CLASS: Msc MATHEMATICS IV SEM

SUBJECT CODE: H-4049
SUBJECT NAME: NUMBER THEORY

TAUGHT BY:DR SATISH KUMAR
ASSOCIATE PROFESSOR
DEPARTMENT OF MATHEMATICS
DN PG COLLEGE MEERUT

Pdf-01 (1) Number Theory | Dr Satish Kr

CH-04 , Theory of congruence

1 Symbol for congruence on set of Integers

$a \equiv b \pmod m$ ⟶ a is congruent to b mod m , m is fixed Integer $a, b \in I$; Integers

$\Rightarrow m \mid (a-b)$

$\Rightarrow \exists$ an Integer k such that $(a-b) = mk$

$\Rightarrow a = b + mk$

Theorem. If $m > 0$, fixed integers , $a, b, c \in I$ then prove

(1) $a \equiv a \pmod m$

(2) If $a \equiv b \pmod m$ then $b \equiv a \pmod m$

(3) If $a \equiv b \pmod m$, $b \equiv c \pmod m$ then $a \equiv c \pmod m$

(4) If $a \equiv b \pmod m$ and $c \equiv d \pmod m$

$\Rightarrow (a+c) \equiv (b+d) \pmod m$

and $ac \equiv bd \pmod m$

(5) If $a \equiv b \pmod m$ then $(a+c) \equiv (b+c) \pmod m$

(6) If $a \equiv b \pmod m$ then $a^k \equiv b^k \pmod m$ for all $k \geq 1$

But if $a^k \equiv b^k \pmod m$ for $k > 2$ then it is not necessarily that $a \equiv b \pmod m$.

Proof. (1) Let $m > 0$, fixed integer , $a, b, c \in I$

We have $a - a = 0$

$a - a = 0 \cdot m$

$\Rightarrow m \mid (a-a)$

$\Rightarrow a \equiv a \pmod m$

(2) if $m>0$, fixed integer

To prove if $a \equiv b \pmod m$
then $b \equiv a \pmod m$

It is given

$$a \equiv b \pmod m$$
$$\Rightarrow m \mid (a-b)$$
$$\Rightarrow m \mid (b-a)$$
$$\Rightarrow b \equiv a \pmod m$$

(3) It is given

$a \equiv b \pmod m$ — (1)
$b \equiv c \pmod m$ — (2)

To prove $a \equiv c \pmod m$

(1) $\Rightarrow$ $m \mid a-b$ — (3)
(2) $\Rightarrow$ $m \mid b-c$ — (4)
(3) & (4) $\Rightarrow$
$\Rightarrow m \mid a-b+b-c$
$\Rightarrow m \mid a-c$
$\Rightarrow a \equiv c \pmod m$

(4) If $a \equiv b \pmod m$ — (1)
$c \equiv d \pmod m$ — (2)

To prove
$(a+c) \equiv (b+d) \pmod m$

(1) $\Rightarrow$ $m \mid a-b$ — (3)
(2) $\Rightarrow$ $m \mid c-d$ — (4)
(3) and (4) $\Rightarrow$
$m \mid a-b+c-d$
$\Rightarrow m \mid (a+c)-(b+d)$
$\Rightarrow (a+c) \equiv (b+d) \pmod m$

Also (3) & (4) $\Rightarrow$

$(a-b) = mr_1 \Rightarrow a = b + mr_1$, $r_1 \in I$

Similarly $c = d + mr_2$, $r_2 \in I$

$ac = (b+mr_1)(d+mr_2)$

$ac = bd + m(r_1 d + mr_1 r_2 + br_2)$

$\Rightarrow ac - bd = m(r_1 d + mr_1 r_2 + br_2)$

$\Rightarrow m \mid (ac-bd)$

$\Rightarrow ac \equiv bd \pmod m$

(v) $a \equiv b \pmod m \Rightarrow m \mid a-b$

$\Rightarrow m \mid (a+c) - (b+c)$

$\Rightarrow a+c \equiv (b+c) \pmod m$.

