UNIT 4: THEORY OF CONGRUENCE-I

UNIT STRUCTURE

4.1 Learning Objectives
4.2 Introduction
4.3 Congruence: Definitions and Examples
4.4 Basic Properties of Congruence
4.5 Residue System
4.6 Linear Congruence
4.7 Let Us Sum Up
4.8 Answers to Check Your Progress
4.9 Further Reading
4.10 Model Questions

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand the concept of congruence
- performing basic computations
- properties and theorems of congruence
- applications in number theory
- understand the concept of residue systems
- types of residue systems
- understand linear congruence
- existence and uniqueness of solutions of linear congruence
- method for solving linear congruence

4.2 INTRODUCTION

Congruence is a fundamental concept in number theory that describes a relationship between integers based on divisibility. Introduced by Carl Friedrich Gauss in Disquisitiones Arithmeticae (1801), it provides a way to classify numbers with similar remainders when divided by a given integer.

For integers a, b and a fixed positive integer m, we say that a is congruent to b modulo m if m divides the difference $a - b$. This is written as:

$$a \equiv b (mod\ m)$$

This means that a and b leave the same remainder when divided by m. For example, $17 \equiv 5 (mod\ 6)$, since both 17 and 5 leave a remainder when divided by 6.

Congruences are widely used in number theory, cryptography and computer science. They simplify calculations, especially in modular arithmetic and form the basis of divisibility rules, the Chinese Remainder Theorem, and Fermat's Little Theorem.

Understanding congruence allows mathematicians to solve problems related to divisibility, prime numbers and integer solutions to equations efficiently making it a powerful tool in mathematical problem solving.

4.3 CONGRUENCE: DEFINITIONS AND EXAMPLES

Definition 4.3.1 Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m, symbolized by

$$a \equiv b(mod\ m)$$

if m divides the difference $a - b$; i.e., $a - b = km$ for some integer k.

Examples: (i) $24 \equiv 3\ (mod\ 7)$ because $7|24 - 3$
(ii) $8 \equiv 3\ (mod\ 5)$ because $5|8 - 3$
(iii) $-8 \equiv 6\ (mod\ 2)$ because $2| - 8 - 6$
(iv) $20 \equiv -4\ (mod\ 6)$ because $6|20 - (-4)$

When $m \nmid a - b$, we say that a is incongruent to b, and in this case we write $a \not\equiv b\ (mod\ m)$.

Examples: (i) $5 \not\equiv 3(mod\ 4)$ because $4 \nmid 5 - 3$
(ii) $25 \not\equiv 12(mod\ 7)$ because $7 \nmid 25 - 12$

Definition 4.3.2 Given an integer a, let q and r be its quotient and remainder upon division by m, so that

$$a = qm + r, \qquad 0 \leq r < m$$

Then by definition of congruence, $a \equiv r\ (mod\ m)$. Because there are m choices for r, we see that every integer is congruent modulo m to exactly one of the values $0, 1, 2, 3, \dots, m - 1$; in particular $a \equiv 0\ (mod\ m)$ if and only if $m|a$. The set of m integers $0, 1, 2, \dots, m - 1$ is called the set of least non-negative residues modulo m.

For example, $0, 1, 2, 3, 4$ is the set of least nonnegative residues modulo 5.

4.4 BASIC PROPERTIES OF CONGRUENCE

Theorem 4.4.1 Let $m > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a\ (mod\ m)$

(b) If $a \equiv b\ (mod\ m)$, then $b \equiv a\ (mod\ m)$

(c) If $a \equiv b\ (mod\ m)$ and $b \equiv c\ (mod\ m)$, then $a \equiv c\ (mod\ m)$

(d) If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$ and $ac \equiv bd \ (mod\ m)$

(e) If $a \equiv b \ (mod\ m)$, then $a + c \equiv b + c \ (mod\ m)$ and $ac \equiv bc \ (mod\ m)$

(f) If $a \equiv b \ (mod\ m)$, then $a^n \equiv b^n \ (mod\ m)$ for any positive integer n.

Proof: (a) For any integer a,

$$m|a - a$$

Therefore $a \equiv a \ (mod\ m)$

(b) Let

$$a \equiv b \ (mod\ m)$$
$$\Rightarrow m|a - b$$
$$\Rightarrow m|b - a$$
$$\Rightarrow b \equiv a \ (mod\ m)$$

(c) Let $a \equiv b \ (mod\ m)$ and $b \equiv c \ (mod\ m)$

$\Rightarrow m|a - b$ and $m|b - c$

$$\Rightarrow m|(a - b) + (b - c)$$
$$\Rightarrow m|a - c$$
$$\Rightarrow a \equiv c \ (mod\ m)$$

(d) Let $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$

$\Rightarrow m|a - b$ and $m|c - d$

$$\Rightarrow m|(a - b) + (c - d)$$
$$\Rightarrow m|(a + c) - (b + d)$$
$$a + c \equiv b + d \ (mod\ m)$$

We have

$m|a - b$ and $m|c - d$

$\Rightarrow a - b = mk$ and $c - d = ml$ for some integers k and l.

$\Rightarrow a = b + mk$ and $c = d + ml$

$$\Rightarrow ac = (b + mk)(d + ml)$$
$$\Rightarrow ac = bd + mbl + mkd + m^2kl$$
$$\Rightarrow ac - bd = m(bl + kd + mkl)$$
$$\Rightarrow m|ac - bd$$
$$\Rightarrow ac \equiv bd \ (mod\ m)$$

(e) Let $a \equiv b\ (mod\ m)$. We have $c \equiv c\ (mod\ m)$. So using (d), we get $a + c \equiv b + c\ (mod\ m)$ and $ac \equiv bc\ (mod\ m)$.

