A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 4EB

Bookmark

Show all steps: ON

Problem

Solving each of the following systems of simultaneous linear congruences; if there is no solution, write "none."

(a) $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 4$; $x = 1 \pmod 5$; $x \equiv 4 \pmod 7$

(b) $6x \equiv 4 \pmod 8$; $10x \equiv 4 \pmod{12}$; $3x \equiv 8 \pmod{10}$

(c) $5x \equiv 3 \pmod 6$; $4x \equiv 2 \pmod 6$; $6x \equiv 6 \pmod 8$

Step-by-step solution

Step 1 of 5

Here, objective is to solve the given system of simultaneous linear congruence's.

Comment

Step 2 of 5

Chinese reminder theorem:

Let $m_1, m_2.....m_p$ are non-zero integers, and relatively prime. Then the system of congruence's $x = a_1 \bmod m_1, x = a_2 \bmod m_2, ...x = a_p \bmod m_p$ has the solution

$x = x_0 \bmod (m_1, m_2, ...m_p)$

Comment

(a)

Consider the pair of congruence

$x = 2(\text{mod } 3), x = 3(\text{mod } 4), x = 1(\text{mod } 5), x = 4(\text{mod } 7)$

The modulo are relatively prime. So we can apply Chinese reminders theorem.

Let $m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7$

$$\begin{aligned} M &= 3 \cdot 4 \cdot 5 \cdot 7 \\ &= 420 \end{aligned}$$

$$\begin{aligned} M_1 &= \frac{M}{m_1} \\ &= \frac{420}{3} \\ &= 140 \end{aligned}$$

$$\begin{aligned} M_2 &= \frac{M}{m_2} \\ &= \frac{420}{4} \\ &= 105 \end{aligned}$$

$$\begin{aligned} M_3 &= \frac{M}{m_3} \\ &= \frac{420}{5} \\ &= 84 \end{aligned}$$

$$\begin{aligned} M_4 &= \frac{M}{m_4} \\ &= \frac{420}{7} \\ &= 60 \end{aligned}$$

$$\begin{aligned} 140y_1 &= 1 \text{ mod } 3 \\ 105y_2 &= 1 \text{ mod } 4 \\ 84y_3 &= 1 \text{ mod } 5 \\ 60y_4 &= 1 \text{ mod } 7 \end{aligned}$$

$$y_1 = 2, y_2 = 1, y_3 = -1, y_4 = 2$$

$$\begin{aligned} x &= 2(140)(2) + 3(105)(1) + 1(84)(-1) + 4(60)(2) \\ &= 56 + 315 - 84 + 480 \\ &= 767 \end{aligned}$$

$$x \equiv 767 \text{ mod } 420$$

Hence, the solution of linear congruence's is $x \equiv 767 \text{ mod } 420$

Comment

(b)

Consider the pair of congruence

$6x = 4(\bmod 8), 10x = 4(\bmod 12), 3x = 8(\bmod 10)$

The modulo are not relatively prime. So we cannot apply Chinese reminders theorem.

$6x = 4(\bmod 8)$
$3x = 2 \bmod 4$
$x = 6 \bmod 4 \text{........}(1)$
$10x = 4(\bmod 12)$

$5x = 2 \bmod 6$
$x = 10 \bmod 6 \text{....}(2)$
$\text{equations } (1) = (2)$
$6 \bmod 4 = 10 \bmod 6$
$6 + 4p = 10 \bmod 6,$
$4p = 4 \bmod 6$
$2p = 2 \bmod 3$
$p = 4 \bmod 3$

Substitute in equation ....(1)

$x = 6 + 4(4 \bmod 3)$
$x = 6 + 16 \bmod 12$
$x = 22 \bmod 12 \text{....}(3)$
$3x = 8(\bmod 10)\text{...}(4)$

equations .....$(3) = (4)$

$22 \bmod 12 = 8 \bmod 10$
$22 + 12k = 8 \bmod 10$
$12k = -4 \bmod 10$
$6k = -2 \bmod 5$
$k = -2 \bmod 5$
$k = 3 \bmod 5$

From equation .....(3)

$x = 22 + 12(3 \bmod 5)$

$x = 22 + 36 \bmod 60$
$x = 58 \bmod 60$

Hence, the solution of linear congruence's is $x = 58 \bmod 60$

Comment

Step 5 of 5

(c)

Consider the pair of congruence

$5x = 3(\bmod 6), 4x = 2(\bmod 6), 6x = 6(\bmod 8)$

The modulo are not relatively prime. So we cannot apply Chinese reminders theorem.

$$5x = 3(\bmod 6)$$
$$x = 15 \bmod 6.............(1)$$
$$4x = 2 \bmod 6$$
$$2x = 1 \bmod 3$$
$$x = 2 \bmod 3........(2)$$
$$(1) = (2)$$
$$15 \bmod 6 = 2 \bmod 3$$
$$15 + 6p = 2 \bmod 3$$
$$6p = -13 \bmod 3$$
$$p = -143 \bmod 3$$
$$p = 1 \bmod 3$$

Substitute in equation ....(1)

$$x = 15 + 6(1 \bmod 3)$$
$$x = 21 \bmod 18.......(3)$$
$$6x = 6 \bmod 8$$
$$3x = 3 \bmod 4$$
$$x = 9 \bmod 4...(4)$$
$$(3) = (4)$$
$$21 + 18k = 9 \bmod 4$$
$$18k = -12 \bmod 4$$
$$9k = -6 \bmod 7$$
$$k = -24 \bmod 7$$
$$k = 4 \bmod 7$$
$$x = 21 + 18(4 \bmod 7)$$

From equation .....(3)

$$x = 21 + 72 \bmod 126$$
$$x = 93 \bmod 126$$

Hence, the solution of linear congruence's is $x = 93 \bmod 126$

Comment