(vi) $a \equiv b \pmod m$

$\Rightarrow m \mid (a-b)$

$\Rightarrow m \mid (a^k - b^k)$ $\left[\because a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1})\right]$

$\Rightarrow a^k \equiv b^k \pmod m$

Converse is not true

Take $a=8$, $b=4$, $m=3$

i.e $a^2 \equiv b^2 \pmod 3$

i.e $8^2 \equiv 4^2 \pmod 3$

i.e $3 \mid (8^2 - 4^2)$

But $3 \nmid (8-4)$ i.e $8 \not\equiv 4 \pmod 3$

Theorem. If a, b, c are integers such that
$ac \equiv bc \pmod{m}$, $m > 0$, fixed integer
and $d = g.c.d$ of c & m.
then $a \equiv b \pmod{\frac{m}{d}}$.

Proof. Let, a, b, c be any three integers
Let $m > 0$ be fixed integers
if $ac \equiv bc \pmod{m}$, Let $d = (c, m)$
then To prove
$a \equiv b \pmod{\frac{m}{d}}$, $d = g.c.d$ of c and m.

It is given $d = (c, m)$
$\Rightarrow c = dr_1$, $r_1 \in I$
& $m = dr_2$, $r_2 \in I$ such that $(r_1, r_2) = 1$

Also it is given
$ac \equiv bc \pmod{m}$
$\Rightarrow m \mid ac - bc$
$\Rightarrow m \mid (a-b)c$
$\Rightarrow m \mid (a-b)dr_1$ [$\because c = dr_1$]
$\Rightarrow \frac{m}{d} \mid (a-b)r_1$
$\Rightarrow r_2 \mid (a-b)r_1$
$\Rightarrow r_2 \mid (a-b)$ [$\because a \mid bc \Rightarrow a \mid b$ if $(a, c) = 1$]
$\Rightarrow \frac{m}{d} \mid a-b$
$\Rightarrow a \equiv b \pmod{\frac{m}{d}}$, proved.

Theorem 03. Prove that $a \equiv b \pmod m$ iff a and b have the same remainder when divided by m.

Proof. Let $a \equiv b \pmod m$

Let r_1 be the remainder when a is divided by m

$\Rightarrow a = mq_1 + r_1, \quad 0 \le r_1 < m$ — (1)

Let r_2 be the remainder when b is divided by m

$\Rightarrow b = mq_2 + r_2, \quad 0 \le r_2 < m$ — (2)

To prove $r_1 = r_2$

It is given $a \equiv b \pmod m$

$\Rightarrow mq_1 + r_1 \equiv mq_2 + r_2 \pmod m$

$\Rightarrow m \mid (mq_1 + r_1) - (mq_2 + r_2)$

$\Rightarrow m \mid m(q_1 - q_2) + (r_1 - r_2)$

$\Rightarrow m \mid 0 + (r_1 - r_2)$

$\Rightarrow r_1 - r_2$ must be zero as $r_1 < m$, $r_2 < m$, $\Rightarrow r_1 - r_2 < m$

$\Rightarrow r_1 = r_2$

Converse if $r_1 = r_2$

then (1) and (2) $\Rightarrow$

$a = mq_1$

$b = mq_2$

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

$\Rightarrow m \mid (a - b)$

$\Rightarrow a \equiv b \pmod m$, proved.

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

Solution: We have

$$2^1 \equiv 2(\text{mod}41)$$

$$2^2 \equiv 4(\text{mod}41)$$

$$2^3 \equiv 8(\text{mod}41)$$

$$2^4 \equiv 16(\text{mod}41)$$

$$2^5 \equiv -9(\text{mod}41) \quad [a = b + mk \Leftrightarrow a \equiv b(\text{mod}\, m),\ a = 32,\ m = 41,\ k = 1 \Rightarrow b = -9$$

$$2^{20} \equiv [-9(\text{mod}41)]^4 \quad [a \equiv b(\text{mod}\, m) \Rightarrow a^k \equiv b^k(\text{mod}\, m)]$$

$$\equiv (-9)^4(\text{mod}41)$$

$$\equiv 81 \times 81(\text{mod}41)$$

$$\equiv (-1) \times (-1)(\text{mod}41)$$

$$\equiv 1(\text{mod}41)$$

$$2^{20} - 1 \equiv 0(\text{mod}41)$$

$\therefore 2^{20} - 1$ is divisible by 41

Example 2: Find the remainder when 5^{48} is divisible by 24.