(f) Let $a \equiv b\ (mod\ m)$. We prove $a^n \equiv b^n\ (mod\ m)$ by induction on n.

Let $P(n)$: $a^n \equiv b^n\ (mod\ m)$.

For $n = 1$, $a \equiv b\ (mod\ m)$, i.e. $P(1)$ is true.

We assume $P(k)$ is true for any positive integer k, i.e. $a^k \equiv b^k\ (mod\ m)$

We have

$a \equiv b\ (mod\ m)$ and $a^k \equiv b^k\ (mod\ m)$

$$\Rightarrow aa^k \equiv bb^k\ (mod\ m) \quad [using\ (e)]$$

$$\Rightarrow a^{k+1} \equiv b^{k+1}\ (mod\ m)$$

Therefore $P(k+1)$ is true. Hence by the principle of mathematical induction, $P(n)$ is true for all positive integer n, i.e. $a^n \equiv b^n\ (mod\ m)$.

Theorem 4.4.2 For arbitrary integers a and b, $a \equiv b\ (mod\ m)$ if and only if a and b leave the same nonnegative remainder when divided by m

Proof: Let $a \equiv b\ (mod\ m)$. Then $m|a - b$

$\Rightarrow a - b = mk$, for some integer k

$$\Rightarrow a = b + mk$$

Let $b = qm + r$, where $o \leq r < m$. Therefore

$$a = b + mk$$
$$= qm + r + mk$$
$$= (q + k)m + r$$

which indicates that a has the same remainder as b.

Conversely, let a and b leave the same non-negative remainder r when divided by n where $o \leq r < m$. i.e. $a = q_1 m + r$ and $b = q_2 m + r$ where $0 \leq r < m$.

Now

$$a - b = (q_1 - q_2)m$$
$$\Rightarrow m|a - b$$
$$\Rightarrow a \equiv b\ (mod\ m)$$

Example 1: Find the remainder obtained by dividing $1! + 2! + 3! + \cdots + 10000!$ by 12.

Solution: Since $4! \equiv 0\ (mod\ 12)$, so $k! \equiv 0\ (mod\ 12)$ for all $k \geq 4$. So

$$1! + 2! + 3! + 4! + \cdots + 10000! \equiv 1 + 2 + 6\ (mod\ 12)$$
$$\equiv 9\ (mod\ 12)$$

Hence the required remainder is 9.

Example 2: Find the remainder when 2^{50} is divided by 7.

Solution: We have

$$2^3 \equiv 1 \ (mod\ 7)$$
$$\Rightarrow (2^3)^{16} \equiv 1^{16} \ (mod\ 7)$$
$$\Rightarrow 2^{48} \equiv 1 \ (mod\ 7)$$
$$\Rightarrow 2^{48}.2^2 \equiv 2^2.1 \ (mod\ 7)$$
$$\Rightarrow 2^{50} \equiv 4 \ (mod\ 7)$$

Hence the required remainder is 4.

Example 3: Give an example to show that $a^2 \equiv b^2 \ (mod\ m)$ need not imply that $a \equiv b \ (mod\ m)$.

Solution: $9^2 \equiv 7^2 \ (mod\ 8)$ but $9 \not\equiv (mod\ 8)$.

Theorem 4.4.3 Let a, b, c be any three integers such that $ac \equiv bc \ (mod\ m)$ and $d = (c, m)$.

Now $d = (c, m) \Rightarrow$ there exists $r, s \in Z$ with $(r, s) = 1$ such that $c = dr, m = ds$.

Also, we have $ac \equiv bc \ (mod\ m)$

$$\Rightarrow m | ac - bc$$
$$\Rightarrow m | adr - bdr$$
$$\Rightarrow m | dr(a - b)$$
$$\Rightarrow \frac{m}{d} | r(a - b)$$
$$\Rightarrow s | r(a - b)$$
$$\Rightarrow s | (a - b) \quad [\because (r, s) = 1]$$
$$\Rightarrow a \equiv b \ (mod\ s)$$
$$\Rightarrow a \equiv b \ \left(mod \frac{m}{d}\right), \qquad where\ \ d = (c, m)$$

Corollary 4.4.4 If $ca \equiv cb \ (mod\ m)$ and $(c, m) = 1$, then $a \equiv b \ (mod\ m)$.

Proof: Let $ca \equiv cb \ (mod\ m)$ and $(c, m) = 1$. Then by theorem 4.4.3

$$a \equiv b \ \left(mod \frac{m}{(c, m)}\right)$$
$$\Rightarrow a \equiv b \ (mod\ m) \quad [\because \ (c, m) = 1]$$

Corollary 4.4.5 If $ca \equiv cb \ (mod\ p)$ and $p \nmid c$, where p is a prime number, then $a \equiv b \ (mod\ p)$.

Proof: Let $ca \equiv cb \ (mod\ p)$ and $p \nmid c$, p is a prime number. Since p is prime and $p \nmid c$, therefore $(p, c) = 1$.

