Index

Unit – 1 ⇝ Number Theory and Counting

Unit – 1.1 ⇝ Number Theory

Method – 1 ⇝ Principle of Mathematical Induction

Principle of Mathematical Induction

→ Principle of mathematical induction can be used to prove that a statement P(n) is valid for all integers $n \geq a$.

→ **Procedure to show P(n) is true for all integers $n \geq a$.**

Where P(n) is a property that is defined for integers "n", "a" be a fixed integer.

- Show that P(a) is true.
- Assume P(k) is true for all integers $k \geq a$,

  then prove that $P(k+1)$ is also true.
- From above two steps, we can conclude that P(n) is true for all integers $n \geq a$.

Examples of Method-1: Principle of Mathematical Induction

C	1	Prove that proposition P, the sum of the first n positive integers is $\frac{n(n+1)}{2}$.
C	2	Prove that proposition P, the sum of the squares of the first n positive integers is $\frac{n(n+1)(2n+1)}{6}$.
C	3	Prove statement $7^n - 2^n$ is divisible by 5, for all integers $n \geq 0$ using mathematical induction.
C	4	Use mathematical induction to prove that $2n+1 < 2^n$, for all integers $n \geq 3$.

Method – 2 ⇝ Congruence Relation

Modulo or Modulus or Mod

→ The modulo (or "modulus" or "mod") is the **remainder** after dividing one number by another.

→ Let **a** and **b** be two integers, then **a** (**mod b**) gives remainder after dividing a by b.

→ For example:

- $12 \pmod 7 = 5$
- $-11 \pmod 3 = 1$

Properties of Modulo

(1) $(a + b) \pmod m = [\, a \pmod m + b \pmod m \,] \pmod m$

(2) $(a - b) \pmod m = [\, a \pmod m - b \pmod m \,] \pmod m$

(3) $(a \times b) \pmod m = [\, a \pmod m \times b \pmod m \,] \pmod m$

(4) $(a^b) \pmod m = \left[(a \pmod m)^b \right] \pmod m$

Congruence Relation

→ Let **a** and **b** are integers and **m** be a **positive integer**.

→ If **m** divides **a − b**, then **m** is known as **modulus** and we can say that "a" is congruent to "b" modulo m.

→ It is denoted by **a ≡ b (mod m)** or **a ≡ b (modulo m)** and read as "a is congruent to b modulo m".

→ When m does **not** divide a − b we say that "a" is incongruent to "b" modulo m.

→ It is denoted by **a ≢ b (mod m)** and read as "a is incongruent to b modulo m".

→ For example:

- $87 \equiv 23 \pmod 4$

  as 4 divides $87 - 23 = 64$

- $27 \not\equiv 8 \pmod 9$

  as 9 does not divide $27 - 8 = 19$.

Basic Properties of Congruence

→ Let $m > 1$ be fixed and a, b, c, d be arbitrary integers.

Then the following properties hold:

(1) If $a \equiv b \pmod{m}$, then there exist "k" such that $\mathbf{a = k \cdot m + b}$, $0 \leq b < m$.

(2) $a \equiv b \pmod{m}$ means that a and b leave the same nonnegative remainder when divided by m.

i.e., $\mathbf{a = k_1 \cdot m + r}$ and $\mathbf{b = k_2 \cdot m + r}$

(3) $\mathbf{a} \equiv \mathbf{a} \pmod{m}$

(4) If $\mathbf{a} \equiv \mathbf{b} \pmod{m}$, then $\mathbf{b} \equiv \mathbf{a} \pmod{m}$.

(5) If $\mathbf{a} \equiv \mathbf{b} \pmod{m}$ and $\mathbf{b} \equiv \mathbf{c} \pmod{m}$, then $\mathbf{a} \equiv \mathbf{c} \pmod{m}$.

(6) If $\mathbf{a} \equiv \mathbf{c} \pmod{m}$ and $\mathbf{b} \equiv \mathbf{d} \pmod{m}$, then

$\mathbf{a} + \mathbf{b} \equiv \mathbf{c} + \mathbf{d} \pmod{m}$ and

$\mathbf{ab} \equiv \mathbf{cd} \pmod{m}$.

