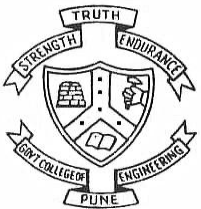


# **Foundation of Cryptography**

## **Session 20**

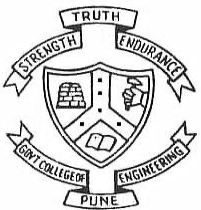
**Date: 17 March 2021**

**Dr. V. K. Pachghare**



**Department of Computer Engineering and Information Technology**  
**College of Engineering Pune (COEP)**  
Forerunners in Technical Education

# Chinese Remainder Theorem



**Department of Computer Engineering and Information Technology**  
**College of Engineering Pune (COEP)**  
Forerunners in Technical Education

### Chinese Remainder Theorem

1. Problem first express as a system of congruences

$$p \equiv b_i \pmod{n_i}$$

where  $n_i$  are relatively prime numbers:  $n_1, n_2, n_3$  and so on

$b_i$  is the respective remainder for modulo  $n_i$  such that  $b_1$  for  $n_1$ ,  $b_2$  for  $n_2$  and so on.

$p$  is the value of solution.

2. Calculate the value of  $N$   $N = n_1 * n_2 * \dots * n_i$

3. Calculate the value of  $N_i = N/n_i$  such that  $N_1 = N/n_1$ ,  $N_2 = N/n_2$  and so on

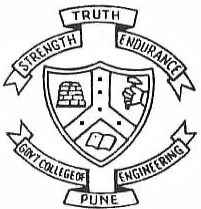
4. Calculate the multiplicative inverse for  $y_i \equiv (N_i)^{-1} \pmod{n_i}$

Where  $y_i$  is the multiplicative inverse of  $N_i \pmod{n_i}$ .

5. The value of  $p$  is calculated as

$$p \equiv (b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r) \pmod{N}$$

where  $p$  is the solution of the problem.



## Solve the simultaneous congruences

$$p \equiv 6 \pmod{11}$$

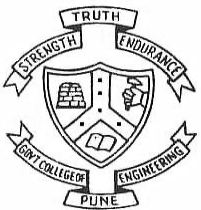
$$p \equiv 13 \pmod{16}$$

$$p \equiv 9 \pmod{21}$$

$$p \equiv 19 \pmod{25}$$

$$N = 11 \times 16 \times 21 \times 25 = 92400$$

$$N_1 = N/11 = 8400$$



# Solve the simultaneous congruences

$$\begin{aligned}p &\equiv 6 \pmod{11} \\p &\equiv 13 \pmod{16} \\p &\equiv 9 \pmod{21} \\p &\equiv 19 \pmod{25}\end{aligned}$$

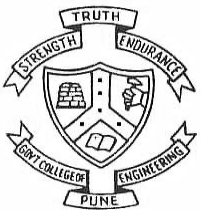
Here  $n_1 = 11$ ,  $n_2 = 16$ ,  $n_3 = 21$  and  $n_4 = 25$   
 $b_1 = 6$ ,  $b_2 = 13$ ,  $b_3 = 9$  and  $b_4 = 19$

$$\begin{aligned}N &= n_1 * n_2 * n_3 * n_4 \\&= 11 \times 16 \times 21 \times 25 \\&= \mathbf{92400}\end{aligned}$$

and find the value of  $N_i = N/n_i$  as below:

$$\begin{aligned}N_1 &= 92400/11 = \mathbf{8400} \\N_2 &= 92400/16 = \mathbf{5775} \\N_3 &= 92400/21 = \mathbf{4400} \\N_4 &= 92400/25 = \mathbf{3696}\end{aligned}$$

$$Y_1=7, Y_2=15, Y_3=11, Y_4=21$$



**Now find out the multiplicative inverse as below:**

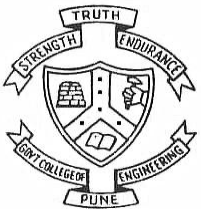
$$y_i \equiv (N_i)^{-1} \pmod{n_i}$$

$$y_1 = (8400)^{-1} \pmod{11} = 8$$

$$y_2 = (5775)^{-1} \pmod{16} = 15$$

$$y_3 = (4400)^{-1} \pmod{21} = 2$$

$$y_4 = (3696)^{-1} \pmod{25} = 6$$



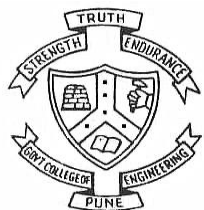
**The solution for above problem is:**

$$P \equiv [b_1 N_1 y_1 + b_2 N_2 y_2 + b_3 (N_3 * y_3) + b_4 (N_4 * y_4)] \text{ mod } N$$