We have

$$ca \equiv cb \ (mod\ p)$$

$$\Rightarrow a \equiv b \ \left(mod \frac{p}{(c,p)}\right)$$

$$\Rightarrow a \equiv b \ (mod\ p) \quad [\because \ (p,c) = 1]$$

Example 4: Show that $33 \equiv 15 \ (mod\ 9)$ implies $11 \equiv 5 \ (mod\ 3)$.

Solution: We have

$$33 \equiv 15 \ (mod\ 9)$$

$$\Rightarrow 3.11 \equiv 3.5 \ (mod\ 9)$$

$$\Rightarrow 11 \equiv 5 \ \left(mod \frac{9}{(3,9)}\right)$$

$$\Rightarrow 11 \equiv 5 \ \left(mod \frac{9}{3}\right) \quad [\because \ (3,9) = 3]$$

$$\Rightarrow 11 \equiv 5 \ (mod\ 3)$$

W CHECK YOUR PROGRESS

Q 1. Show that 41 divides $2^{20} - 1$.

Q 2. Find the remainder when 2^{24} is divided by 17.

Q 3. Find the remainder when 3^{287} is divided by 23.

Q 4. If $a \equiv b \ (mod\ m)$ and the integers a, b, m are all divisible by $d > 0$, then $\frac{a}{d} \equiv \frac{b}{d}\left(mod \frac{m}{d}\right)$.

Q 5. If $a \equiv b \ (mod\ m)$, prove that $\gcd(a, m) = \gcd(b, m)$.

Q 6. Find the remainder when 41^{65} is divided by 7.

Q 7. What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

Q 8. Prove that the integer $53^{103} + 103^{53}$ is divisible by 39, and that $111^{333} + 333^{111}$ is divisible by 7.

Q 9. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients a_i, if $a \equiv b \ (mod\ m)$, then prove that $f(a) \equiv f(b) \ (mod\ m)$.

4.5 RESIDUE SYSTEM

Definition 4.5.1 (Complete Residue System) Let m be a fixed positive integer. A set $\{a_1, a_2, \dots, a_n\}$ of integers is called a complete residue system modulo m written as CRS $(mod\ m)$ if
(i) $a_i \not\equiv a_j\ (mod\ m)$, for each $i \neq j$
(ii) For each integer n there exists a unique a_i such that $n \equiv a_i\ (mod\ m)$
Thus as per above $0, 1, 2, \dots, m-1$ is a CRS $(mod\ m)$.
For example, $\{0, 1, 2, 3, 4\}$ is a CRS $(mod\ 5)$.

Theorem 4.5.2 If k-integers $a_1, a_2, \dots, a_k$ form a CRS $(mod\ m)$, then $m = k$.

Proof: We know that $\{0, 1, 2, \dots, m-1\}$ form a CRS $(mod\ m)$. Hence for each j, $1 \leq j \leq k$ there exists a unique integer i with $0 \leq i \leq m-1$ such that

$$a_i \equiv i\ (mod\ m)$$

Therefore

$$k \leq m \qquad (i)$$

But $\{a_1, a_2, \dots, a_k\}$ is also a CRS $(mod\ m)$, so for each $i,\ 0 \leq i \leq m-1$, there exists a unique $j,\ 1 \leq j \leq k$ such that $i \equiv a_j\ (mod\ m)$
Therefore

$$m \leq k \qquad (ii)$$

From (i) and (ii), we obtain

$$m = k$$

Theorem 4.5.3 If $\{r_1, r_2, \dots, r_m\}$ is a CRS $(mod\ m)$ and if c is any integer, then $\{c + r_1, c + r_2, \dots, c + r_m\}$ is also a CRS $(mod\ m)$.

Proof: We have to prove $c + r_i \not\equiv c + r_j (mod\ m)$. Since r_i and r_j are elements of a CRS $(mod\ m)$. So

$$r_i \not\equiv r_j\ (mod\ m)$$
$$\Rightarrow m \nmid r_i - r_j$$
$$\Rightarrow m \nmid (c + r_i) - (c + r_j)$$
$$\Rightarrow c + r_i \not\equiv c + r_j\ (mod\ m)$$

Let n be any integer. Since $\{r_1, r_2, \dots, r_m\}$ is a CRS $(mod\ m)$, therefore $n \equiv r_i (mod\ m)$, for some $r_i \in \{r_1, r_2, \dots, r_m\}$. Since c is any integer, so there exists $r_j \in \{r_1, r_2, \dots, r_m\}$ such that $n \equiv c + r_j (mod\ m)$ where $r_i \equiv c + r_j\ (mod\ m)$.
Hence $\{c + r_1, c + r_2, \dots, c + r_m\}$ is a CRS $(mod\ m)$.

Definition 4.5.4 (Reduced Residue System) The set of integers $\{a_1, a_2, \dots, a_k\}$ is called a reduced residue system or RRS $(mod\ m)$ if
(i) $(a_i, m) = 1$ for all $1 \leq i \leq k$
(ii) $a_i \not\equiv a_j\ (mod\ m)$ for $i \neq j$

(iii) If n is an integer relative prime to m, then $n \equiv a_i \ (mod\ m)$, for a unique a_i in $\{a_1, a_2, \dots, a_k\}$.
For example, for any prime p, $\{0, 1, 2, \dots, p-1\}$ is a CRS $(mod\ p)$ and the set $\{1, 2, \dots, p-1\}$ is a RRS $(mod\ p)$.