(7) If $a \equiv b \pmod{m}$, then

$a + \mathbf{c} \equiv b + \mathbf{c} \pmod{m}$ and

$a\mathbf{c} \equiv b\mathbf{c} \pmod{m}$.

Examples of Method-2: Congruence Relation

C	1	Which of the following is true? (1) $-446 \equiv -278 \pmod{7}$ (2) $383 \equiv 126 \pmod{15}$ **Answer: (1) True (2) False**
C	2	Find the smallest non-negative integer which is congruent modulo $m = 8$ to each of the following numbers: (1) 379 (2) -578 **Answer: (1) 3 (2) 6**

Method – 3 ⇝ Encrypting and Decrypting a Message using Caesar Cipher Method

Cryptography

→ The word cryptography is derived from the Greek **kryptos**, meaning "hidden" and **graphein** meaning "to write".

→ Cryptography is the science of secret writing with the goal of hiding the meaning of a message.

Basic Terminologies:

(1) **Plaintext** : The **original information** that needs to be protected.

(2) **Ciphertext** : The transformed, **encrypted** form of the plaintext.

(3) **Encryption** : The process of converting **plaintext into ciphertext**.

(4) **Decryption** : The process of converting **ciphertext back into plaintext**.

Caesar Cipher

→ One of the earliest cryptographic systems was used by the great Roman emperor **Julius Caesar** around 50 B.C.

→ In which each letter of the alphabet is replaced by the letter that occurs **three** places down the alphabet.

i.e., **A** would be replaced by **D**, **B** by **E** and so forth.

→ **Steps to Encrypt a Message Using Caesar Cipher Method**

- **Step 1:**
  - Assign unique integer **p** to each alphabet of given plaintext.

    For assigning an integer use the following table.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- **Step 2:**
  - Encrypt each integer **p** to an integer **c** by following congruence relation.

    $\mathbf{c} \equiv (\mathbf{p} + \mathbf{3}) (\mathbf{mod\ 26})$
  - Here, p + 3 represents that each letter of given plaintext will be shifted forward by 3 places.
- **Step 3:**
  - Translate back this integer **c** to alphabet to write a ciphertext.

→ For example:

- Encrypt a message "**ENEMY**" using Caesar cipher.

  Step 1: Assigning unique integer **p** to each alphabet of given plaintext.

Plaintext	E	N	E	M	Y
p	4	13	4	12	24

Step 2: Encryption by using $\mathbf{c} \equiv (\mathbf{p} + \mathbf{3}) (\mathbf{mod\ 26})$.

$\mathbf{p = 4} \quad \Rightarrow \quad c \equiv (4 + 3) (\text{mod } 26) = 7 (\text{mod } 26)$

$= 7$

$\mathbf{p = 13} \quad \Rightarrow \quad c \equiv (13 + 3) (\text{mod } 26) = 16 (\text{mod } 26)$

$= 16$

$\mathbf{p = 12} \quad \Rightarrow \quad c \equiv (12 + 3) (\text{mod } 26) = 15 (\text{mod } 26)$

$= 15$

$\mathbf{p = 24} \quad \Rightarrow \quad c \equiv (24 + 3) (\text{mod } 26) = 27 (\text{mod } 26)$

$= (26 \cdot 1 + \mathbf{1}) (\text{mod } 26)$

$= 1$

Step 3: Translating this integer **c** to alphabet to write a ciphertext.

c	7	16	7	15	1
Ciphertext	H	Q	H	P	B

Hence, encrypted message is "**HQHPB**".

→ **Steps to Decrypt a Message Using Caesar Cipher Method**

- **Step 1:**
  - Assign unique integer **c** to each alphabet of given ciphertext.
- **Step 2:**
  - Decrypt each integer **c** to an integer **p** by following congruence relation.

