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 $m_1, m_2 \ldots m_r$ be +ve integers s.t. $(m_i, m_j) = 1$ $i \neq j$ and let $a_1, a_2 \ldots a_r$ be any integers. Then the congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

have solutions. If x_0 is one such solution, then any other solution x is of the form

$$x = x_0 + km$$

where $m = m_1 m_2 \cdots m_r$ & k is some integer.

Proof: $\left(\frac{m}{m_i}, m_i\right) = 1$

$\exists\, b_i \in \mathbb{Z}$ s.t. $\frac{m}{m_i} b_i \equiv 1$, $i = 1, 2, \cdots r$

$$\boxed{x_0 = \sum_{i=1}^{r} \frac{m}{m_i} b_i a_i}$$

$x_0 \equiv a_i \pmod{m_i}$.

$i = 1, 2 \cdots n$.

$j \neq i$ $\quad \frac{m}{m_i} b_i \equiv 0 \pmod{m_j}$

Theorem Let m_1 & m_2 denote two +ve relatively prime integers. Then

$$\phi(m_1 m_2) = \phi(m_1)\,\phi(m_2)$$

Note: ① If A & B are finite sets and $f: A \to B$ is bijective, then $|A| = |B|$.

② If A & B are finite sets, then

$$|A \times B| = |A|\,|B|.$$

$A \times B = \{(x,y) \mid x \in A,\ y \in B\}$

$|A|, |B|, |C|$
$\varphi(m_1) \quad \varphi(m_2) \quad \varphi(m_1 m_2)$

We establish a 1-1 correspondence between $A \times B$ & C.

$A \times B \simeq C$

$\varphi(m_1)\varphi(m_2) = \varphi(m_1 m_2)$

Proof: Let $m = m_1 m_2$.

We know that $\varphi(m)$ is the no. of +ve integers $\leq m$ that are relatively prime to m

(a) $C = \{ c \mid 1 \leq c \leq m, \ (c, m) = 1 \}$

IIIly $A = \{a \mid 1 \le a \le m_1, (a, m_1) = 1\}$

$B = \{b \mid 1 \le b \le m_2, (b, m_2) = 1\}$.

$|A| = \varphi(m_1)$, $|B| = \varphi(m_2)$, $|C| = \varphi(m)$

Proof:

Let $c \in G$. Then by division algorithm

{divide c by m_1}

there exist unique q_1 & a s.t. $\left.\begin{array}{l} 0 < a \le m_1 \\ c = q_1 m_1 + a \end{array}\right\}$

$$\Rightarrow c - a = q_1 m_1$$

$$\Rightarrow m_1 \mid c - a$$

$$\Rightarrow c \equiv a \pmod{m_1}$$

Since $(c, m) = 1$, $(c, m_1) = 1$

$$\Rightarrow (a, m_1) = 1$$

$$\therefore a \in A$$

|||ly there exists unique $b \in B$

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 $(a, m_1) = 1$ & $(b, m_2) = 1$.

Given that m_1, m_2 are relatively primes, by Chinese remainder theorem, there exists integer x_0 such that

$$x_0 \equiv a \pmod{m_1}$$
$$x_0 \equiv b \pmod{m_2}$$

By division algorithm, there exists unique c st. $c \equiv x_0 \pmod{m}$ & $0 < c \leq m$

$$\Rightarrow c \equiv x_0 \pmod{m_1}$$
$$\& \; c \equiv x_0 \pmod{m_2}$$

$$\Rightarrow \quad c \equiv a \pmod{m_1}$$

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

$$(a, m_1) = 1 \Rightarrow (c, m_1) = 1$$

$$(b, m_2) = 1 \Rightarrow (c, m_2) = 1$$

$\underline{m = m_1 m_2}$

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

$$\therefore c \in G$$

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

Hence we have established a one-one correspondence between C and $A \times B$.

$$\therefore |C| = |A \times B|$$

$$= |A|\,|B|$$

$$\boxed{\varphi(m) = \varphi(m_1)\,\varphi(m_2)}$$

$$\left\{\begin{array}{l} f : C \longrightarrow A \times B \\ \text{by } f(c) = (a, b) \\ \text{where } \quad c \equiv a \pmod{m_1} \\ \qquad\qquad c \equiv b \pmod{m_2} \\ f \text{ is bijective} \end{array}\right. \quad \left\{\begin{array}{l} \text{well-defined} \\ 1-1 \\ \text{onto} \end{array}\right.$$

If p_1 & p_2 are two primes, $(p_1, p_2) = \begin{cases} p_1 ; & p_1 = p_2 \\ 1 & p_1 \neq p_2 \end{cases}$

If p_1 & p_2 are distinct primes, α_1, α_2 are nonnegative integers,

$$(p_1^{\alpha_1}, p_2^{\alpha_2}) = 1 \quad (\text{ie})$$

$p_1^{\alpha_1}$ & $p_2^{\alpha_2}$ are relatively primes

<u>Corollary 1</u>: If $m_1, m_2, \ldots, m_r$ are pairwise relatively prime integers then

$$\phi(m_1 m_2 \cdots m_r) = \phi(m_1)\,\phi(m_2)\cdots\phi(m_r).$$

Corollary 2: If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is the canonical factorization of m, when $p_1, p_2, \ldots, p_r$ are distinct primes

$$\varphi(m) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_r^{\alpha_r})$$

p is prime $\quad \varphi(p) = p-1$

$$1, 2, 3, \ldots\ldots, p-2, p-1, \cancel{p}$$

$$\varphi(p^2)$$

$$\underbrace{1, 2, 3, \dots, p-1}_{p-1}, \cancel{p}, \underbrace{p+1, \dots}_{p-1}, (2p-1), \cancel{2p}, 2p+1, \dots \cancel{3p}, \dots$$

$$(\dots\dots), \cancel{(p-1)p}, \dots\dots (p^2-1), \cancel{p^2}$$

$$\varphi(p^2) = p^2 - p = p(p-1)$$

$$\varphi(p^3) =$$

$$1 \dots\dots p^2 \; (p^2+1 \dots, \dots 2p^2) \dots \; (p^3-(p-1) \dots p^3-1, p^3)$$

$$p\,p(p-1) = p^2(p-1)$$

$$\varphi(p^3) = p^2(p-1) = p^3 - p^2$$

$\alpha \geq 0$

$$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$$

$$= p^\alpha - p^{\alpha-1}$$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ is primary decomposition of m

$$\varphi(m) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \cdots \varphi(p_\alpha^{\alpha_r})$$

$$= p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}\left(\frac{p_1 - 1}{p_1}\,\frac{p_2 - 1}{p_2} \cdots \frac{p_r - 1}{p_r}\right)$$

If $m = \prod p^{\alpha}$,

$$\varphi(m) = \prod \varphi(p^{\alpha})$$

$$= \prod p^{\alpha-1}(p-1)$$

$$= \prod p^{\alpha}\left(\frac{p-1}{p}\right)$$

$$= \left(\prod p^{\alpha}\right) \prod \left(1 - 1/p\right)$$

$$\boxed{\phi(m) = m\prod_{p}\left(1-\frac{1}{p}\right)}$$

Let $f(x)$ be a polynomial with integral coefficients.

If m is any +ve integers, then $N(m)$ denotes the number of solutions (incongruent) of

$$f(x) \equiv 0 \pmod{m}$$

Theorem: If $m = m_1 m_2$ where m_1 & m_2 are relatively prime integers then

$$N(m) = N(m_1)\, N(m_2)$$