Example Show that $\{1, 5, 7, 11\}$ is a RRS $(mod\ 12)$.
Solution: Clearly, conditions of the definition of RRS are satisfied. Let n be any integer relatively prime to 12, i.e. $(n, 12) = 1$. Then by division algorithm,

$$n = 12q + r, \quad 0 \le r < 12$$
$$\Rightarrow n - r = 12q, \qquad 0 \le r < 12$$
$$\Rightarrow 12 | n - r, \quad 0 \le r < 12$$
$$\Rightarrow n \equiv r \ (mod\ 12), \quad 0 \le r < 12$$

Since $(r, 12) = (n, 12) = 1$, so $r = 1$ or 5 or 7 or 11 and hence $n \equiv 1$ or 5 or 7 or 11 $(mod\ 12)$. Thus $\{1, 5, 7, 11\}$ is a RRS $(mod\ 12)$.

W CHECK YOUR PROGRESS

Q 10. Show that the set $\{49, 20, 10, 17, -18, -27\}$ is CRS $(mod\ 6)$.

Q 11. Show that the set $\{-19, -1, 22, 43, 46, 79, 113, 452\}$ is a RRS $(mod\ 15)$.

Q 12. For each positive integer n we define a number $\phi(n)$ as

$$\phi(n) = \begin{cases} 1, & if\ n = 1 \\ the\ number\ positive\ integers\ relatively\ prime\ to\ n, if\ n > 1 \end{cases}$$

ϕ is known as Euler's ϕ-function. If $\{a_1, a_2, \dots, a_k\}$ form a RRS $(mod\ m)$, then $k = \phi(m)$.

4.6 LINEAR CONGRUENCE

Definition 4.6.1 (Linear Congruence) An expression of the form $ax \equiv b \ (mod\ m), a \not\equiv 0 \ (mod\ m)$ is called a linear congruence modulo m.

Definition 4.6.2 (Diophantine Equation) The term Diophantine equation is applied to any equation of one or more unknowns that is to be solved in the integers. The simplest type of Diophantine equation that we shall consider is the linear Diophantine equation in two unknowns:

$$ax + by = c$$

where a, b, c are given integers and a, b are not both zero.

Lemma 4.6.3 The linear Diophantine equation $ax + by = c$ admits a solution if and only if $d | c$, where $d = (a, b)$. If (x_0, y_0) is any particular solution of this equation, then all other solutions are given by

$x = x_0 + \left(\frac{b}{d}\right)t$ and $y = y_0 - \left(\frac{a}{d}\right)t$, where $t \in Z$.

Proof: Proof will be given in unit-5.

Theorem 4.6.4 Let m be a positive integer. The linear congruence $ax \equiv b\ (mod\ m)$ has a solution if and only if $d|b$, where $d = \gcd(a, m)$. If $d|b$, then it has d mutually incongruent solutions modulo m.

Proof: The given linear congruence is

$$ax \equiv b\ (mod\ m)$$
$$\Rightarrow m|ax - b$$
$$\Rightarrow ax - b = my \text{ for some integer } y$$
$$\Rightarrow ax - my = b \qquad (1)$$

Therefore congruence $ax \equiv b\ (mod\ m)$ has a solution $\Leftrightarrow$ the linear Diophantine equation $ax - my = b$ has a solution $\Leftrightarrow d|b$, where $d = (a, m)$.

Also if (x_0, y_0) is a solution of (1), then x_0 is a solution $ax \equiv b\ (mod\ m)$ and the other solutions are given by

$$x = x_0 + \frac{m}{d}t \quad where\ \ 0 \le t \le d - 1$$

We have

$x_0, x_0 + \frac{m}{d}, x_0 + \frac{m}{d}.2, \ldots, x_0 + \frac{m}{d}(d-1)$ are all solutions of $ax \equiv b\ (mod\ m)$.

Let $x_0 + \frac{m}{d}t_i$ and $x_0 + \frac{m}{d}t_j$ be two solutions of $ax \equiv b\ (mod\ m)$ among the above d solutions, $0 \le t_i, t_j \le d - 1$. If possible, let

$$x_0 + \frac{m}{d}t_i \equiv x_0 + \frac{m}{d}t_j\ (mod\ m)$$
$$\Rightarrow \frac{m}{d}t_i \equiv \frac{m}{d}t_j\ (mod\ m)$$
$$\Rightarrow m|\frac{m}{d}(t_i - t_j)$$
$$\Rightarrow d|t_i - t_j$$

which is a contradiction as $0 \le t_i, t_j \le d - 1$. Therefore $x_0 + \frac{m}{d}t_i \equiv x_0 + \frac{m}{d}t_j\ (mod\ m)$ and hence $x_0, x_0 + \frac{m}{d}, x_0 + \frac{m}{d}.2, \ldots, x_0 + \frac{m}{d}\ (d-1)$ are d mutually incongruent solutions of $ax \equiv b\ (mod\ m)$.

We now show that any other solution of the form $x_0 + \frac{m}{d}t$ is congruent modulo m to one of the d congruent solutions of $ax \equiv b\ (mod\ m)$.

Since $t \geq d$, therefore by division algorithm,

$$t = dq + r, \ \ 0 \leq r < d$$

Hence

$$x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(dq + r)$$

$$= x_0 + mq + \frac{m}{d}r$$

$$\equiv x_0 + \frac{m}{d}r \ (mod\ m) \ \ with \ \ 0 \leq r < d$$

Therefore the congruence $ax \equiv b\ (mod\ m\ )$ if admits a solution x_0, then it has d mutually incongruent solutions $x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \dots, x_0 + \frac{(d-1)m}{d}$.