    $\mathbf{p \equiv (c - 3)(mod\ 26)}$
- **Step 3:**
  - Translate back this integer **p** to alphabet to write a plaintext.

→ For example:

- Decrypt a message "**CHEUD**" using Caesar cipher.

  Step 1: Assigning unique integer **c** to each alphabet of given ciphertext.

Ciphertext	C	H	E	U	D
c	2	7	4	20	3

Step 2: Decryption by using $\mathbf{p \equiv (c - 3)(mod\ 26)}$

$\mathbf{c = 2} \Rightarrow p \equiv (2 - 3)(mod\ 26) = -1(mod\ 26)$

$= (-1 + \mathbf{26})(mod\ 26)$

$= 25(mod\ 26)$

$= 25$

$\mathbf{c = 7} \Rightarrow p \equiv (7 - 3)(mod\ 26) = 4(mod\ 26)$

$= 4$

$\mathbf{c = 4} \Rightarrow p \equiv (4 - 3)(mod\ 26) = 1(mod\ 26)$

$= 1$

$\mathbf{c = 20} \Rightarrow p \equiv (20 - 3)(mod\ 26) = 17(mod\ 26)$

$= 17$

$\mathbf{c = 3} \Rightarrow p \equiv (3 - 3)(mod\ 26) = 0(mod\ 26)$

$= 0$

Step 3: Translating this integer **p** to alphabet to write a plaintext.

p	25	4	1	17	0
Plaintext	Z	E	B	R	A

Hence, decrypted message is "**ZEBRA**".

Shift Cipher

→ We simply shift every plaintext letter by a fixed number of positions say **k** in the alphabet.

→ To encrypt or decrypt a message, relation $c \equiv (p + \mathbf{k}) \pmod{26}$ or $p \equiv (c - \mathbf{k}) \pmod{26}$ are used,

where **k** is known as **key** and it is always a positive integer from 1 to 25.

→ Note that, shift cipher with a key value of $\mathbf{k = 3}$ is known as "**Caesar Cipher**".

Examples of Method-3: Encrypting and Decrypting a Message using Caesar Cipher Method

C	1	Convert given plaintext **"YOU ARE GENIUS"** into ciphertext by using key value $k = 4$. **Answer**: **CSY EVI KIRMYW**
C	2	Convert given ciphertext **"ANPNSLX"** into plaintext by using key value $k = 5$. **Answer**: **VIKINGS**

Method – 4 ⇝ Encrypting and Decrypting a Message using RSA Cryptosystem

RSA Cryptosystem

→ In 1976, three researchers at the Massachusetts Institute of Technology Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman introduced the RSA system.

→ The RSA cryptosystem is an example of a "**public key**" system.

→ This means that everyone can know the encryption key, but it is computationally infeasible for an unauthorized person to deduce the corresponding decryption key.

→ **RSA Key Generation**

- **Step 1:**
  - Choose two large primes $\mathbf{p}$ and $\mathbf{q}$.
- **Step 2:**
  - Compute $\mathbf{n = p \cdot q}$ (Will be used as modulus)
- **Step 3:**
  - Compute $\mathbf{\Phi(n) = (p - 1)(q - 1)}$.
- **Step 4:**
  - Select the public exponent $\mathbf{e}$ such that

    $\mathbf{e} \in \{ 1, 2, 3, \ldots, \Phi(n) - 1 \}$ and

    $\mathbf{gcd(e, \Phi(n)) = 1}$.
- **Public Key:**
  - $\mathbf{k_{pub} = (n, e)}$
- **Step 5:**
  - Compute the private key $\mathbf{d}$ such that

    $\mathbf{d \cdot e \equiv 1 \pmod{\Phi(n)}}$ OR $\mathbf{d \equiv e^{-1} \pmod{\Phi(n)}}$.

