Lecture 41

06 December 2021 16:55

Chinese Remainder Theorem

THE CHINESE REMAINDER THEOREM Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

$x \% m_1 = a_1 \longrightarrow x \to 0$ to $m_1 - 1$

$x \% m_2 = a_2$

$x \to 0$ to $m_1 m_2 \ldots m_n - 1$

$x \% m_n = a_n$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo m to this solution.)

Methodology

(i) Find $m = m_1 m_2 \ldots m_k$

(ii) Find $M_k = \frac{m}{m_k}$

(iii) Find inverse of M_k $modulo$ $m_k = y_k$

(iv) $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_k M_k y_k$ is a solution of $x = a_k (\text{mod } m_k)$

Q22. Solve

(i) $x \equiv 2 \ (mod\ 3)$

$x \equiv 3 \ (mod\ 5)$

$x \equiv 2 \ (mod\ 7)$

$m_1 = 3$ $\quad m_2 = 5$ $\quad m_3 = 7$

$a_1 = 2$ $\quad a_2 = 3$ $\quad a_3 = 2$

$m = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{105}{3} = 35$, $\quad M_2 = \frac{105}{5} = 21$, $\quad M_3 = \frac{105}{7} = 15$

Inverse of 35 mod. 3, $\quad$ Inverse of 21 mod 5, $\quad$ Inverse of 15 mod 7

Inverse of 2 mod 3 $\quad$ Inverse of 1 mod 5 $\quad$ Inverse of 1 mod 7

$3 \mid 2y_1 - 1$ $\quad 5 \mid 1 \cdot y_2 - 1$ $\quad 7 \mid 1 \cdot y_3 - 1$

$y_1 = 2$

$3 \mid 2y_1 - 1$ $\quad 5 \mid 1 \cdot y_2 - 1$ $\quad 7 \mid 1 \cdot y_3 - 1$

$y_1 = 2$ $\quad y_2 = 1$ $\quad y_3 = 1$

$$x \equiv (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \bmod 105$$

$x \equiv (233) \bmod 105$, $\quad x \equiv 23 \bmod 105$

(ii) $x \equiv 2 \ (mod\ 3)$
$x \equiv 1 \ (mod\ 4)$
$x \equiv 3 (mod\ 5)$

m

$a_1 = 2$ $\quad a_2 = 1$ $\quad a_3 = 3$

$m_1 = 3$ $\quad m_2 = 4$ $\quad m_3 = 5$

$$m = 3 \cdot 4 \cdot 5 = 60$$

$M_1 = \frac{60}{3} = 20$, $\quad M_2 = \frac{60}{4} = 15$, $\quad M_3 = \frac{60}{5} = 12$

Inverse of 20 mod 3 $\quad$ Inverse of 15 mod 4 $\quad$ Inverse of 12 mod 5

Inverse 2 mod 3 $\quad$ Inverse of 3 mod 4 $\quad$ Inverse of 2 mod 5

$3 \mid 2y_1 - 1$ $\quad 4 \mid 3y_2 - 1$ $\quad 5 \mid 2y_3 - 1$

$y_1 = 2$ $\quad y_2 = 3$ $\quad y_3 = 3$

$$x \equiv (2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3) \bmod 60$$

$x \equiv 233 \bmod 60$, $\quad x \equiv 53 \bmod 60$

(iii) $x \equiv 7 (mod\ 9)$
$x \equiv 4 (mod\ 12)$
$x \equiv 16 (mod\ 21)$

Not Relatively Prime.

$9 = 3^2$ Prime Involved 3

$12 = 2^2 \cdot 3$ " 2, 3

$21 = 3 \cdot 7$ " 3, 7

$x \equiv 7 \bmod 3$, $\quad x \equiv 1 \bmod 3$

$x \equiv 4 \ (mod\ 2)$, $\quad x \equiv 0 \bmod 2$

$x \equiv 4 \pmod 2$, $x \equiv 0 \bmod 2$

$x \equiv 4 \pmod 3$ $x \equiv 1 \bmod 3$

$x \equiv 16 \pmod 3$ $x \equiv 1 \bmod 3$

$x \equiv 16 \pmod 7$ $x \equiv 2 \bmod 7$

$21 = 3 \cdot 7)$

$x \equiv 1 \bmod 3$

$x \equiv 0 \bmod 2$

$x \equiv 2 \bmod 7$

$a_1 = 1$ $a_2 = 0$ $a_3 = 2$

$m_1 = 3$ $m_2 = 2$ $m_3 = 7$

$m = 3 \cdot 2 \cdot 7 = 42$

$M_1 = 14$ $M_2 = 21$ $M_3 = 6$

Inverse of $14 \bmod 3$ | Inverse of $21 \bmod 2$ | Inverse of $6 \bmod 7$

$2 \bmod 3$ | $1 \bmod 2$ | $6 \bmod 7$

$3 \mid 2y_1 - 1$ | $2 \mid y_2 \cdot 1 - 1$ | $7 \mid y_3 6 - 1$

$y_1 = 2$ | $y_2 = 1$ | $y_3 = 6$

$x \equiv (1 \cdot 14 \cdot 2 + 0 \cdot 21 \cdot 1 + 2 \cdot 6 \cdot 6) \bmod 42$, $x \equiv 16 \bmod 42$