Example 1: Solve $6x \equiv 15\ (mod\ 21)$.

Solution: The given linear congruence is

$$6x \equiv 15\ (mod\ 21)$$

Here $a = 6, b = 15, m = 21$. Therefore $(a, m) = (6, 21) = 3$ and $3|15$. Therefore the given linear congruence has 3 mutually incongruent solutions.

We see that $x_0 = 6$ is a solution of the given congruence. Hence $6, 6 + \frac{21}{3}, 6 + 2 \times \frac{21}{3}$ i.e. $6, 13, 20$ are the 3-incongruent solution $(mod\ 21)$.

Example 2: Solve $39x \equiv 65\ (mod\ 52)$.

Solution: The given congruence is

$$39x \equiv 65\ (mod\ 52)$$

Here $a = 39, b = 65, m = 52$. Therefore $\gcd(39, 52) = 13$ and $13|65$.

Hence the given congruence has 13 mutually incongruent solution $(mod\ 52)$. We have

$$39x \equiv 65 (mod\ 52)$$

$$\Rightarrow 3x \equiv 5 \left(mod\ \frac{52}{\gcd(13, 52)}\right)$$

$$\Rightarrow 3x \equiv 5\ (mod\ 4)$$

We see that $x_0 = 3$ is a solution of the given congruence. Hence $x = x_0 + \frac{52}{13}t = 3 + 4t$, where $t = 0, 1, 2, \dots, 12$ are the incongruent solutions $(mod\ 52)$.

Example 3: Solve $20x \equiv 4\ (mod\ 30)$.

Solution: The given linear congruence is

$$20x \equiv 4 \ (mod \ 30)$$

Here $a = 20, b = 4$ and $m = 30$. Therefore $(20, 30) = 10$ and $10 \nmid 4$. Hence the given congruence $20x \equiv 4 \ (mod \ 30)$ has no solution in Z.

W CHECK YOUR PROGRESS

Q 13. Solve the following linear congruences:

(a) $222x \equiv 12 \ (mod \ 18)$

(b) $207x \equiv 6 \ (mod \ 18)$

(c) $18x \equiv 30 \ (mod \ 42)$

(d) $9x \equiv 21 \ (mod \ 30)$

(e) $12x \equiv 44 \ (mod \ 59)$

(f) $47x \equiv 11 \ (mod \ 249)$

24.7 LET US SUM UP

- **Congruence:** Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m, symbolized by
  $$a \equiv b \ (mod \ m)$$
  if n divides the difference $a - b$; i.e. $a - b = km$ for some integer k. When $m \nmid a - b$, we say that a is incongruent to b, and in this case we write $a \not\equiv b \ (mod \ m)$.
- Let $m > 1$ be fixed and a, b, c, d be arbitrary integers. Then
  (a) $a \equiv a \ (mod \ m)$.
  (b) If $a \equiv b \ (mod \ m)$, then $b \equiv a \ (mod \ m)$.
  (c) If $a \equiv b \ (mod \ m)$ and $b \equiv c \ (mod \ m)$, then $a \equiv c \ (mod \ m)$.
  (d) If $a \equiv b \ (mod \ m)$ and $c \equiv d \ (mod \ m)$, then $a + c \equiv b + d \ (mod \ m)$ and $ac \equiv bd \ (mod \ m)$.
  (e) If $a \equiv b \ (mod \ m)$, then $a + c \equiv b + c \ (mod \ m)$ and $ac \equiv bc \ (mod \ m)$.
  (f) If $a \equiv b \ (mod \ m)$, then $a^n \equiv b^n (mod \ m)$ for any positive integer n.
- For arbitrary integers a and b, $a \equiv b \ (mod \ m)$ if and only if a and b leave the same non-negative remainder when divided by m.
- Let a, b, c be any three integers such that $ac \equiv bc \ (mod \ m)$. Then $a \equiv b \ \left(mod \frac{m}{d}\right)$ where $d = \gcd(c, m)$.
- If $ca \equiv cb \ (mod \ m)$ and $\gcd(c, m) = 1$, then $a \equiv b \ (mod \ m)$.

- If $ca \equiv cb \ (mod\ p)$ and $p \nmid c$, where p is prime number, then $a \equiv b \ (mod\ p)$.

- **Complete Residue System:** Let m be a fixed positive integer. A set $\{a_1, a_2, \dots, a_n\}$ of integers is called a complete residue system modulo m written as CRS $(mod\ m)$ if
  $a_i \not\equiv a_j \ (mod\ m)$, for each $i \neq j$
  For each integer n there exists a unique a_i such that $n \equiv a_i \ (mod\ m)$
- If k-integers $a_1, a_2, \dots, a_k$ forms a CRS (mod m), then $m = k$.
- If $\{r_1, r_2, \dots, r_m\}$ is a CRS $(mod\ m)$ and if c is any integer, then $\{c + r_1, c + r_2, \dots, c + r_m\}$ is also a CRS $(mod\ m)$.
- **Reduced Residue System:** The set of integers $\{a_1, a_2, \dots, a_k\}$ is called a reduced residue system modulo m or RRS $(mod\ m)$ if
  (i) $(a_i, m) = 1$ for all $1 \leq i \leq k$
  (ii) $a_i \not\equiv a_j \ (mod\ m)$ for $i \neq j$
  (iii) If n is an integer relative prime to m, then $n \equiv a_i \ (mod\ m)$, for a unique a_i in $\{a_1, a_2, \dots, a_k\}$.