    Note that here $d \in \{ 1, 2, 3, \ldots, \Phi(n) - 1 \}$
- **Private Key:**
  - $\mathbf{k_{pr} = (n, d)}$

→ **RSA Encryption & Decryption**

- **RSA Encryption**
  - Given the public key $\mathbf{k_{pub}} = (\mathbf{n}, \mathbf{e})$ and the plaintext $\mathbf{m}$, then ciphertext $\mathbf{c}$ is $\mathbf{c \equiv m^e \pmod n}$.
- **RSA Decryption**
  - Given the private key $\mathbf{k_{pr}} = (\mathbf{n}, \mathbf{d})$ and the ciphertext $\mathbf{c}$, then plaintext $\mathbf{m}$ is $\mathbf{m \equiv c^d \pmod n}$.

→ For example:

- Encrypt a message $m = 12$ using RSA cryptosystem with public key $(35, 11)$.

  Given message is $m = 12$ and public key is $\mathbf{k_{pub}} = (\mathbf{35}, \mathbf{11})$.

  So, $n = 35$ and $e = 11$.

  Now,

  $$c \equiv m^e \pmod n$$

  $$\Rightarrow c \equiv 12^{11} \pmod{35}$$

  $$\Rightarrow c \equiv (12 \times 12^2 \times 12^8) \pmod{35}$$

  $$\Rightarrow c \equiv [\, 12 \pmod{35} \times 12^2 \pmod{35} \times 12^8 \pmod{35} \,] \pmod{35}$$

  Here,

  $12 \pmod{35} = 12$

  $12^2 \pmod{35} = 144 \pmod{35}$
  $= 4$

  $12^8 \pmod{35} = (12^2)^4 \pmod{35}$
  $= \left(12^2 \pmod{35}\right)^4 \pmod{35}$
  $= (4)^4 \pmod{35}$
  $= 256 \pmod{35}$
  $= 11$

  So,

  $$c \equiv (\, 12 \times 4 \times 11 \,) \pmod{35}$$

  $$c \equiv 528 \pmod{35}$$

  $$c \equiv 3 \pmod{35}$$

  Hence, encrypted message is $c = 3$.

Examples of Method-4: Encrypting and Decrypting a Message using RSA Cryptosystem

C	1	Encrypt a message $m = 9$ using RSA algorithm with $p = 5$, $q = 11$, $e = 3$. **Answer: $c = 14$.**
C	2	Decrypt a message $c = 4$ using RSA cryptosystem with value $p = 3$, $q = 11$, $e = 3$. **Answer: $m = 16$.**
C	3	Decrypt a message $c = 19$ using RSA cryptosystem with value $p = 11$, $q = 17$, $d = 23$. **Answer: $m = 94$**

Unit – 1.2 ⇝ Counting

Method – 5 ⇝ Basics of Counting

Basic Principles of Counting

→ We first learn two basic counting principles:

(1) Product Rule

(2) Sum Rule

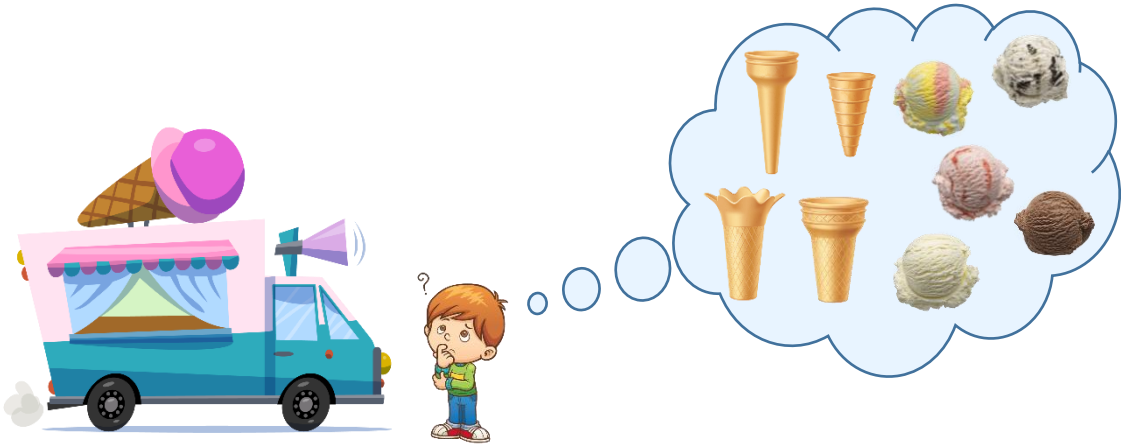
(1) **Product Rule**

- If an event can occur in **m** different ways, following which another event can occur in **n** different ways, then the total number of occurrences of the events in the given order is $\mathbf{m \times n}$.
- In general, if events $\mathbf{E_1, E_2, E_3, \ldots, E_n}$ can occur one after another in $\mathbf{m_1, m_2, m_2, \ldots, m_n}$ different ways respectively, then the total number of occurrences of the events in the given order is $\mathbf{m_1 \times m_2 \times m_2 \times \ldots \times m_n}$.
- For example:
  - You went to buy an ice-cream.

    There are **4** different choices for **cones**.

    There are **5** different flavours of **ice creams**.

    How many choices do you have?



A **cone** can be chosen in **4** different ways.

An **ice cream** can be chosen in **5** different ways.

Hence, there are $\mathbf{4 \times 5 = 20}$ pairs of a cone and an ice-cream.

(2) **Sum Rule**

- If an event can be occurred in either in **m** different ways or in **n** different ways, then total number of occurrences of event is given is $\mathbf{m + n}$."
- "In general, if events $\mathbf{E_1, E_2, E_3, \ldots, E_n}$ cannot occur simultaneously in $\mathbf{m_1, m_2, m_2, \ldots, m_n}$ different ways respectively, then the total number of occurrences of the events is $\mathbf{m_1 + m_2 + m_2 + \cdots + m_n}$."
- For example
  - You went to a pet shop and find that the pet shop have **4** birds, **3** cats, **2** rabbits, **7** fish.

4 birds **3 cats** **2 rabbits** **7 fish**

You can pick only one animal as a pet, how many choices do you have for a pet?

i.e., you can choose a bird **or** a cat **or** a rabbit **or** a fish.

- A **bird** can be chosen in **4** different ways.
- A **cat** can be chosen in **3** different ways.
- A **rabbit** can be chosen in **2** different ways.
- A **fish** can be chosen in **7** different ways.
- So, there are $\mathbf{4 + 3 + 2 + 7 = 16}$ ways to select a pet.

Examples of Method-5: Basics of Counting

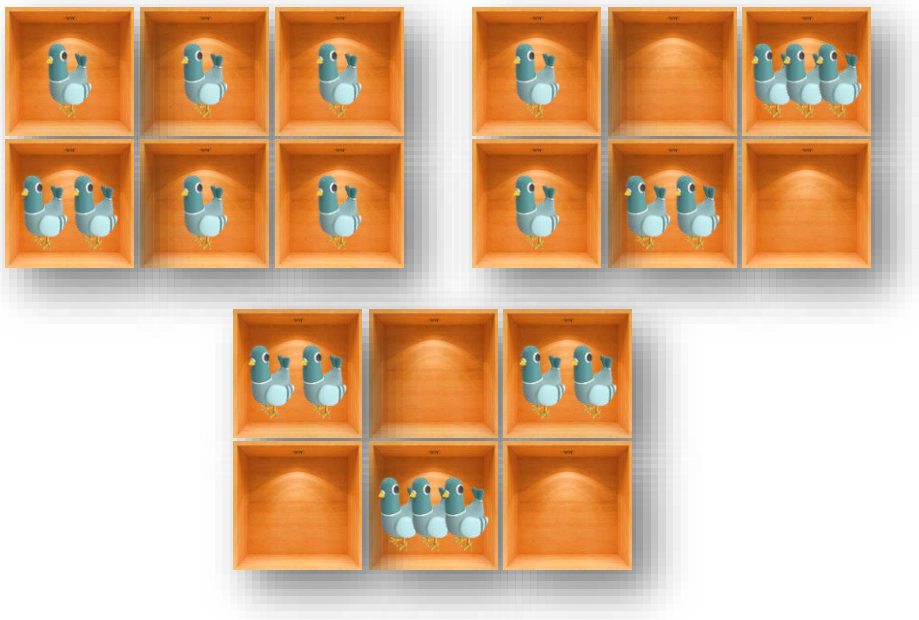
C	1	The chairs of an auditorium are to be labelled with an uppercase English letter followed by a positive integer not exceeding 100. What is the largest number of chairs that can be labelled differently? **Answer: 2600**
C	2	Find the number of 4 letter words, with or without meaning, which can be formed out of the letters of the word ROSE, (**1**) When the repetition of the letters is not allowed. (**2**) When the repetition of the letters is allowed. **Answer: (1) 24 (2) 256**
C	3	How many even numbers lying between 100 and 1000 can be formed with the digits 0, 1, 2, 3, 4, 5, if the repetition of the digits is not allowed? **Answer: 52**
C	4	How many words with or without meaning starting with a vowel can be formed using letters of a words "COMPUTER". **Answer: 15120**
C	5	A new company with just two employees, Adam and Paul, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees? **Answer: 132**