Solution: We have

$$5 \equiv 5(\text{mod}24)$$

$$5^2 \equiv 1(\text{mod}24)$$

$$[5^2]^{24} \equiv [1(\text{mod}24)]^{24} \quad [a \equiv b(\text{mod}\, m) \Rightarrow a^k \equiv b^k(\text{mod}\, m)]$$

$$5^{48} \equiv 1^{24}(\text{mod}24)$$

$$5^{48} \equiv 1(\text{mod}24)$$

$\therefore$ When 5^{48} is divided by 24 the remainder is 1

Example 3: Find the remainder when the sum $S = 1! + 2! + 3! + \cdots\cdots + 100!$ is divided by 8.

Solution: We have $1! \equiv 1(\text{mod}8)$, $2! \equiv 2(\text{mod}8)$, $3! \equiv 6(\text{mod}8)$, $4! \equiv 0(\text{mod}8)$ $5! \equiv 0(\text{mod}8)$, $6! \equiv 0(\text{mod}8)$

$\vdots$

$\vdots$

$1000! \equiv 0(\text{mod}8)$

$$\Rightarrow 1! + 2! + 3! + \cdots\cdots + 1000! \equiv 1 + 2 + 6 + 0 + 0 + \cdots\cdots (\text{mod}8)$$
$$\equiv 9(\text{mod}8)$$
$$\equiv 1(\text{mod}8)$$

∴Remainder is 1.

Example 4: Find the remainder when 2^{24} is divided by 17.

Solution: We have

$$2 \equiv 2(\text{mod}17)$$
$$2^2 \equiv 4(\text{mod}17)$$
$$2^3 \equiv 8(\text{mod}17)$$
$$2^4 \equiv -1(\text{mod}17)$$
$$[2^4]^6 \equiv [-1(\text{mod}17)]^6$$
$$2^{24} \equiv (-1)^6(\text{mod}17)$$
$$2^{24} \equiv 1(\text{mod}17) \qquad [(-1)^6 = 1]$$

∴Remainder is 1

Example 5: Find the remainder when 2^{340} is divided by 341.

Solution: We have

$$341 = 11 \times 31$$

$$\therefore 2^1 \equiv 2(\text{mod}11), 2^2 \equiv 4(\text{mod}11)$$

$$2^3 \equiv 8(\text{mod}11), 2^4 \equiv 5(\text{mod}11), 2^5 \equiv -1(\text{mod}11)$$

$$[2^5]^{68} \equiv (-1)^{68}(\text{mod}11)$$

$$2^{340} \equiv 1(\text{mod}11)$$

And

$$2^1 \equiv 2(\text{mod}31)$$

$$2^2 \equiv 4(\text{mod}31)$$

$$2^3 \equiv 8(\text{mod}31)$$

$$2^4 \equiv 16(\text{mod}31)$$

$$2^5 \equiv 1(\text{mod}31)$$

$$\therefore [2^5]^{68} \equiv 1^{68}(\text{mod}31)$$

$$2^{340} \equiv 1(\text{mod}31)$$

$$\therefore 2^{340} \equiv 1(\text{mod}11 \times 31)$$

$$2^{340} \equiv 1(\text{mod}341)$$

$\therefore$ Remainder is 1.

Example 6: Find the remainder when 3^{287} is divided by 23.

Solution: We have

$$287 = 256 + 16 + 8 + 4 + 2 + 1 \quad \text{——— (1)}$$

Now

$$3 \equiv 3 (\text{mod} 23)$$

$$3^2 \equiv 9 (\text{mod} 23) \quad \text{——— (2)}$$

$$3^4 \equiv -11 (\text{mod} 23) \quad \text{——— (3)}$$

$$3^8 \equiv 6 (\text{mod} 23) \quad \text{——— (4)}$$

$$3^{16} \equiv 6^2 (\text{mod} 23)$$

$$\equiv -10 (\text{mod} 23) \quad \text{——— (5)}$$

$$3^{32} \equiv (-10)^2 (\text{mod} 23)$$

$$\equiv 8 (\text{mod} 23)$$

$$3^{64} \equiv 8^2 (\text{mod} 23)$$

$$\equiv -5 (\text{mod} 23)$$

$$3^{128} \equiv (-5)^2 (\text{mod} 23)$$

$$\equiv 2 (\text{mod} 23)$$

$$3^{256} \equiv 2^2 (\text{mod} 23)$$

$$\equiv 4 (\text{mod} 23) \quad \text{——— (6)}$$

$\therefore 3^{287} = 3^{256} \times 3^{16} \times 3^8 \times 3^4 \times 3^2 \times 3$