- **Linear Congruence:** An expression of the form $ax \equiv b \ (mod\ m), a \not\equiv 0 \ (mod\ m)$ is called a linear congruence modulo m.

- Let m be a positive integer. The linear congruence $ax \equiv b \ (mod\ m)$ has a solution if and only if $d|b$, where $d = \gcd(a, m)$. If $d|b$, then it has d mutually incongruent solutions modulo m.

K 4.8 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q 1. We have

$$2^5 \equiv -9 \ (mod\ 41)$$
$$\Rightarrow (2^5)^4 \equiv (-9)^4 \ (mod\ 41)$$
$$\Rightarrow 2^{20} \equiv 81 \times 81 \ (mod\ 41)$$
$$\Rightarrow 2^{20} \equiv (-1)(-1) (mod\ 41)$$
$$\Rightarrow 2^{20} \equiv 1 \ (mod\ 41)$$
$$\Rightarrow 41 | 2^{20} - 1$$

Answer to Q 2. We have

$$2^4 \equiv -1 \ (mod\ 17)$$
$$\Rightarrow (2^4)^6 \equiv (-1)^6 \ (mod\ 17)$$
$$\Rightarrow 2^{24} \equiv 1 \ (mod\ 17)$$

Hence required remainder is 1.

Answer to Q 3. Left as an exercise.

Answer to Q 4. Let $a \equiv b \ (mod\ m)$. Then

$$m|a-b$$
$$\Rightarrow a-b=mk \text{ for some integer } k.$$

Since $d|a, d|b, d|n$, so

$\Rightarrow a=dk_1, b=dk_2, n=dk_3$ for some integers k_1, k_2, k_3 and

$$a-b=mk$$
$$\Rightarrow dk_1-dk_2=(dk_3)k$$
$$\Rightarrow k_1-k_2=kk_3$$
$$\Rightarrow \frac{a}{d}-\frac{b}{d}=k\left(\frac{n}{d}\right)$$
$$\Rightarrow \frac{a}{d}\equiv\frac{b}{d}\left(mod\frac{n}{d}\right)$$

Answer to Q 5. Let $a \equiv b \ (mod\ m)$. Then

$$m|a-b$$
$$\Rightarrow a-b=mk \text{ for some integer } k.$$

Let $\gcd(a,m)=d$. Then there exist r and s with $(r,s)=1$ such that $a=dr$ and $m=ds$.

Now

$$a-b=mk \Rightarrow dr-b=dsk$$
$$\Rightarrow d(r-sk)=b$$
$$\Rightarrow d|b$$

Let $d'=\gcd(b,m)$. Since $d|m$ and $d|b$, so $d \leq d'$.

By similar reasoning as above, $d'|a$ and $d'|m \Rightarrow d' \leq d$

Hence $d=d'$ i.e. $\gcd(a,m)=\gcd(b,m)$.

Answer to Q 6. We have

$$41 \equiv 6 \ (mod\ 7)$$
$$\Rightarrow 41^5 \equiv 6^5 \equiv 7776 \ (mod\ 7)$$
$$\Rightarrow 41^5 \equiv (110\times 7+6)(mod\ 7)$$
$$\Rightarrow 41^5 \equiv 6 \ (mod\ 7)$$
$$\Rightarrow (41^5)^{13} \equiv 6^{13} \ (mod\ 7) \qquad (1)$$

We have

$$6^2 \equiv 1 \ (mod\ 7)$$
$$\Rightarrow (6^2)^6 \equiv 1^6 (mod\ 7)$$
$$\Rightarrow 6^{12} \equiv 1 \ (mod\ 7)$$
$$\Rightarrow 6^{12}.6 \equiv 1.6 \ (mod\ 7)$$
$$\Rightarrow 6^{13} \equiv 6 \ (mod\ 7) \qquad (2)$$

From (1) and (2), we get

$$41^{65} \equiv 6 \ (mod\ 7)$$

Answer to Q 7. We have

$$1^5 \equiv 1 \ (mod\ 4)$$
$$2^5 \equiv 0 \ (mod\ 4)$$
$$3^5 \equiv 3 \ (mod\ 4)$$

$$4^5 \equiv 0\ (mod\ 4)$$

and

$$1 \equiv 5 \equiv 9 \ldots (mod\ 4)$$
$$2 \equiv 6 \equiv 10 \ldots (mod\ 4)$$
$$3 \equiv 7 \equiv 11 \ldots (mod\ 4)$$
$$4 \equiv 8 \equiv 12 \ldots (mod\ 4)$$