Theorem 12:

FERMAT'S LITTLE THEOREM If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod p.$$

Furthermore, for every integer a we have

$$a^p \equiv a \pmod p.$$

$p \to$ prime

$p \nmid a$

Q23. Evaluate

(i)

7^{121} **mod** 13.

$p = 13 \to$ prime $\quad 13 \nmid 7$

$7^{12} \equiv 1 \text{ mod } 13$,

$(7^{12})^{10} \equiv (1)^{10} \text{ mod } 13$

$7^{120} \equiv 1 \text{ mod } 13$

$7^{121} \equiv 7 \text{ mod } 13$

(ii)

23^{1002} **mod** 41.

$41 \to$ prime, $\quad 41 \nmid 23$

$(23)^{40} \equiv 1 \text{ mod } 41$, $\quad (23)^{1000} \equiv 1 \text{ mod } 41$

$(23)^{1002} \equiv (23)^2 \text{ mod } 41$

$(23)^{1002} \equiv 529 \text{ mod } 41$

$(23)^{1002} \equiv 37 \text{ mod } 41$

$$\boxed{23^{1002} \text{ mod } 41 = 37}$$

(iii)

a) Use Fermat's little theorem to compute 5^{2003} **mod** 7, 5^{2003} **mod** 11, and 5^{2003} **mod** 13.

b) Use your results from part (a) and the Chinese remainder theorem to find 5^{2003} **mod** 1001. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

(a) 5^{2003} mod 7 , $\quad 5^{6} \equiv 1 \text{ mod } 7$, $\quad 5^{1998} \equiv 1 \text{ mod } 7$

(a) $5^{2003} \bmod 7$, $\quad 5^{6} \equiv 1 \bmod 7$, $\quad 5^{1998} \equiv 1 \bmod 7$

$2003 = \underline{6(333)} + 5$ $\qquad 5^{2003} \equiv 5^{5} \bmod 7$

$$5^{2003} \equiv 3 \bmod 7$$

$5^{2003} \bmod 11$, $\quad 5^{10} \equiv 1 \bmod 11$, $\quad 5^{2000} \equiv 1 \bmod 11$

$$5^{2003} \equiv 5^{3} \bmod 11$$

$$5^{2003} \equiv 4 \bmod 11$$

$5^{2003} \bmod 13$, $\quad 5^{12} \equiv 1 \bmod 13$, $\quad 5^{1992} \equiv 1 \bmod 13$

$2003 = 12(166) + 11$ $\qquad 5^{2003} \equiv 5^{11} \bmod 13$

$= 1992 + 11$

$$5^{2003} \equiv 8 \bmod 13$$

(b) $5^{2003} \bmod 1001$

$1001 = 7 \cdot 11 \cdot 13$

$$\left.\begin{array}{l} 5^{2003} \bmod 7 = 3 \\ 5^{2003} \bmod 11 = 4 \\ 5^{2003} \bmod 13 = 8 \end{array}\right\} \quad \left.\begin{array}{l} x \equiv 3 \bmod 7 \\ x \equiv 4 \bmod 11 \\ x \equiv 8 \bmod 13 \end{array}\right\}$$

$a_1 = 3$ $\qquad a_2 = 4$ $\qquad a_3 = 8$

$m_3 = 13$

$a_1 = 3$ $\quad$ $a_2 = 4$ $\quad$ $a_3 = 8$

$m_1 = 7$ $\quad$ $m_2 = 11$ $\quad$ $m_3 = 13$

$m = 1001$

$M_1 = 143$ $\quad$ $M_2 = 91$ $\quad$ $M_3 = 77$

Inverse of $143 \bmod 7$, $\quad$ Inverse of $91 \bmod 11$, $\quad$ Inverse of $77 \bmod 13$

$3 \bmod 7$ $\quad$ $3 \bmod 11$ $\quad$ $12 \bmod 13$

$7 \mid 3y_1 - 1$ $\quad$ $11 \mid 3y_2 - 1$ $\quad$ $13 \mid 12y_3 - 1$

$y_1 = 5$ $\quad$ $y_2 = 4$ $\quad$ $y_3 = 12$

$$x \equiv (3 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12) \bmod 1001$$

$x \equiv 10993 \bmod 1001$, $\quad$ $x \equiv 983 \bmod 1001$