A mod B (A%B)

A - A ÷ B × B

Page No.

Date

ITC Mod 5

- Prime No. Generation :-

1 In Cryptography, prime no.s play imp role, especially in algos like RSA (Relatively Slow Algorithm).

2 Cryptographic applications require prime no.s of a specific size to withstand attacks. Specialized algos are used to generate & verify prime no.s in cryptographic contexts

3 These algos ensure that generated no.s are prime which is crucial ~~that~~ for security of cryptographic protocols

- Random Number Generation

1 In Cryptography, randomness of generated numbers is crucial for security of cryptographic algos & protocols.

2 Pseudo random no. generators are used to generate random like sequences of no.s. They start from seed (initial value) and produce a random no. sequence.

3 They are deterministic, same seed → same sequence.

4 These generators meet specific criteria to ensure that their output is indistinguishable from true randomness by any efficient algo.

- Congruences :-

1 Reflexive : $a \equiv a \pmod{M}$

integer ↙ +ve int ↙

2 Symmetric : if $a \equiv b \pmod{M}$ then $b \equiv a \pmod{M}$

3 Transitive : if $a \equiv b \pmod{M}$ and $b \equiv c \pmod{M}$ then $a \equiv c \pmod{m}$

4 Addition : if $a \equiv b \pmod{M}$ and $c \equiv d \pmod{M}$

$a + c \equiv b + d \pmod{M}$

5 Multiplication : $a \times c \equiv b \times d \pmod{M}$

- Solving Linear Congruences $ax + by = d$

$ax + by = d \pmod{M}$

a, b, d, m are integers

To Find : int x and y , Method : Extended Euclidean Algo

Page No.
Date

1. Find x' and y' such that $ax' + by' = \gcd(a,b)$
Bezout Coeff.
2. If d isn't divisible by GCD (a,b)
no solutions exist, else, divide both sides of eqⁿ
$ax' + by' = \gcd(a,b)$ by $\gcd(a,b)$
$\frac{ax' + by'}{\gcd(a,b)} = 1$ congruence $ax'' + by'' \equiv 1 \pmod M$ is obtained
3. Multiply both sides of new congruence by d.
$\therefore d(ax'' + by'') \equiv d \pmod M$
$ax''d + by''d \equiv d \pmod M$
4. $x = x''d$ and $y = y''d$ are the solⁿ
[i didn't understand shit]

- Questions
1. Solve the linear congruence $3x + 5y \equiv 7 \pmod{11}$
→ GCD of $(3,5) = 1$ $ax' + by' = \gcd(a,b)$
Apply Extended Euclidean theorem, $ax' + by' = 1$
when $x' = 2$ and $y' = -1$ set them in such a way to get 1
$3x' + 5y' = 1$
$2x - y \equiv 1 \pmod{11}$
Multiply both sides by 7
$14x - 7y = 7 \pmod{11}$
$x = 14$ $y = -7$ [what even is going on?]
2. $4x + 6y \equiv 10 \pmod{18}$
→ gcd $(4,6) = 2$
where $x' = 2$ and $y' = -1$
But 2 doesn't divide 10
No solutions exist. [idk, wtf?]
3. Find GCD of 18, 12 using Euler's method.
→
$$
\begin{array}{l}
12 \overline{)\,18\,}(1 \\
\quad -12 \\
\hline
\text{GCD} \to 6 \overline{)\,12\,}(2 \\
\qquad -12 \\
\hline
\qquad 0
\end{array}
$$
GCD = 6
[seriously? TT]

Page No.
Date

4. Find GCD of 385, 756 by Euler's method

$$
\begin{array}{l}
385 \overline{)756} \,(1 \\
\quad -385 \\
\quad 371 \overline{)385} \,(1 \\
\qquad -371 \\
\qquad 14 \overline{)371} \,(26 \\
\qquad\quad -364 \\
\qquad\quad 7 \overline{)14} \,(2 \\
\qquad\qquad -14 \\
\qquad\qquad 0
\end{array}
$$

GCD = 7

• Chinese Remainder Theorem

1. Fundamental theorem in number theory that provides a solution to systems of simultaneous congruences

$x = a_1 \bmod m_1 \qquad x = a_2 \bmod m_2 \qquad x = a_3 \bmod m_3$

m_1, m_2 and m_3 are mutually prime

$$M = m_1 * m_2 * m_3$$

$$M_i = \frac{M}{m_i} \quad \text{for } i = 1, 2, 3$$

$$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \bmod M$$

where x_i = multiplicative inverse of M_i

i.e. $(M_i * x_i) \equiv 1 \bmod m_i$

Applications: Number Theory, Cryptography, Computer Science, Optimization of Modular arithmetic operations.