Therefore each block of 4 numbers will have same remainder sum.
Since $1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 0 + 3 + 0\ (mod\ 4)$ i.e. $1^5 + 2^5 + 3^5 + 4^5 \equiv 0\ (mod\ 4)$ and the 25 blocks will all have remainder 0, therefore

$$1^5 + 2^5 + 3^5 + \cdots + 100^5 \equiv 0\ (mod\ 4)$$

Answer to Q 8. We have $39 = 3 \times 13, 53 = 3 \times 17 + 2 = 3 \times 18 - 1$ and $103 = 34 \times 3 + 1$
So
$53 \equiv -1\ (mod\ 3)$ and $103 \equiv 1\ (mod\ 3)$
$\Rightarrow 53^{103} \equiv (-1)^{103}\ (mod\ 3)$ and $103^{53} \equiv 1^{53}\ (mod\ 3)$

$$\Rightarrow 53^{103} + 103^{53} \equiv 0\ (mod\ 3)$$

Also $53 \equiv 1\ (mod\ 13)$ and $103 \equiv -1\ (mod\ 13)$
$\Rightarrow 53^{103} \equiv 1\ (mod\ 13)$ and $103^{53} \equiv -1\ (mod\ 13)$
$\Rightarrow 53^{103} + 103^{53} \equiv 0\ (mod\ 13)$
Since $3 \mid 53^{103} + 103^{53}$, $13 \mid 53^{103} + 103^{53}$ and $\gcd(3, 13) = 1$
Therefore

$$3 \times 13 = 39 \mid 53^{103} + 103^{53}$$
$$\Rightarrow 53^{103} + 103^{53} \equiv 0\ (mod\ 39)$$

Second Part: We have

$$111 = 16 \times 7 - 1$$
$$\Rightarrow 111 \equiv -1\ (mod\ 7)$$
$$\Rightarrow 111^{333} \equiv (-1)^{333} (mod\ 7)$$
$$\Rightarrow 111^{333} \equiv -1\ (mod\ 7) \qquad (1)$$

Also, we have

$$333 = 47 \times 7 + 4$$
$$\Rightarrow 333 \equiv 4\ (mod\ 7)$$
$$\Rightarrow 333 \equiv 2^2\ (mod\ 7)$$
$$\Rightarrow 333^{111} \equiv 2^{222} (mod\ 7) \qquad (2)$$

Since $2^6 = 64 = 9.7 + 1$, therefore $2^6 \equiv 1\ (mod\ 7)$

$$\Rightarrow (2^6)^{37} \equiv 1^{37}\ (mod\ 7)$$
$$\equiv 2^{222} \equiv 1\ (mod\ 7) \qquad (3)$$

Using (3) in (2), we get

$$333^{111} \equiv 1\ (mod\ 7) \qquad (4)$$

From (1) and (4), we obtain

$$111^{333} + 333^{111} \equiv 0\ (mod\ 7)$$

Answer to Q 9. Let $a \equiv b\ (mod\ m)$. Then

$$a^k \equiv b^k\ (mod\ m)$$
$$\Rightarrow a_k a^k \equiv a_k b^k\ (mod\ m)$$

Summing these congruences for $k = 0, 1, 2, \dots, n$, we get

$$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \equiv a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n \ (mod\ m)$$
$$\Rightarrow f(a) \equiv f(b) \ (mod\ m)$$

Answer to Q 10. The given set $\{49, 20, 10, 17, -18, -27\}$ is a complete system residue modulo 6 because the set consists of 6 integers whose least residue (mod 6) are $1, 2, 4, 5, 0, 3$ which is a permutation of the number $0, 1, 2, 3, 4, 5, 6$.

Answer to Q 11. We see that the least residues (mod 15) of the integers of the given set $\{-19, -1, 22, 43, 46, 79, 113, 452\}$ are $11, 14, 7, 13, 1, 4, 8, 2$. Also these integers are less than 15 and coprime to 15.

Clearly first two conditions of definition of the reduced residue system are hold directly.

Let n be any integer relatively prime to 15. Then by division algorithm,

$$n = 15q + r, \quad 0 \le r < 15$$
$$\Rightarrow n \equiv r \ (mod\ 15), \qquad 0 \le r < 15$$

Also, we have $(r, 15) = 1$, so $r = 1, 2, 4, 7, 8, 11, 13, 14$. Thus $n \equiv 1, 2, 4, 7, 8, 11, 13$ or $14\ (mod\ 15)$.

Answer to Q 12. Let $t_1, t_2, \dots, t_{\phi(m)}$ be the $\phi(m)$ positive integers that are less than m and relatively prime to m. First, we show $\{t_1, t_2, \dots, t_{\phi(m)}\}$ forms a RRS $(mod\ m)$. If possible, let

$$t_i \equiv t_j (mod\ m), \qquad i \ne j$$
$$\Rightarrow m | t_i - t_j$$
$$\Rightarrow m \le t_i - t_j$$

which is a contradiction as $t_i, t_j \le m$. Thus $t_i \not\equiv t_j \ (mod\ m)$, for all $i \ne j$.

Let a be any integer relatively prime to m, i.e. $(a, m) = 1$.

By division algorithm,

$$a = mq + r, \qquad 0 \le r < m$$
$$\Rightarrow a \equiv r \ (mod\ m), \qquad 0 \le r < m$$

Also $(r, m) = 1$, therefore

$a \equiv t_i (mod\ m)$ for some $i,\ 1 \le i \le \phi(m)$.

Thus $\{t_1, t_2, \dots, t_{\phi(m)}\}$ form a RRS $(mod\ m)$. Then for all $i,\ 1 \le i \le k,\ (a_i, m) = 1, \exists$ a unique $l,\ 1 \le l \le \phi(m)$ such that $a_i \equiv t_l \ (mod\ m)$. Therefore

$$k \le \phi(m) \qquad (1)$$

By the given condition, $\{a_1, a_2, \dots, a_k\}$ is a RRS $(mod\ m)$.

