Chapter 9:- Cryptography

§9.1 – Modular Arithmetic

Here we introduce another type of Arithmetic which will be between the reminders of a given fixed number.

$$M_n = \{0, 1, 2, \dots, n-1\}$$

$a \bmod n$ = reminder of a divided by n.

Example:-

(1) $7 \bmod 3 = 1$

(2) $33 \bmod 11 = 0$.

(3) $-1 \bmod 5 = 4$.

(4) $-20 \bmod 3 = -20 + 3\times 7 \pmod 3$
$= -20 + 21 \pmod 3$
$= 1 \pmod 3$
$= 1$

Example:-

- $55 \bmod 4 = 55 - 4\times 13 \pmod 4$
$= 55 - 52 \pmod 4$
$= 3 \pmod 4$
$= 3$
- $26 \bmod 4 = 26 - 4\times 6 \pmod 4$
$= 26 - 24 \pmod 4$
$= 2 \bmod 4$
$= 2$

Exercise:-

- $45 \bmod 6$, $104 \pmod 6$
- $(45 + 104) \pmod 6$, $(45 - 104) \pmod 6$
- $(45 \cdot 104) \pmod 6$, $104^2 \pmod 6$
- $(104)^5 \bmod 6$.

Theorem:-

1- $r \bmod n = r$ if $r = 0, 1, 2, \dots, n-1$

2- $a \bmod n = a - k\times n \pmod n$, $k \in \mathbb{Z}$.

3- $a \bmod n = r$, $b \bmod n = s$
- $(a+b) \pmod n = (r+s) \bmod n$.
- $(a \cdot b) \bmod n = (r \cdot s) \bmod n$.

§ 9.2 - Cryptography

"The Science of Secret messages".

- **Encryption method:**
  A method to convert an original message M into a secret message C.
- **Decryption method:**
  A method that reverses the encryption i.e., to convert the secret message C into an original message.

Cryptosystem is a system consists of encryption and decryption methods.

Cryptography is the science that deals with cryptosystems.

Notation:

1. M is called the plaintext (small letter)
2. C is called the ciphertext (capital letter)

1- Caesar Cipher

was first used by Julius Caesar to give orders to his troops.

Encryption $C = M + 3 \pmod{26}$

Decryption $M = C - 3 \pmod{26}$

Example: Encrypt "attack now"

letters	a	t	t	a	c	k	n	o	w
M	0	19	19	0	2	10	13	14	22
$(M+3) \bmod 26$	3	22	22	3	5	13	16	17	25
C	D	W	W	D	F	N	Q	R	Z

"DWWDFNQRZ"