$$3^{287} \equiv 4 \times (-10) \times 6 \times (-11) \times 9 \times 3 (\text{mod} 23)$$

$$3^{287} \equiv (-40) \times (-66) \times 27 (\text{mod} 23)$$

$$3^{287} \equiv 6 \times 3 \times 4 (\text{mod} 23)$$

$$3^{287} \equiv 24 \times 3 (\text{mod} 23)$$

$$3^{287} \equiv 1 \times 3 (\text{mod} 23)$$

$$3^{287} \equiv 3 (\text{mod} 23)$$

Example 7: What is the remainder when 11^{35} is divided by 13.

Solution: We know that

$$35 = 32 + 2 + 1$$

Now $11 \equiv -2(\text{mod}13)$ ——— (1)

$$11^2 \equiv (-2)^2(\text{mod}13)$$

$$\equiv 4(\text{mod}13) \quad \text{——— (2)}$$

$$11^4 \equiv 4^2(\text{mod}13)$$

$$\equiv 3(\text{mod}13)$$

$$11^8 \equiv 3^2(\text{mod}13)$$

$$\equiv -4(\text{mod}13)$$

$$11^{16} \equiv (-4)^2(\text{mod}13)$$

$$\equiv 3(\text{mod}13)$$

$$11^{32} \equiv 3^9(\text{mod}13)$$

$$\equiv 9(\text{mod}13)$$

$$\equiv -4(\text{mod}13) \quad \text{——— (3)}$$

$\therefore 11^{35} = 11^{32} \times 11^2 \times 11$

$$11^{35} \equiv (-4) \times 4 \times (-2)(\text{mod}13)$$

$$11^{35} \equiv (-16) \times (-2)(\text{mod}13)$$

$$11^{35} \equiv (-3) \times (-2)(\text{mod}13)$$

$$11^{35} \equiv 6(\text{mod}13)$$

$\therefore$ **Remainder = 6**

Example 8: What is the remainder when the sum $1^5 + 2^5 + 3^5 + \cdots\cdots + 100^5$ is divided by 4.

Solution: We have

$$1 + 2 + 3 + \cdots\cdots + 100 = (4n_1 + 1) + (4n_2 + 3) + 2n_3$$

Where

$$n_1 = 0,1,2,3 \ldots\ldots\ldots 24$$

$$n_2 = 0,1,2,3 \ldots\ldots\ldots 24$$

$$n_3 = 1,2,3 \ldots\ldots\ldots 50$$

Now,

For $n_1 = 0,1,2,3 \ldots\ldots\ldots 24$

$$1^5 \equiv 1(\text{mod}4)$$

$$5^5 \equiv 1(\text{mod}4)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$(4n_1 + 1)^5 \equiv 1(\text{mod}4)$$

For $n_2 = 0,1,2,3 \ldots\ldots\ldots 24$

$$3^5 \equiv 3(\text{mod}4)$$

$$7^5 \equiv 3(\text{mod}4)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$(4n_2 + 3)^5 \equiv 3(\text{mod}4)$$

And

For $n_3 = 1,2,3 \ldots\ldots\ldots 50$

$$2^5 \equiv 0(\text{mod}4)$$

$$4^5 \equiv 0(\text{mod}4)$$

$$\vdots$$

$$\vdots$$

$$\vdots$$

$$(2n_3)^5 \equiv 0(\text{mod}4)$$

Now,

$$1^5 + 2^5 + 3^5 + \cdots\cdots + 100^5 = (4n_1 + 1)^5 + (4n_2 + 3)^5 + (2n_3)^5$$

Where

$$n_1 = 0,1,2,3 \ldots\ldots\ldots 24$$

$$n_2 = 0,1,2,3 \ldots\ldots\ldots 24$$

$$n_3 = 1,2,3 \ldots\ldots\ldots 50$$

$$\equiv 25 \times 1(\text{mod}4) + 25 \times 3(\text{mod}4) + 50 \times 0(\text{mod}4)$$

$$\equiv (25 \times 1 + 25 \times 3 + 50 \times 0)(\text{mod}4)$$

$$\equiv 100(\text{mod}4)$$

$$\equiv 0(\text{mod}4)$$

$\therefore$ Remainder $= 0$.