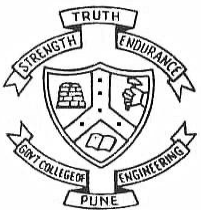
$$\begin{array}{llll} b_1 = 6, & b_2 = 13, & b_3 = 9 & b_4 = 19 \\ N_1 = 8400, & N_2 = 5775, & N_3 = 4400 & N_4 = 3696 \\ y_1 = 8, & y_2 = 15, & y_3 = 2 & y_4 = 6 \end{array} \quad \text{and } N = 92400$$

$$\begin{aligned} &= 6(8400)(8) + 13(5775)(15) + 9(4400)(2) + 19(3696)(6) \text{ mod } 92400 \\ &= 6 \times 67200 + 13 \times 86625 + 9 \times 8800 + 19 \times 22176 \\ &= 2029869 \text{ mod } 92400 \\ &= 89469 \end{aligned}$$

**So the solution is 89469**



An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time, they came out even. What is the smallest number of eggs she could have had?

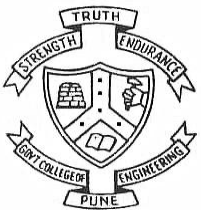




Problem is now expressed as a system of congruence as:

$$p \equiv b_i \pmod{n_i}$$

$$P \equiv 1 \pmod{2}$$

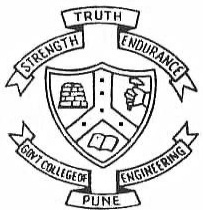


Problem is now expressed as a system of congruence as:

$$p \equiv b_i \pmod{n_i}$$

$$P \equiv 1 \pmod{2}$$

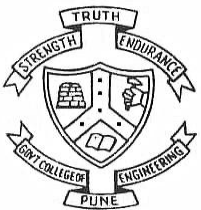
$$P \equiv 1 \pmod{3}$$



$$P \equiv 1 \pmod{2}$$

$$P \equiv 1 \pmod{3}$$

$$P \equiv 1 \pmod{4}$$



$$P \equiv 1 \pmod{2}$$

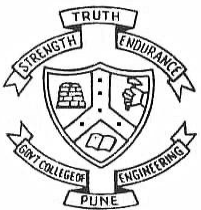
$$P \equiv 1 \pmod{3}$$

$$P \equiv 1 \pmod{4}$$

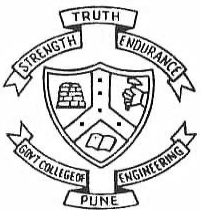
$$P \equiv 1 \pmod{5}$$

$$P \equiv 1 \pmod{6}$$

$$P \equiv 0 \pmod{7}$$



congruence	$b_i$	$n_i$
$P = 1 \pmod{2}$	1	2
$P = 1 \pmod{3}$	1	3
$P = 1 \pmod{4}$	1	4
$P = 1 \pmod{5}$	1	5
$P = 1 \pmod{6}$	1	6
$P = 0 \pmod{7}$	0	7



$$2 = 1 \times 2$$

$$3 = 1 \times 3$$

$$4 = 1 \times 2 \times 2 = 2^2$$

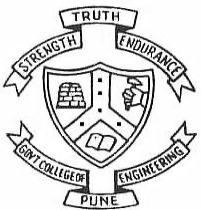
$$5 = 1 \times 5$$

$$6 = 1 \times 2 \times 3$$

$$7 = 1 \times 7$$

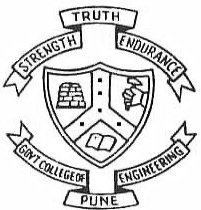
We have to select the factors having highest power.

$$\text{So, } 2^2 = 4$$



congruence	$b_i$	$n_i$	
$P= 1 \pmod{2}$	1	2	<b>Not selected</b>
$P= 1 \pmod{3}$	1	<b>3</b>	
$P= 1 \pmod{4}$	1	<b>4</b>	
$P= 1 \pmod{5}$	1	<b>5</b>	
$P= 1 \pmod{6}$	1	6	<b>Not selected</b>
$P= 0 \pmod{7}$	0	<b>7</b>	

