ITC

→ **Chinese Remainder Theorem**

$X = a_1 \pmod{m_1}$ ⟶ Given

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

Given		To find			
a_1	m_1	$M_1 = \frac{M}{m_1}$	M_1^{-1}	$M_1 \times M_1^{-1} = 1 \bmod m_1$	
a_2	m_2	$M_2 = \frac{M}{m_2}$	M_2^{-1}	$M_2 \times M_2^{-1} = 1 \bmod m_2$	$M = m_1 \times m_2 \times m_3$
a_3	m_3	$M_3 = \frac{M}{m_3}$		$M_3 \times M_3^{-1} = 1 \bmod m_3$	

If there's already a value with X

Multiply with its inverse on B.S

$4x = 5 \pmod 9$

$4^{-1} \times 4x = 4^{-1} \times 5 \pmod 9$

$x = 4^{-1} \pmod 9 \times 5 \pmod 9$ [Here treat inverse normally]

Or divide fully by x term if possible

$2x = 6 \pmod{20}$

$2x = 2 \times 3 \pmod{2 \times 10}$

$x = 3 \pmod{10}$

Then solve normally....

→ **GCD (Euclidean Algorithm)**

q r_1 r_2 r

x x

gcd

gcd (_ , _)

bigger r_1

smaller r_2

Q

r_2 r_1

r

→ **Euler's Totient Function**

$\phi(n)$

	Criteria of 'n'	Formula
$\phi(n)$	'n' is prime	$\phi(n) = (n-1)$
	$n = p \times q$	$\phi(n) = (p-1) \times (q-1)$
	'p' & 'q' are primes	
	$n = a \times b$	$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots$
	Either a or b is composite	
	Both are composite	where p_1, p_2 are distinct primes.

→ **Euler's Theorem**

For every positive integer 'a' & 'n' which are said to be relatively prime then $a^{\phi(n)} = 1 \pmod{n}$

→ **Fermat's Little Theorem**

If 'p' is a prime number & 'a' is a positive integers not divisible by 'p' then $a^{p-1} = 1 \pmod{p}$

→ **Modular Arithmetic**

Properties

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$
   $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$
   $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

→ **Fast modular Arithmetic (Modular Exponentiation)**

Type - I : Little difference

Just solve normally (Make use of difference / powers / etc) Get a positive integer answer

Eg. ① $23^3 \bmod 30$ ② $31^{500} \bmod 30$ ③ $242^{829} \bmod 243$
④ $11^7 \bmod 13$

Type 2 - Big difference

Solve using power

raised to 1

raised to 2

raised to 4

Till less than power given in qn.

Obtain one positive integer answer for each power.

Use all these powers to calculate final answer

Eg. ① $88^7 \bmod 187$

② Last two digits of $29^5 \approx 29^5 \bmod 100$

③ $3^{100} \bmod 29$

26
32
78
104

classmate
Date
Page

Cryptography Methods. Use mapping 0 – A, 25 – Z

→ **Caesar Cipher**

$C = (p + k) \bmod 26$ [encrypt]

$p = (c - k) \bmod 26$ [decrypt]

→ **Vigenere Cipher**

① Given plaintext & key

② key is also word (of length = plaintext length)

③ Use each letter mapping of both pt & k

$C = (p + k) \bmod 26$ [encrypt]

$p = (C - k) \bmod 26$ [decrypt]

→ **Affine Cipher**

① Given plaintext & two keys k_1 & k_2

$T = (p \times k_1) \bmod 26$ $\quad p = (T \times k_1^{-1}) \bmod 26$

$C = (T + k_2) \bmod 26$ $\quad T = (C - k_2) \bmod 26$

How to find modular inverse?

$7^{-1} \bmod 26$

$7 \times x \bmod 26 = 1$

$x = 15 \quad \therefore k_1^{-1} = 15$

→ **Row column Transposition Cipher**

① Will be given plaintext, key (optionally no. of columns & rows)

② The key sequence is basically no. of columns

③ Get no. of rows = total / no. of columns

④ Place plaintext row wise (fill last by x y z . .)

⑤ Get ciphertext by reading column wise in key number sequence from 1.

PAGE No.
DATE / /

To decrypt,

① break the cipher & assign key no. from 1

② No. of elements in one column = total / no. of columns
(basically no. of rows)

③ Place them column wise in given key sequence

④ Read row wise to obtain plaintext.