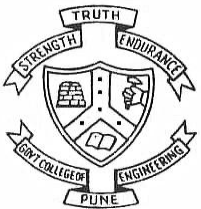


# **Foundation of Cryptography**

## **Session 21**

**Date: 19 March 2021**

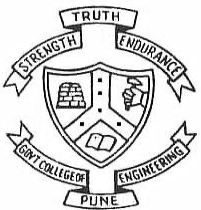
**Dr. V. K. Pachghare**



---

**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

# 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  $\pm 7 \pmod{16}$  ( $b_1 \Rightarrow \pm 1, \pm 7$ )

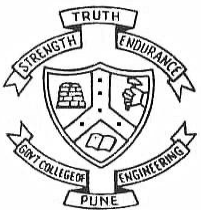
$P^2 = 1 \pmod{9}$  having 2 solutions ( $3^2$  here power is 2)

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

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  $x \bmod 144$

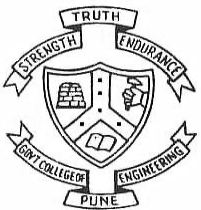
$$b_1 = \pm 1, \pm 7$$

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

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:**

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

**The solution for above problem is:**

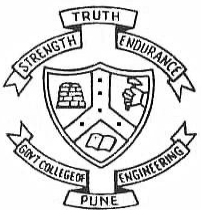
$$P \equiv [b_1 N_1 y_1 + b_2 N_2 y_2] \pmod{N}$$

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

$$N_1 = 9, \quad N_2 = 16$$
$$y_1 = 9, \quad y_2 = 4$$

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

**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**

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