Example 9: What is the remainder when $3^{12} + 5^{12}$ is divided by 13.

Solution: We have

$$3^2 \equiv 9(\text{mod}13)$$

$$3^4 \equiv 9^2(\text{mod}13)$$

$$3^4 \equiv 81(\text{mod}13)$$

$$\equiv 3(\text{mod}13)$$

$$3^{12} \equiv 3^3(\text{mod}13)$$

$$\equiv 27(\text{mod}13)$$

$3^{12} \equiv 1(\text{mod}13)$ ..... (1)

And

$$5^2 \equiv -1(\text{mod}13)$$

$$5^{12} \equiv (-1)^6(\text{mod}13)$$

$5^{12} \equiv 1(\text{mod}13)$ ..... (2)

$(1) + (2)$

$$3^{12} + 5^{12} \equiv 1(\text{mod}13) + 1(\text{mod}13)$$
$$\equiv 1 + 1(\text{mod}13)$$
$$\equiv 2(\text{mod}13)$$

$\therefore$ Remainder $= 2$

Test of divisibility

Let n be any natural number

$n = (\cdots a_3 a_2 a_1 a_0)_{10}$

$n = a_0 \times 10^0 + a_1 \times 10^1 + a_2 10^2 + a_3 10^3 + \cdots$ (Decimal representation of n)

Here a_0 is unit place
a_1 is tenth place
a_2 is Hundred place etc

(1) We say $2 | n$ if 2 divides unit place of n

i.e $2 | n$ if $2 | a_0$

i.e $a_0 \equiv 0 \pmod 2 \Rightarrow 2 | n \iff a_0 \equiv 0 \pmod 2$

This is application of congruence relation

Now

(2) $3 | n \iff 3 | (a_0 + a_1 + a_2 + a_3 + \cdots)$

$\iff 3 | (a_0 + a_1 + a_2 + a_3 \cdots)$

i.e $3 |$ (Sum of all places of n namely unit place, tenth place etc)

Now $(a_0 + a_1 + a_2 + \cdots)$ has come $\cdots 22 \cdots$.

$n = (a_0 \times 10^0 + a_1 10^1 + a_2 10^2 + a_3 10^3 \cdots)$

Final $n \equiv (a_0 + a_1 10 + a_2 10^2 + a_3 10^3 \cdots) \pmod 3$

$\underline{n \equiv (a_0 + a_1 + a_2 + \cdots) \pmod 3} \Rightarrow 3 | n \iff 3 | \sum_{i=0}^{n} a_i$

as $a_1 10 \equiv a_1 \pmod 3$

$a_2 \cdot 10^2 \equiv 100 a_2 \pmod 3$

$a_2 10^2 \equiv a_2 \pmod 3$ and so on

Note (1) n and $(a_0 + a_1 + a_2 + \cdots)$ have the same remainders when divided by 3.

(2) $n \pmod 3 \equiv (a_0 + a_1 + \cdots) \pmod 3$

$a \equiv b \pmod 3$, $a = n$, $b = a_0 + a_1 + \cdots$, Ex $n = 2153$
$\Rightarrow 3 | (3 + 5 + 1)$

(3) $4 \mid n \iff 4 \mid (a_0 + 2a_1)$

$n = a_0 + 10a_1 + 10^2 a^2 + 10^3 a^3 + \cdots$

$n \pmod 4 \Rightarrow (a_0 + a_1 \cdot 10 + a_2 10^2 + a_3 10^3 + \cdots) \pmod 4$

$n \pmod 4 \equiv (a_0 + 2a_1 + 0 + 0 + \cdots) \pmod 4$

$\Rightarrow 4 \mid n$ iff $4 \mid (a_0 + 2a_1)$

[$\because a \equiv b \pmod 4$ ~~have the~~ means a & b have the same remainders when divided by 4.]

i.e $n \equiv (a_0 + 2a_1) \pmod 4$

$\Rightarrow a_0$ is unit place of n

a_1 is tenth place of n.

ex $n = 528$ Here $a_0 = 8$

$a_1 = 2$

ii $a_0 + 2a_1 = 8 + 2 \times 2$

$= 12$

Now $4 \mid n \Rightarrow 4 \mid 528$: etc.

