Tutorial

[This Notes are from Tut
For exam follow what
Sir discussed in
class]

$n_1, n_2 \dots n_K$ +ve integers

⇓

co-prime

given congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_K \pmod{n_K}$$

solution $N = \prod n_i$

$$x = \sum_{i=1}^{K} a_i y_i z_i \qquad y_i = N/n_i \qquad z_i \equiv y_i^{-1} \bmod n_i$$

↳ The formula

If solns U, V exists then $\left[n_i \mid (U - V) = 0 \right]$

⇓

$$U \equiv V \pmod{\left(\prod n_i\right)}$$

Question 1

$X \equiv 2 \pmod{3}$

$X \equiv 3 \pmod{5}$

$X \equiv 2 \pmod{7}$

$N = 105$

a_i	y_i	z_i	$\Rightarrow$
2	35	2	1H0
3	21	1	63
2	15	1	30

$\Rightarrow 233$

$X = 233$

Smaller $(X) = 233 \bmod (105)$

$= ((105 \times 2) + (23)) \bmod (105)$

$= 23$

Question 2

Using CRT Find last 2 digits of 49^{19}

Let say $Y \equiv 49^{19} \bmod (100)$

$\gcd(25, 4) = 1$

Let $X \equiv 49^{19} \bmod (25)$

$X \equiv 49^{19} \bmod (4)$

$$X \equiv \left[49^{19} \left(\frac{100}{25}\right)^{4} \left(\left(\frac{100}{25}\right)^{-1} \bmod 25 \right) + 49^{19} \left(\frac{100}{4}\right) \left(\left(\frac{100}{4}\right)^{-} \bmod (4) \right) \right] \bmod (100)$$

$(4)^{-} \bmod 25 = z_1 \Rightarrow 4z_1 = 1 \bmod 25$ $\quad z_1 = 19$ from this 2

$(25)^{-} \bmod 4 = z_2 \Rightarrow 25 z_2 = 1 \bmod 4$ $\quad z_2 = 1$

$$\equiv (49)^{19} (4 \times 19) + (49)^{19} (25) \bmod (100)$$

$$\equiv (49)^{19} (101) \bmod (100)$$

$X \equiv (49)^{19} \pmod{100}$ same as Y

Rewriting $X \equiv (149)^{19} \bmod 25 = 24 \bmod 25$

$X \equiv (149)^{19} \bmod 4 = 1 \bmod 4$

Use CRT now

24	4	19	1824
1	25	1	25

$\Rightarrow (1849) \bmod 100$

$\Rightarrow 49$

Last 2 Digits are 49

If CRT is mentioned do using CRT