So  $n_i = 3, 4, 5, 7$

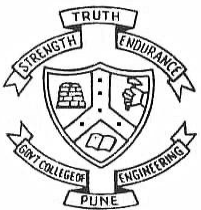


To solve for p we get we first calculate the value of N as

$$n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

$$N = n_3 * n_4 * n_5 * n_7$$

$$N = 3*4*5*7 = 420$$





To solve for p we get we first calculate the value of N as

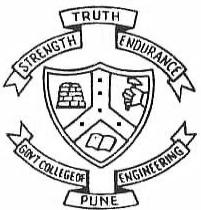
$$N = 420 \text{ and } n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

and find the value of  $N_i = N/n_i$  as below:

$$N_3 = 420/3 = 140;$$

$$N_4 = 420/4 = 105;$$

$$N_5 = 420/5 = 84 ;$$

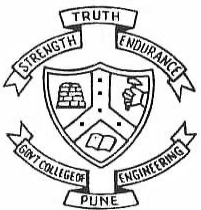


To solve for p we get we first calculate the value of N as

$$N = 420 \text{ and } n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

and find the value of  $N_i = N/n_i$  as below:

$$N_3 = N/n_3 = 420/3 = 140;$$



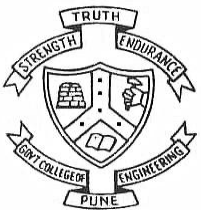
To solve for p we get we first calculate the value of N as

$$N = 420 \text{ and } n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

and find the value of  $N_i = N/n_i$  as below:

$$N_3 = 420/3 = 140;$$

$$N_4 = 420/4 = 105;$$



To solve for p we get we first calculate the value of N as

$$N = 420 \text{ and } n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

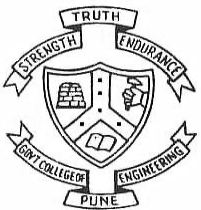
and find the value of  $N_i = N/n_i$  as below:

$$N_3 = 420/3 = 140;$$

$$N_4 = 420/4 = 105;$$

$$N_5 = 420/5 = 84 ;$$

$$N_7 = 420/7 = 60$$



**Now find out the multiplicative inverse as below:**

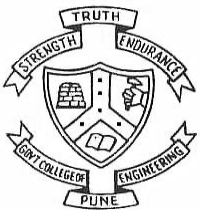
$$y_i \equiv (N_i)^{-1} \pmod{n_i}$$

$$N = 420$$

$$n_3 = 3, \quad n_4 = 4, \quad n_5 = 5, \quad n_7 = 7$$

$$N_3 = 140; \quad N_4 = 105; \quad N_5 = 84; \quad N_7 = 60$$

$$y_3 = (140)^{-1} \pmod{3} = 2$$



**Now find out the multiplicative inverse as below:**

$$y_i \equiv (N_i)^{-1} \pmod{n_i}$$

$$N = 420 \text{ and}$$

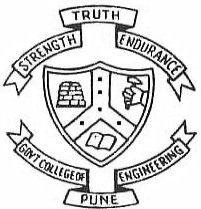
$$n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

$$N_3 = 140; \quad N_4 = 105; \quad N_5 = 84; \quad N_7 = 60$$

$$y_3 = (140)^{-1} \pmod{3} \Rightarrow 140 \pmod{3} = 2 \pmod{3}$$

$$= 2 \times y_3 \pmod{3} = 2 \text{ (here } y_3 \text{ must be 2 so that } 2 \times y_3 \pmod{3} = 1)$$

$$y_4 = (105)^{-1} \pmod{4} = 1$$



**Now find out the multiplicative inverse as below:**

$$y_i \equiv (N_i)^{-1} \pmod{n_i}$$

$$N = 420$$

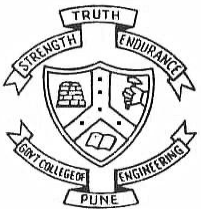
$$n_3 = 3, \quad n_4 = 4, \quad n_5 = 5, \quad n_7 = 7$$

$$N_3 = 140; \quad N_4 = 105; \quad N_5 = 84; \quad N_7 = 60$$

$$y_3 = (140)^{-1} \pmod{3} = 2$$

$$y_4 = (105)^{-1} \pmod{4} = 1$$

$$y_5 = (84)^{-1} \pmod{5} = 4$$



**Now find out the multiplicative inverse as below:**

$$y_i \equiv (N_i)^{-1} \pmod{n_i}$$

$$N = 420$$

$$n_3 = 3, n_4 = 4, n_5 = 5, n_7 = 7$$

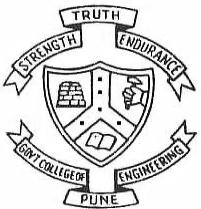
$$N_3 = 140; \quad N_4 = 105; \quad N_5 = 84; \quad N_7 = 60$$

