2).$$

- As $x_i$ and $x_j$ as well as $y_i$ and $y_j$ have the same parity, then the coordinates of $G_{ij}$ are integers. The claim in the example is proven.
- This claim could be generalized in $n$-dimensional space: "In $n$-dimensional space, let's consider $2^n + 1$ points with integer coordinates. Then one always could find 2 points so that the segment connecting them, excluding two ends, passes to another point with integer coordinates".

# Example 14

First, we consider some concepts.

Let $a_1, a_2, \ldots a_n$ be sequence of real numbers.

- $n$ is the ***length*** of the given sequence.
- ***Subsequence*** of the given sequence is the sequence with the form $a_{i_1}$, $a_{i_2}$, …, $a_{i_m}$, where $1 \le i_1 < i_2 < \ldots < i_m \le n$
- Sequence is ***strictly increasing*** if $a_i < a_{i+1}$ for every $i=1,..,n$.
- Sequence is ***strictly decreasing*** if $a_i < a_{i+1}$ for every $i=1,..,n$.

Example: Consider the sequence: 1, 5, 6, 2, 3, 9.

- 5, 6, 9 is strictly increasing subsequence
- 6, 3 is strictly decreasing subsequence

# Example 14

**Theorem:** Sequence of $n^2+1$ *distinct* numbers always contains either strictly increasing subsequence of length $n+1$ or strictly decreasing subsequence of length $n+1$.

**Example:** Sequence

8, 11, 9, 1, 4, 6, 12, 10, 5, 7

consists of $10 = 3^2+1$ elements, has to contain either strictly increasing subsequence of length 4 or strictly decreasing subsequence of length 4.

1, 4, 6, 12
1, 4, 6, 7
11, 9, 6, 5

**Proof:** Assume $a_1, a_2, \ldots, a_{n^2+1}$ is a sequence consisting of $n^2+1$ distinct numbers. Assign to each element $a_k$ an ordered pair $(i_k, d_k)$, where $i_k$ is the length of the longest strictly increasing subsequence starting from $a_k$ and $d_k$ is the length of the longest strictly decreasing subsequence starting from $a_k$.

Example: 8, 11, 9, 1, 4, 6, 12, 10, 5, 7

$a_2 = 11 \Rightarrow (i_2, d_2) = (2, 4)$

$a_4 = 1 \Rightarrow (i_4, d_4) = ?$

- Let assume there does not exist strictly increasing and decreasing subsequence of length $n+1$. Thus $i_k$ and $d_k$ are positive integers $\leq n$, where $k = 1, 2, \ldots, n^2+1$.

# Example 14

- As $1 \le i_k, d_k \le n$, following the product rule, there are $n^2$ distinct ordered pairs $(i_k, d_k)$.

➔ As there are $n^2 + 1$ ordered pair $(i_k, d_k)$, so according to the Dirichlet principle, two of them are identical.

It means there exists 2 elements $a_s$ and $a_t$ in the sequence where $s < t$ such that $i_s = i_t$ and $d_s = d_t$.

We show that it is impossible:

- As elements in the sequence are distinct, so

  either $a_s < a_t$ or $a_s > a_t$.

  – If $a_s < a_t$, then because $i_s = i_t$ , we could build increasing subsequence of length $i_t+1$ starting from $a_s$, by concatenating it to increasing subsequence of length $i_t$, starting from $a_t$.

  **… , $a_s$, …, $a_t$, ….**

  The longest subsequence starting from $a_s$ has the length at least of $i_t + 1$, it measn $i_s > i_t$.

  It is contradiction to the assumption $i_s = i_t$.

  – Similarly, if $a_s > a_t$, we could show that $d_s$ must be greater than $d_t$, and also come to a contradiction.

Theorem is thus proven.