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

Let $f(x)$ be the polynomial with integral coefficien

Theorem Let $m = m_1 m_2$, where m_1 & m_2 are relatively primes. If $N(m)$ denotes the no. of solution of $f(x) \equiv 0 \pmod{m}$, then

$$N(m) = N(m_1) N(m_2).$$

Proof Let $\mathcal{C}(m) = \{1, 2, \ldots m\}$. Then $\mathcal{C}(m)$ is a complete residue system $\pmod{m}$.

$N(m)$ is the number of solutions of $f(x) \equiv 0 \pmod m$ in $\mathcal{C}(m)$.

Let $A = \{a \in \mathcal{C}(m) \mid f(a) \equiv 0 \pmod m\}$

$$A_i = \{a_i \in \mathcal{C}(m_i) \mid f(a_i) \equiv 0 \pmod{m_i}\} \quad i = 1, 2.$$

So $|A| = N(m)$, $|A_1| = N(m_1)$ & $|A_2| = N(m_2)$

To prove the result it is enough to

$$A \cong A_1 \times A_2.$$

Let $a \in A$. Then $f(a) \equiv 0 \pmod{m}$

since $m_i \mid m$, $i = 1, 2$,

$$f(a) \equiv 0 \pmod{m_i}$$

Since $\mathcal{C}(m_i)$ is a complete residue system $\pmod{m_i}$

$\exists!\, a_i \in \mathcal{C}(m_i)$ s.t. $a \equiv a_i \pmod{m_i}$

$$\Rightarrow f(a_i) \equiv 0 \pmod{m_i}$$

$$a_i \in A_i, \quad i = 1, 2$$

Thus for each $a \in A$, there corresponds a unique pair (a_1, a_2) in $A_1 \times A_2$.

Suppose that $(a_1, a_2) \in A_1 \times A_2$.

Then $$f(a_1) \equiv 0 \pmod{m_1}$$
$$f(a_2) \equiv 0 \pmod{m_2}.$$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

Given that $(m_1, m_2) = 1$.

Then by Chinese remainder theorem

$\exists$ unique $a \in \mathcal{C}(m)$ such that

$$a \equiv a_i \pmod{m_i}, \quad i = 1, 2.$$

$$\Rightarrow f(a) \equiv 0 \pmod{m_i}, \quad i = 1, 2.$$

x_0 soln
$x_0 \pmod m$
$\downarrow \div m$
$a \in \mathcal{C}(m)$
unique

$$\Rightarrow f(a) \equiv 0 \pmod{m}$$

$\therefore a \in A.$

We have established a one-one correspondence between A and $A_1 \times A_2$.

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

Note: $a_1, a_2, \dots, a_n$

$$f(x) \equiv 0 \pmod{m} \quad \text{---} \; (1)$$

$m = m_1 m_2$, $(m_1, m_2) = 1$ $\qquad$ $1 < m_1 < m$, $1 < m_2 < m$

$b_1, b_2, \dots, b_r \rightarrow f(x) \equiv 0 \pmod{m_1}$

$c_1, c_2, \dots, c_s \rightarrow f(x) \equiv 0 \pmod{m_2}$

$$\boxed{n = rs}$$

(b_i, c_j), $i = 1, 2, \ldots r$
$j = 1, 2, \ldots s$

Apply the Chinese remainder theorem on

$$\left.\begin{aligned} x &\equiv b_i \pmod{m_1} \\ x &\equiv c_j \pmod{m_2} \end{aligned}\right\} \text{ — } (2)$$

we find a solution $a_{ij} \pmod{n}$

satisfying (1)

$$\boxed{n = rs}$$

Note: $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_2}$ canonical factorization

$i \neq j \quad (p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$

As a generalization of the previous theorem,

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

$$\boxed{f(x) \equiv 0 \pmod{p_i^{\alpha_i}}} \longrightarrow f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$$

If a_i is a solution of $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ $i = 1, 2, \cdots r$,