$$y_3 = (140)^{-1} \pmod{3} = 2$$

$$y_4 = (105)^{-1} \pmod{4} = 1$$

$$y_5 = (84)^{-1} \pmod{5} = 4$$

$$~~y_7 = (60)^{-1} \pmod{7} = 2~~ \quad (\text{as } b = 0)$$

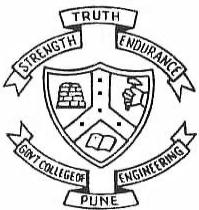




$$P \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r \pmod{N}$$

$b_i$	$N_i$	$y_i$	$N$
1	140	2	420
1	105	1	
1	84	4	
0	60	2	

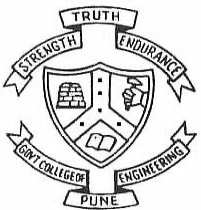
$$p = 1(N_3 * y_3) + 1(N_4 * y_4) + 1(N_5 * y_5) + 0(N_7 * y_7)$$



$$P \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r \pmod{N}$$

$b_i$	$N_i$	$y_i$	$N$
1	140	2	420
1	105	1	
1	84	4	
0	60	2	

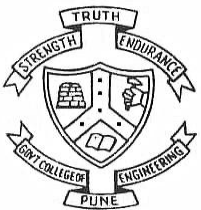
$$\begin{aligned}
 p &= 1(N_3 * y_3) + 1(N_4 * y_4) + 1(N_5 * y_5) + 0(N_7 * y_7) \\
 &= 1(140)(2) + 1(105)(1) + 1(84)(4) + 0(60)(2)
 \end{aligned}$$



$$P \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r \pmod{N}$$

$b_i$	$N_i$	$y_i$	$N$
1	140	2	420
1	105	1	
1	84	4	
0	60	2	

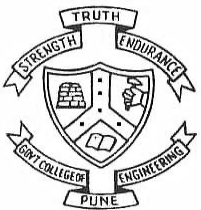
$$\begin{aligned}
 p &= 1(N_3 * y_3) + 1(N_4 * y_4) + 1(N_5 * y_5) + 0(N_7 * y_7) \\
 &= 1(140)(2) + 1(105)(1) + 1(84)(4) + 0(60)(2) \\
 &= 280 + 105 + 336 + 0
 \end{aligned}$$



$$P \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r \pmod{N}$$

$b_i$	$N_i$	$y_i$	$N$
1	140	2	420
1	105	1	
1	84	4	
0	60	2	

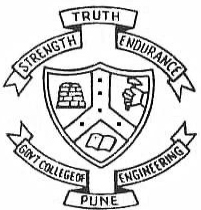
$$\begin{aligned}
 p &= 1(N_3 * y_3) + 1(N_4 * y_4) + 1(N_5 * y_5) + 0(N_7 * y_7) \\
 &= 1(140)(2) + 1(105)(1) + 1(84)(4) + 0(60)(2) \\
 &= 280 + 105 + 336 + 0 \\
 &= 721 \pmod{420}
 \end{aligned}$$



$$P \equiv b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r \pmod{N}$$

$b_i$	$N_i$	$y_i$	$N$
1	140	2	420
1	105	1	
1	84	4	
0	60	2	

$$\begin{aligned}
 p &= 1(N_3 * y_3) + 1(N_4 * y_4) + 1(N_5 * y_5) + 0(N_7 * y_7) \\
 &= 1(140)(2) + 1(105)(1) + 1(84)(4) + 0(60)(2) \\
 &= 280 + 105 + 336 + 0 \\
 &= 721 \pmod{420} \\
 &= \mathbf{301} \text{ -----Solution}
 \end{aligned}$$



# Find a solution using Chinese remainder theorem to $p^2 = 1 \pmod{144}$

$$144 = 16 \times 9 = 2^4 \times 3^2$$

$$\text{GCD}(16, 9) = 1$$

Therefore,

$P^2 = 1 \pmod{16}$  having 4 solutions ( $2^4$  here power is 4)

$P = \pm 1$  or  $\pm 7 \pmod{16}$  ( $b_1 \Rightarrow \pm 1, \pm 7$ )

$P^2 = 1 \pmod{9}$  having 2 solutions ( $3^2$  here power is 2)