Thus for each $l,\ 1 \le l \le \phi(m), \exists$ a unique $i,\ 1 \le i \le k$ such that $t_l \equiv a_i \ (mod\ m)$. therefore

$$\phi(m) \le k \qquad (2)$$

From (1) and (2), we obtain

$$k = \phi(m)$$

Answer to Q 13. (a) The given linear congruence is

$$222x \equiv 12\ (mod\ 18)$$

Since $222 = 18 \times 12 + 6 \equiv 6\ (mod\ 18)$, so the given congruence becomes

$$6x \equiv 12\ (mod\ 18)$$

Here $(6, 18) = 6$ and $6|12$. So the given congruence has 6 mutually incongruent solutions modulo 18.

Now

$$6x \equiv 12\ (mod\ 18)$$
$$\Rightarrow 6x \equiv 6.2\ (mod\ 18)$$
$$\Rightarrow x \equiv 2\ \left(mod\ \frac{18}{(6, 18)}\right)$$
$$\Rightarrow x \equiv 2\ (mod\ 3)$$

Hence by inspection, $x_0 = 2$ is a particular solution.

The other solutions are given by

$$x = x_0 + \frac{m}{d}t,\ \ 0 \leq t \leq 6 - 1$$
$$= 2 + \frac{18}{6}t,\ \ 0 \leq t \leq 5$$
$$= 2 + 3t,\ \ 0 \leq t \leq 5$$

(b) The given linear congruence is

$$207x \equiv 6\ (mod\ 18)$$

We have $207 = 18 \times 11 + 9 \equiv 9\ (mod\ 18)$. Therefore, the given congruence $207x \equiv 6\ (mod\ 18)$ becomes

$$9x \equiv 6\ (mod\ 18)$$
$$\Rightarrow 3.3x \equiv 3.2\ (mod\ 18)$$
$$\Rightarrow 3x \equiv 2\ \left(mod \frac{18}{(3, 18)}\right)$$
$$\Rightarrow 3x \equiv 2\ (mod\ 6)$$

Here $(3, 6) = 3$ and $3 \nmid 2$

Hence the given linear congruence has no solution in Z.

(c) Left as an exercise.

(d) The given linear congruence is

$$9x \equiv 21\ (mod\ 30)$$

Here $(9, 30) = 3$ and $3|21$. Therefore, given linear congruence has 3 mutually incongruent solutions.

Now, we convert the given congruence into Diophantine equation as follows:

$$30|9x - 21$$
$$\Rightarrow 9x - 21 = 30y, \quad \text{for some integer } y$$
$$\Rightarrow 9x - 30y = 21 \qquad (1)$$
$$\Rightarrow 9x - (9 \times 3 + 3)y = 9 \times 2 + 3$$
$$\Rightarrow 9(x - 3y - 2) - 3y = 3$$
$$\Rightarrow 9u - 3y = 3, \qquad where\ u = x - 3y - 2$$
$$\Rightarrow 3u - y = 1 \qquad (2)$$

Putting $u = 0$ in (2), we get $y = -1$

Putting $y = -1$ in (1), we get

$$9x - 30.(-1) = 21$$
$$\Rightarrow 9x = -9$$
$$\Rightarrow x = -1 \equiv 30 - 1 \ (mod\ 30)$$
$$\therefore \quad x \equiv 29 \ (mod\ 30)$$

Hence $29, 29 + \frac{30}{3}, 29 + \frac{2.30}{3}$ i.e. $29, 39, 49$ are three incongruent solutions.

(e) Left as an exercise.

(f) Left as an exercise.

O 4.9 FURTHER READING

1. David M. Burton, Elementary Number Theory (7th Edn.), McGraw Hill Education (India) Private Limited, Chennai-60016, 2018.

2. S.B. Malik, Basic Number Theory (2nd revised Edn.), Vikas Publishing House Private Limited, Noida-201301, 2017.

3. H. Kishan, Number Theory, Krishna Prakashan Media (P) Ltd., Meerut-250001 (UP), India, 2017.

4. George E. Andrews, Number Theory, Hindustan Publishing Corporation, New Delhi.

5. Hardy, G.H. and Wright, E.M., Theory of Numbers, Oxford Science Publications, 2003.

M 4.10 MODEL QUESTIONS

1. Find the remainder when

(a) 2^{14} is divided by 17.

(b) 11^{35} is divided by 13.

(c) 3^{100} is divided by 5.

2. Show that the set $\{5, 12, -3, -4, 7, 22\}$ form a CRS $(mod\ 6)$.

3. Show that the set $\{5, 11, 17, 23, 29, 35\}$ form a RRS $(mod\ 18)$.

4. Solve the following linear congruences:

(a) $30x \equiv 52 \ (mod\ 49)$

(b) $5x \equiv 2 \ (mod\ 26)$

(c) $17x \equiv 9 \ (mod\ 276)$

(d) $15x \equiv 25 \ (mod\ 35)$

(e) $6x \equiv 15\ (mod\ 21)$

(f) $18x \equiv 30\ (mod\ 42)$

(g) $25x \equiv 10\ (mod\ 29)$

(h) $5x \equiv 2\ (mod\ 26)$

5. Prove the assertions below:

(a) If a is an odd integer, then $a^2 \equiv 1\ (mod\ 8)$

(b) For any integer a, $a^3 \equiv 0, 1\ \ or\ 6\ (mod\ 7)$

(c) For any integer a, $a^4 \equiv 0\ or\ 1\ (mod\ 5)$

6. If $a_1, a_2, \dots, a_n$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $aa_1, aa_2, \dots, aa_n$ is also a CRS $(mod\ n)$.

*** *** ***