

Bharathidasan University

Tiruchirappalli - 620 024 Tamil Nadu, India

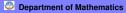
Programme: M.Sc., Mathematics

Course Title :Theory of Numbers COurse Code : 21M04CC

Chinese Remainder Theorem

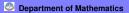
Dr. V. Piramanantham

Professor Department of Mathematics



Chinese Remainder Theorem:
Let
$$m_1, m_2, \dots, m_r$$
 be the integers st.
 $(m_i, m_j) = 1$ it j and let $a_1 a_1 \dots a_r$
be any integers. Then the congruences
 $x \equiv a_1 \pmod{m_1}$
 $x \equiv a_2 \pmod{m_2}$
is
 $z \equiv a_r \pmod{m_r}$
have solutions. If π_0 is one such
solution, then any other solution x is of
the form

$$\begin{aligned} \chi = \chi_0 + km \\ \text{where } m = m_1 m_2 \dots m_r \quad \Delta \quad k \text{ is some integer.} \\ \hline proof: & \left(\frac{m}{m_i}, m_i\right) = 1 \\ \text{Jbi} \quad \in \mathcal{I} \quad \text{st.} \quad \frac{m}{m_i} \text{bi} = 1, i = 1, 2 \dots r \\ \hline \chi_0 = \sum_{i=1}^r \frac{m}{m_i} \text{biai} \\ \chi_0 = a_i \pmod{m_i}. \quad \text{Jti} \quad \frac{m}{m_i} \text{bi} = 0 \pmod{m_j} \\ i = 1, 2 \dots n. \end{aligned}$$



◆□ → ◆□ → ◆ □ → ◆ □ → ● □ □

Theorem Let
$$m_1 \& m_2$$
 denote two
+ve relatively prime integers. Then
 $p(m, m_2) = p(m_1) p(m_2)$
NOTE: $O \supseteq f$ A 4B are finite sets and
 $f: A \Rightarrow B$ is bijective, then $|A| = |B|$.
 $B \supseteq f$ A 4B are finite sets the
 $|A \times B| = |A| |B|$.
 $A \times B = [(x,y)/x \in A, y \in B]$

 $\begin{array}{c|c} \hline (A) & (B) & (C) \\ \hline (M_{1}) & (M_{2}) & (M_{1}) \end{array}$ we establish a 1-1 correspondence AXB~C between AXB&C. $\varphi(m_{i})\varphi(m_{i}) = \varphi(m_{i}m_{j})$ Proof: Let m=m, M2. ve know hot (m) is the no of the integers im that are relatively prime to m $(u) C = \{ c \mid i \leq c \leq m \}, (c, m) = i \}$

Illy
$$A = \int a / 1 \le a \le m_1, (a, m_1) = 1$$

 $B = \int b / 1 \le b \le m_2, (b, m_2) = 1$
 $|A| = Q(m_1), |B| = Q(m_2), |C| = Q(m)$
Proof:
Let $C \in G$. Then by division algorithm
 $\begin{cases} divide \ c \ by \ m_1 \end{cases}$
there exist unique 2, & a st. $0 \le a \le m_1$
 $C = 2, m_1 + a$

< ロ > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > < 0 > <

$$= \int c^{-a} = \xi_{i} m_{i}$$

$$= \int m_{i} c^{-a}$$

$$= \int c \equiv a \pmod{m_{i}}$$

$$= \int c \equiv a \pmod{m_{i}}$$

$$= \int (c, m) = 1$$

$$= \int (a, m_{i}) = 1$$

$$= \int (a, m_{i}) = 1$$

$$\therefore a \in A$$

$$= \int (a \in B)$$

$$= \int (a \in B)$$

For each
$$c \in G$$
 there exists
a unique pair $(a, b) \in A \times B$.
Let $(a, b) \in A \times B$ be any pair
then $(a, m_1) = 1 \quad \& (b, m_2) = 1$.
Griven that m_1, m_2 are relatively primes,
by Ghinese remainder theorem, there

exists integer
$$\chi_0$$
 such that
 $\chi_0 \equiv \alpha \pmod{m_1}$
 $\chi_0 \equiv b \pmod{m_2}$
By division algorithm, there exists
unique c st. $c \equiv \chi_0 \pmod{m}$ $k \circ < c \leq m$
 $\equiv c \equiv \chi_0 \pmod{m_1}$
 $\xi = c \equiv \chi_0 \pmod{m_2}$