Method – 6 ⇝ Pigeonhole Principle

Pigeonhole Principle

→ If **n** pigeonholes (boxes) are occupied by **n + 1** or more pigeons (objects), then at least one pigeonhole (box) is occupied by two or more pigeons (objects).

→ Suppose we distribute 7 pigeons in 6 pigeonholes.



→ The pigeonhole principle is also called the **Dirichlet drawer principle**.

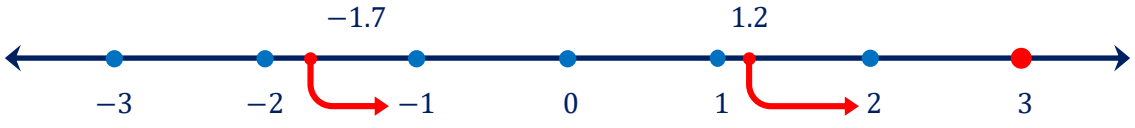
Least integer function **or** Ceiling function **(Prerequisite)**

→ A function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \min\{ n \in \mathbb{Z} : n \geq x \}$, $\forall x \in \mathbb{R}$ is known as a least integer function or ceiling function.

→ It is denoted by $\lceil x \rceil$ and read as "ceiling value of x".

→ For example:

→ $\lceil 1.2 \rceil = 2$, $\lceil 3 \rceil = 3$, $\lceil -1.7 \rceil = -1$



Generalized Pigeonhole Principle

→ If **n** pigeonholes are occupied by **kn + 1** or more pigeons, where k is a positive integer, then at least one pigeonhole is occupied by k + 1 or more pigeons.

OR

→ If **n** boxes are occupied by **m** objects provided m > n, then there is at least one box containing at least $\left\lceil \frac{m}{n} \right\rceil$ objects.

→ For example:

- At least how many out of 100 people would share same birth month?

  n = **12** months (Boxes)

  m = **100** people (Objects)

  Now,

  $$\left\lceil \frac{100}{12} \right\rceil = \lceil 8.33 \rceil = 9$$

  Hence, among 100 people, at least **9** would share same birth month.

Examples of Method-6: Pigeonhole Principle

C	1	If there are 30 students in a class, then at least how many would have last names that begin with the same letter? **Answer: 2**
C	2	What is the minimum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and E? **Answer: 26**
C	3	A laundry bag contains many red, white and blue socks. Find the minimum number of socks that one needs to choose in order to get four pairs (eight socks) of the same colour. **Answer: 22**
C	4	How many cards must be selected from a standard deck of 52 cards to guarantee that at least three cards of the same suit are selected? **Answer: 9**

C	5	What is the minimum number of employees in a company so that there will be at least 10 employees in one department and the departments in the company are HR, Marketing, Tech and Support? **Answer: 37**

*** * * * * End of the Unit * * * * ***