• Questions -

1. Find x such that $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 4$, $x \equiv 1 \bmod 5$

$m_1 = 3$, $m_2 = 4$, $m_3 = 5$

$$M = 3 \times 4 \times 5 = 60$$

$$M_1 = \frac{60}{3} = 20 \qquad M_2 = \frac{M}{m_2} = \frac{60}{4} = 15 \qquad M_3 = \frac{60}{5} = 12$$

Page No.
Date

$M_1 x_1 = 1 \bmod m_1 \rightarrow 20x_1 = 1 \bmod 3$

$20 \times 2 = 40$

$x_1 = 2$

$40 \div 13 = 39$

remainder $= 1$

$M_2 x_2 \equiv 1 \bmod 4$

$15x_2 \% 4 = 1 \rightarrow x_2 = 3$

$M_3 x_3 = 1 \bmod 5$

$12 x_3 \% 5 = 1 \rightarrow x_3 = 3$

$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 a_3 x_3) \bmod M$

$= [(20 \times 2 \times 2) + (15 \times 3 \times 3) + (12 \times 3 \times 1)] \bmod 60$

$= 251 \bmod 60 = 11$

2 $x \equiv 1 \bmod 5$, $x \equiv 1 \bmod 7$, $x \equiv 3 \bmod 11$

$\rightarrow$ $M = m_1 \times m_2 \times m_3 = 385$

$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$

$M_2 = 385/7 = 55$ $\quad M_3 = 385/11 = 35$

$M_1 x_1 = 1 \bmod 5 \rightarrow 77x_1 = 1 \bmod 5$

$77 x_1 \% 5 = 1 \rightarrow x_1 = 3$

$M_2 x_2 = 1 \bmod 7 \rightarrow 55 \% 7 x_2 = 1 \rightarrow x_2 = 6$

$M_3 x_3 = 3 \bmod 11 \rightarrow 35 \% 11 x_2 = 3 \rightarrow x_3 = 6$

$x_1 = 3 \quad x_2 = 6 = x_3$

$x = [77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 3] \bmod 385$

$= 1191 \bmod 385 = 36$

- Euler's Totient Function

$\phi(n) = \{x \mid 1 \le x < n\}$, $\gcd(x_i, n) = 1$

eg $n = 10$

$\phi(n) = \{1, 3, 7, 9\} \rightarrow \gcd = 1$

$\phi(10) = 4$

Rules:-

1 $\phi(p) = p - 1$ if p is prime

eg. $\phi(2) = 2 - 1 = 1 = \{1\}$

$\phi(41) = 41 - 1 = 40$

2 If $a = p^n$ where p is prime and gcd (a,n) = 1
$\phi(p^n) = p^n - p^{n-1}$
eg $\phi(32) = \phi(2^5) = 2^5 - 2^4 = 16$
3 $\phi(m.n) = \phi(m).\phi(n)$ if m, n are relatively prime.
$\phi(10) = \phi(2\times5) = \phi(2).\phi(5)$
$= (2-1)(5-1) = 1\times4 = 4$ $\phi(10) = 4$
$\phi(35) = \phi(5\times7) = \phi(5).\phi(7) = (5-1)(7-1) = 24$
4 If P_1, P_2 are prime divisors on n, then
$\phi(n) = n * \left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\cdots\left(1-\frac{1}{P_n}\right)$
$\therefore \phi(60.0) = 600 * \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 160$

- Fast Modular Exponentiation

To efficiently compute large powers modulo of number
Commonly used in number theory and cryptography

1 Evaluate 3^{100} mod 15
→ $(100)_{10} = (1100100)$

1	1	0	0	1	0	0
3	12	9	6	3	9	6

1 [3^2 mod 15 = 9 mod 15 = 9 mod 15 = 9
[(9×3) mod 15 = 27 mod 15 = 12

should be 1 but figure out the calculation yourself ← 0 : 12^2 mod 15 = 144 mod 15 = 9
0 : 9^2 mod 15 = 6
1 [6^2 mod 15 = 6
[(6×3) mod 15 = 18 mod 15 = 3
0 : 3^2 mod 15 = 9 mod 15 = 9
0 : 9^2 mod 15 = 81 mod 15 = 6
3^{10} mod 15 = 6

2 Evaluate 5^{101} mod 10
→ $(101)_{10} = (1100101)$

1	1	0	0	1	0	1
5	5 5	5	5 5	5	5 5

1] 5^2 mod 10 = 5
] (5×5) mod 10 = 5
0 : 5^2 mod 10 = 5

5^{101} mod 10 = 5

Page No.
Date

- ## Fermat's Theorem / Fermat's Little Theorem

Its a fundamental result in no. theory, named after the mathematician (who cares). If p is a prime no. and a is an integer not divisible by p, then:

$$a^{p-1} \equiv 1 \pmod p$$

If p is a prime no. & a is any int. not divisible by p, then a^{p-1} leaves a remainder of 1 when divided by p.

Often used in modular arithmetic and cryptography for primality testing and modular exponentiation.

Applications in number theory, cryptography & algo design.

1. Evaluate $40^{110} \bmod 37$ using Fermat's theorem.

→ $p = 37$ $\quad \therefore p-1 = 36 \quad 110 = (36\times3+2)$

$40^{110} \bmod 37 = 40^{(36\times3+2)} \bmod 37$

$40 \equiv 3 \bmod 37$ — ① $\quad 40 - 37 = 3$

$40^{(36\times3+2)} \bmod 37 = [(40^{36} \bmod 37)(40^{36} \bmod 37)(40^{36} \bmod 37)(40^{2} \bmod 37)] \bmod 37$

from ①, $[(3^{110} \bmod 37 \times 3) \times 9] \bmod 37$

$= (1\times9) \bmod 37 = 9$

- ## Cryptography

Securing communication by converting plain text in cipher text. Involves many algos and protocols to ensure data confidentiality, integrity, authentication and non reduplication.