$P = \pm 1 \pmod{9}$  ( $b_1 \Rightarrow \pm 1$ )

Obtaining  $b_i = \pm 1, \pm 7$ .

$$p = 1 \pmod{16}$$

$$p = 1 \pmod{16}$$

$$p = -1 \pmod{16}$$

$$p = -1 \pmod{16}$$

$$p = 7 \pmod{16}$$

$$p = 7 \pmod{16}$$

$$p = -7 \pmod{16}$$

$$p = -7 \pmod{16}$$

$$p = 1 \pmod{9}$$

$$p = -1 \pmod{9}$$

$$p = 1 \pmod{9}$$

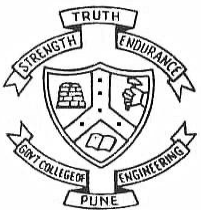
$$p = -1 \pmod{9}$$

$$p = 1 \pmod{9}$$

$$p = -1 \pmod{9}$$

$$p = 1 \pmod{9}$$

$$p = -1 \pmod{9}$$



Department

on Technology

Forerunners in Technical Education

Here  $n_1 = 16$ ,  $n_2 = 9$

Each case has unique solution for  $x \bmod 144$

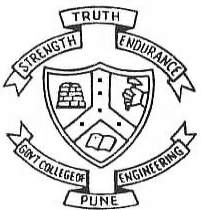
$$b_1 = \pm 1, \pm 7$$

$$\begin{aligned} N &= n_1 * n_2 \\ &= 16 \times 9 \\ &= 144 \end{aligned}$$

and find the value of  $N_i = N/n_i$  as below:

$$N_1 = 144/16 = \mathbf{9}$$

$$N_2 = 144/9 = \mathbf{16}$$



**Now find out the multiplicative inverse as below:**

$$\begin{aligned}y_i &\equiv (N_i)^{-1} \pmod{n_i} \\y_1 &= (9)^{-1} \pmod{16} = 9 \\y_2 &= (16)^{-1} \pmod{9} = 4\end{aligned}$$

**The solution for above problem is:**

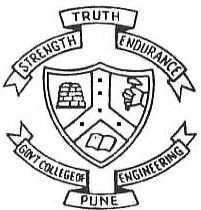
$$P \equiv [b_1 N_1 y_1 + b_2 N_2 y_2] \pmod{N}$$

$$b_i = \pm 1, \pm 7$$

$$\begin{aligned}N_1 &= 9, & N_2 &= 16 \\y_1 &= 9, & y_2 &= 4\end{aligned}$$

$$\begin{aligned}p &= 1(9)(9) + 1(4)(11) \pmod{144} \\&= 81 + 64 \\&= 145 \pmod{144} \\&= 1 \pmod{70}\end{aligned}$$

**So the solution is 1**





$$\begin{aligned} p &= 1(9)(9) + (-1)(4)(16) \bmod 144 \\ &= 81 - 64 \\ &= 17 \bmod 144 \end{aligned}$$

**So the solution is 17**

$$\begin{aligned} p &= -1(9)(9) + (1)(4)(16) \bmod 144 \\ &= -81 + 64 \\ &= -17 \bmod 144 \end{aligned}$$

**So the solution is -17**

$$\begin{aligned} p &= (-1)(9)(9) + (-1)(4)(16) \bmod 144 \\ &= -81 - 64 \\ &= -145 \bmod 144 \end{aligned}$$

**So the solution is -1**

$$\begin{aligned} p &= (7)(9)(9) + (1)(4)(16) \bmod 144 \\ &= 567 + 64 \\ &= 631 \bmod 144 = 55 \bmod 144 \end{aligned}$$

**So the solution is 55**

$$\begin{aligned} p &= (7)(9)(9) + (-1)(4)(16) \bmod 144 \\ &= 567 - 64 \\ &= 503 \bmod 144 = 71 \bmod 144 \end{aligned}$$

**So the solution is 71**

$$\begin{aligned} p &= (-7)(9)(9) + (1)(4)(16) \bmod 144 \\ &= -567 + 64 \\ &= -503 \bmod 144 = -71 \bmod 144 \end{aligned}$$

**So the solution is -71**

$$\begin{aligned} p &= (-7)(9)(9) + (-1)(4)(16) \bmod 144 \\ &= -567 - 64 \\ &= -603 \bmod 144 = -55 \bmod 144 \end{aligned}$$

**So the solution is -55**

$$\mathbf{P = 1, 17, -17, -1, 55, 71, -71, -55}$$