$(a_1, a_2, \ldots, a_r)$

CRT − find $a \equiv a_i \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \cdots r$

a is a soln of $f(x) \equiv 0 \pmod{m}$

Polynomial congruence with prime power moduli

Solve the congruence

$$x^3 + 2x - 3 \equiv 0 \pmod{45}$$

$$\mathscr{C}(5) = \{0, 1, 2, 3, 4\}$$

$$45 = 5 \cdot 9$$

$$x^3 + 2x - 3 \equiv 0 \pmod{5}$$

has the solutions 1 and 3

$$x^3 + 2x - 3 \equiv 0 \pmod{9}$$

has the solutions 1, 2, 6,

$$\mathscr{C}(9) = \{0, 1, 2, 3, \cdots 9\}$$

$A = ?$

$$A_1 = \{1, 3\}$$

$$A_2 = \{1, 2, 6\}$$

$1 \pmod 9$ $\quad A_2$

(mod 5) A_1

	1	2	6
1	1	11	6
3	28	38	33

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 9 \end{cases}$$

$\Downarrow$ CRT

$$f(x) \equiv 0 \pmod{45}$$

$$|A_1 \times A_2| = 6$$

$$\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 9 \end{cases}$$

$m = 45$

$\frac{m}{m_i} \quad b_i \quad a_i$

$$x_0 = 9 \cdot 4 \cdot 1 + 5 \cdot 2 \cdot 2 = 36 + 20$$

$$11^3 + 2 \cdot 11 - 3 \equiv 0 \pmod{45}$$

$$11^3 + 2 \cdot 11 - 3 = 121 \cdot 11 + 22 - 3 = 31 \cdot 11 + 19$$

$$= 31 \cdot 11 + 19$$
$$= 341 + 19$$
$$= 360$$
$$\equiv 0 \pmod{45}$$

$$= 36 + 20$$
$$= 56 \pmod{45}$$

$$x_0 = 11$$

CRT on $x \equiv 1 \pmod 5$ $\quad x \equiv 6 \pmod 9$

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2$$
$$= 9 \cdot 4 \cdot 1 + 5 \cdot 2 \cdot 6$$
$$= 36 + 60 = 96 \pmod{45}$$
$$= 6$$

CRT $\quad x \equiv 3 \pmod 5 \quad x \equiv 1 \pmod 9$

$$x_0 = 9 \cdot 4 \cdot 3 + 5 \cdot 2 \cdot 1$$
$$= 36 \cdot 3 + 10$$
$$= 108 + 10 = 118 \equiv 28 \pmod{45}$$

CRT $\quad x \equiv 3 \pmod 5 \quad x \equiv 2 \pmod 9$

$$x_0 = 9 \cdot 4 \cdot \underline{3} + 5 \cdot 2 \cdot \underline{2}$$
$$= 108 + 20 = 128$$
$$\equiv 38 \pmod{45}$$

CRT $\quad x \equiv 3 \pmod 5 \quad x \equiv 6 \pmod 9$

$$x_0 = 9 \cdot 4 \cdot 3 + 5 \cdot 2 \cdot 6$$
$$= 108 + 60 = 168$$
$$\equiv 33 \pmod{45}$$

The solutions of $x^3 + 2x - 3 \equiv 0 \pmod{45}$ are $1, 6, 11, 28, 33, 38$.

EXERCISE:

(1) Solve the congruence

$$x^3 + 4x + 8 \equiv 0 \pmod{15}$$

method: $x^3 + 4x + 8 \equiv 0 \pmod{3} \xrightarrow{\text{soln}}$

$\pmod{5} \xrightarrow{\text{soln}}$

CRT $\quad x \equiv a_1 \pmod{3} \quad x \equiv a_2 \pmod{5}$

$m = 15$

$$x_0 = \frac{m}{m_1} b_1 a_1 + \frac{m}{m_2} b_2 a_2$$

$$= 5 \cdot 2 a_1 + 3 \cdot 6 a_2$$

$5 \cdot b_1 \equiv 1 \pmod{3}$ $\qquad x_6 = 10 a_1 + 18 a_2$

$3 \cdot \cancel{b_2} \equiv 1 \pmod{5}$

2

$$x_6 = 10 a_1 + 18 a_2$$