Techniques are obtained from mathematical concepts and a set of rule based calculations known as algos to convert messages in ways that make it hard to decode them.

~~Used for key~~ Algos used for cryptographic key generation, digital signing and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

Page No.
Date

- Encryption :-

Process of encoding info. Original representation → alt form (plain text → Cipher text)
Only authorized parties can decipher a ciphertext back to plain text and access original info.

	Encryption	Decryption
1	Normal msg → meaningless msg.	meaningless → original
2	plain → alt (cipher)	cipher → plain
3	Sender's end	receiver's end
4	secret key or public key used	secret key or private key used.

	Symmetric Cryptography	Assymmetric Cryptography
1	Keys must be securely distributed to all parties involved.	Public keys can be freely distributed, while pvt keys must be kept secret.
2	Shorter key lengths are sufficient for encryption/decrypt	Longer key lengths for enhanced security, making it slow.
3	Faster due to simpler algos and shorter key length	Slower due to complex algos and longer key length.
4	Susceptible to key distribution issues and need to protect the key	↓ vulnerable to key distributⁿ issues, but key protectⁿ is crucial.
5	Suitable for encrypting large amounts of data in a secure environment	Ideal for secure communication b/w parties w/o a prior exchange of keys.

- Shannon's Characteristics of a good cipher :-

1. Amt of secrecy needed should determine the amt. of labour appropriate for encryption / decryption.
2. Set of keys and enciphering algo. should be free from complexity.
3. Implementation should be simple.
4. Errors in ciphering should not propagate.
5. Size of ciphertext should be no larger than size of plain text.

- Confusion :-

Process of making the reln. b/w plain text and cipher text as complex and confusing as possible. Even a small change

Page No.
Date

in plain text should produce a significantly differ cipher text. This is typically achieved through techniques like substitution, where elements of the plain text are replaced with elements from a different set

- Diffusion :-
Spreading influence of each plain text element over many cipher text elements, thereby dispersing the statistical structure of the plain text.
Goal: ensure that the influence of any one plain text element is spread out over the entire cipher text, making it difficult to discern any patterns. Techniques such as permutation, where order of elements is changed are commonly used to achieve diffusion.

- Substitution Ciphers : A : 0 $\longrightarrow$ Z : 25

1 Caesar Substitution :-
Encode 'UPLOAD' using Casesar substitution. Show decoding too.

→
```
                  U   P   L   O   A   D
letter 3rd of   +3  +3  +3  +3  +3  +3        (k+3) % 26
                ------------------------
this one          X   S   O   R   D   G
```

```
decoding          X   S   O   R   D   G
                 -3  -3  -3  -3  -3  -3       (k-3) % 26
                ------------------------
                  U   P   L   O   A   D
```

2 Vignere Cipher : size (key) < size (msg)
Encode msg "WRITTEN" using key "HAPPY"
Show decoding too.

→ M_i = WRITTEN K_i = HAPPY
$C_i = (M_i + k_i) \% 26$

M_i	W	R	I	T	T	E	N
k_i	H	A	P	P	Y	H	A
$(M_i + k_i) \% 26$	3	17	23	8	17	11	13
C_i	D	R	X	I	R	L	N

: Encoded msg

Page No.
Date / /

Decoding : $C_i = (M_i - k_i) \% 26$

M_i	D	R	X	I	R	L	N
k_i	H	A	P	P	Y	H	A
$(M_i - k_i) \% 26$	22	17	8	19	19	4	13
C_i	W	R	I	T	T	E	N

3 Affine Cipher :
Encode 'DRIVE' using Affine Cipher. Take suitable values of a and b. Show decoding.

→ $a = 9$ $b = 2$ $c = (ax + b) \% 26$
↳ message to be encoded

x	D	R	I	V	E
$(ax+b) \% 26$	3	25	22	9	12
c	D	Z	W	J	M

Decoding :- y = multiplicat^n inverse of a
$y \cdot a \equiv 1 \bmod M$

y	1	2	3
$y \cdot a$	9	18	27
$(y \cdot a) \% 26$	9	18	1

use $y = 3$
$M = y(c - b) \% 26$

D	Z	W	J	M
3	17	8	21	4
D	R	I	V	E

• Transposition Ciphers

1 Using transposition cipher encode message "system update" using key "apps". Show decoding too.

→ A P P S
1 2 3 4 alphabetical order

1	2	3	4
A	P	P	S
s	y	s	t
e	m	u	p
d	a	t	e

don't consider spaces

"sedymasutpe"

if redundant space, put ϕ

Decoding :-

sed	yma	sut	tpe
1	2	3	4
s	y	s	t
e	m	u	p
d	a	t	e

" system update "