(4) Simulary

$5 \mid n \iff 5 \mid a_0$, a_0 is unit place of n.

(5) $6 \mid n \iff 6 \mid [a_0 + 4(a_1 + a_2 + a_3 + \cdots)]$

i.e $6 \mid [$unit place $+ 4(a_1 + a_2 + a_3 + \cdots)]$

$\Rightarrow a_1 =$ 10th place, a_2 is 10^2th place etc

ex $6 \mid 216$

or $6 \mid [8 + 4(1+2)] \Rightarrow 6 \mid 18$. Here $a_0 = 6$

$a_1 = 1$

$a_2 = 2$

(6) $7 \mid n \iff 7 \mid [(a_2 a_1 a_0) - (a_5 a_4 a_3) + (a_8 a_7 a_6) - \cdots]$

$N = a_2 a_1 a_0 + (a_5 a_4 a_3) 10^3 + (a_8 a_7 a_6)(10^3)^2 + \cdots$

$10^3 \equiv -1 \pmod 7$

Also $10^3 \equiv -1 \pmod{13}$ so $13 \mid n \iff 13 \mid [(a_2 a_1 a_0) - (a_5 a_4 a_3) + \cdots]$

(7) $11 \mid n \iff 11 \mid (a_0 - a_1 + a_2 + a_3 + \cdots)$

$n = a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots$

$n \pmod{11} \equiv (a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots) \pmod{11}$

$10 \equiv -1 \pmod{11}$

$10^2 \equiv 1 \pmod{11}$

$10^3 \equiv -1 \pmod{11}$

$10^4 \equiv 1 \pmod{11}$

$\therefore (a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots) \equiv (a_0 - a_1 + a_2 - a_3 + \cdots) \pmod{11}$

$\Rightarrow 11 \mid n \iff 11 \mid (a_0 - a_1 + a_2 - a_3 + \cdots)$

$11 \mid n \iff 11 \mid \sum_{i=0}^{m} (-1)^i a_i$

(8) $101 \mid n \iff (101) \mid [(a_1 a_0) - (a_3 a_2) + (a_5 a_4) - \cdots]$

(9) $9 \mid n \iff 9 \mid (a_0 + a_1 + a_2 + a_3 + \cdots)$

as $n \equiv (a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 + \cdots) \pmod{9}$

$n \equiv (a_0 + a_1 + a_2 + a_3 + \cdots) \pmod{9}$

as $10 \equiv 1 \pmod{9}$

$10^2 \equiv 1 \pmod{9}$

$10^3 \equiv 1 \pmod{9}$ --- etc.

Explanation of 8 $n = (a_0 + 10a_1) + 10^2 a_2 + 10^3 a_3 + 10^4 a_4 + 10^5 a_5$

$= (a_0 + 10a_1) + 10^2 (a_2 + 10a_3) + 10^4 (a_4 + a_5) + \cdots$

$(a_0 + 10a_1) \pmod{101} \equiv a_0 + 10a_1$

$10^2 \equiv -1 \pmod{101}$

$10^4 \equiv 1 \pmod{101}$ etc.

Let m be a fixed positive integer ($m \geq 1$) Then a set $S = \{a_1, a_2, a_3, \cdots, a_k\}$ of integers is called complete residue system mod m (written as CRS (mod m)) if

(i) $a_i \not\equiv a_j \pmod{m}$ for each $i \neq j$.