▲□▶ ▲圖▶ ▲厘▶ ▲厘▶

$$=) \quad c \equiv a \pmod{m_1}$$

$$c \equiv b \pmod{m_2}$$

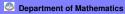
$$(a, m_1) \equiv l \equiv) \quad (c, m_1) \equiv l$$

$$(b, m_2) \equiv l \equiv) \quad (c, m_2) \equiv l$$

$$=j \quad (c, m) \equiv l$$

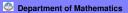
$$\therefore c \in Q$$
For each pair $(a, b) \in A \times B$, there
$$exists \quad unique \quad c \in Q.$$

Hence we have established a
one-one correspondence between C
and
$$A \times B$$
.
 $.|c| = |A \times B|$
 $= |A||B|$
 $\int q(m) = q(m_i) q(m_2)$

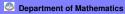


$$\begin{aligned}
f: C \longrightarrow A \times B \\
by f(c) = (a, b) \\
where c \equiv a (mod m_i) \\
c \equiv b (mod m_2) \\
f y bijective \begin{cases} nell defined \\ 1-1 \\
onto \end{cases}$$

$$if k_1 d k_2 are bivo primed, (k_1, k_2) = f k_1; k_1 = k_2 \\
(1 k_1 + k_2) = f k_1; k_1 = k_2 \\
(1 k_1 + k_2) = f k_2; k_1 = k_2
\end{aligned}$$



If
$$p_1 R p_2$$
 are distinct frings, d_1, d_2 are nonnegative
integers, $(p_1^{d_1}, p_2^{d_2}) = I$ (i.e)
 $\vec{p}_1 R p_2^{d_2}$ are relatively primes
(orollary 1: If $m_1 m_2, ..., m_r$ are pairwise
relatively prime integers then
 $Q(m_1 m_2 - -m_r) = Q(m_1) Q(m_2) \cdots Q(m_r).$



・ロン ・四マ ・ヨン ・ヨン

corollary 2: If M=p, p2 --- p, y the canonical factorization of m, when Pipe, ..., Pr are distinct primes $\varphi(m) = \varphi(p_1^{\gamma_1}) \varphi(p_2^{\gamma_2}) - \varphi(p_r^{\gamma_r})$ primo $\varphi(p) = p_{-1}$ 3 p-2, p-1 1, 2,

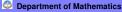
b 26 \$+) (9 b-1 $\varphi(p^2) = p^2 - p = p(p-1)$ $\varphi(p^3) =$ 1 p = 4 b 26 Department of Mathematics 15/21

 $\varphi \varphi(\varphi_{-1}) = \varphi^2(\varphi_{-1})$ $\varphi(p^{3}) = p^{2}(p-r) = p^{3}-p^{2}$ $- q(p^{\prime}) = p^{\prime - 1}(p^{-1})$ $- p^{\prime - 1}(p^{-1})$ d > 0 $\varphi\left(p^{\chi}\right) = p^{\chi} - p^{\chi-1} = p^{\chi-1}(p_{-1})$ э.

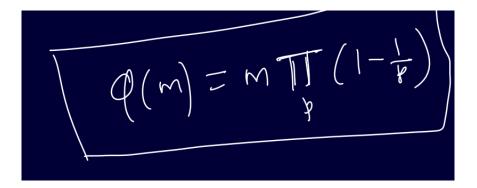


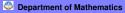
f m=pdip2---pdr is primary decomposition of m $\varphi(m) = \varphi(p_1^{d_1}) \varphi(p_2^{d_2}) \cdots \varphi(p_n^{d_n})$ $= p_{1}^{\prime} (p_{1}^{-1}) p_{2}^{\prime} (p_{2}^{-1}) \cdots p_{r}^{\prime} (p_{r}^{-1})$ $= p_{1}^{\alpha_{1}} p_{2}^{\alpha_{2}} \cdots p_{8}^{\alpha_{r}} \left(\frac{p_{1}^{-1}}{p_{1}} \frac{p_{2}^{-1}}{p_{2}} \cdots \frac{p_{r}^{-1}}{p_{r}} \right)$

 $Tf m = T p^{\alpha}$ $Q(m) = \Pi Q(p')$ = $\frac{1}{1} p^{\alpha-1}(p-1)$ $= TT p^{\alpha} \left(\frac{p-1}{p} \right)$ 1) (I- 1/4) ba



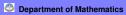
(日)





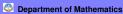
э

Let
$$f(x)$$
 be a polynomial with
integral coefficients.
If m is any tree integers, then
 $N(m)$ denotes the number of
solutions (incongruent) of
 $f(x) \equiv 0 \pmod{m}$



<ロ> <同> <同> <同> < 同> < 同>

Theorem:
$$T \neq m = m_1 m_2$$
 where
 $m_1 & m_2$ are relatively prime integers
then $N(m) = N(m_1) N(m_2)$



◆□ > ◆□ > ◆臣 > ◆臣 > ─ 臣