(ii) For each integer n there exist a unique a_i;

$n \equiv a_i \pmod{m}$

Ex. $S = \{0, 1, 2, 3, \cdots, (m-1)\}$ is a complete residue system mod m

Here $a_0 = 0, a_1 = 1, a_2 = 2, a_3 = 3, \cdots a_{m-1} = m-1$

We observe that $a_i \not\equiv a_j$ for $i \neq j$

i.e $0 \not\equiv 1 \pmod{m}$

$1 \not\equiv 2 \pmod{m}$ etc Take $m = 3$ or 4 or 5 etc

and $\exists$ a unique n s.t

$n \equiv a_i \pmod{m}$ $(i = m-1)$

Take $m = 4$, $i = 3$

$n \equiv a_3 \pmod{4}$

$n \equiv 3 \pmod{4}$ $\Rightarrow n = 3$

if $n = 7$ then $7 \equiv 3 \pmod{4}$ etc

(2) Show $(5, 12, -3, -4, 7, 22) \pmod{6}$ is CRS

Ans Let $S = \{a_1, a_2, a_3, a_4, a_5, a_6\}$, $m = 6$

$a_1 = 5$, $a_2 = 12$, $a_3 = -3$, $a_4 = -4$, $a_5 = 7$,

$a_6 = 22$

$a_1 \bmod 6 \Rightarrow 5 \bmod 6 = 5 \Rightarrow a_1 = 5 \Rightarrow 5 \equiv 5 \pmod{6}$ — (1)

$a_2 \bmod 6 \Rightarrow 12 \bmod 6 = 0 \Rightarrow 12 \equiv 0 \pmod{6}$ — (2)

$-3 \equiv -3 \pmod{6}$

$-3 \equiv (-3 + 6k) \bmod 6 \Rightarrow -3 + 6k \equiv 3 \pmod{6}$ — (3)

$-4 \equiv -4 \pmod 6$

$-4 \equiv (-4+6k) \pmod 6$

$-4 \equiv 2 \pmod 6$ for $k=1$ — (4)

$7 \equiv 1 \pmod 6$ — (5)

$22 \equiv 4 \pmod 6$ — (6)

$\because$ (1) $\Rightarrow a_1 = 5$ i.e $5 \equiv 5 \pmod 6$

(2) $\Rightarrow a_2 = 0$ i.e $12 \equiv 0 \pmod 6$

(3) $\Rightarrow a_3 = 3$ i.e $-3 \equiv 3 \pmod 6$

(4) $\Rightarrow a_4 = 2$ i.e $-4 \equiv 2 \pmod 6$

(5) $\Rightarrow a_5 = 1$ i.e $7 \equiv 1 \pmod 6$

(6) $\Rightarrow a_6 = 4$ i.e $22 \equiv 4 \pmod 6$

$\therefore (5, 12, -3, -4, 7, 22) \pmod 6$

is equivalent to $(0, 1, 2, 3, 4, 5)$ in some order mod 6.

$\therefore$ Given set S is CRS mod 6.

Note. $(5, 12, -3, -6, 7, 22) \pmod 6$ is a permutation of $\{0, 1, 2, 3, 4, 5\} \pmod 6$.

(3) Show $S = \{49, 20, 10, 17, -18, -27\} \pmod 6$ is CRS

Ans $49 \equiv 1 \pmod 6$ [1 is remainder when 49 is divided by 6]

$20 \equiv 2 \pmod 6$ [2 is remainder when 20 is divided by 6 or $20 = a + 6k \Rightarrow a = 20 - 6k$, $a = 2$ for $k=3$]

$10 \equiv 4 \pmod 6$ [$10 = a + 6k \Rightarrow a = 10 - 6k \Rightarrow a = 4$ for $k=1$]

$17 \equiv 5 \pmod 6$ [$17 = a + 6k \Rightarrow a = 17 - 6k$, $= 5$ for $k=2$]

$-18 \equiv 0 \pmod 6$ [$-18 = a + 6k \Rightarrow a = -18 - 6k$, $a = 0$ for $k=-3$]

$-27 \equiv 3 \pmod 6$ [$-27 = a + 6k \Rightarrow a = -27 - 6k$, $a = 3$, $k = -5$]

$\therefore (0\ 1\ 2\ 3\ 4\ 5) \pmod 6$ is a permutation of S (mod 6)

$\Rightarrow$ S is CRS mod 6.

Reduced residue system. (RRS)

The set $S = \{a_1, a_2, \cdots a_R\}$ is called R.R.S (mod m) if

(1) $(a_i, m) = 1$

(2) $a_i \not\equiv a_j \pmod m$ for all $i \neq j$

(3) if $(n, m) = 1$ then $n \equiv a_i \pmod m$ for unique i.

ex Show $\{1, 5, 7, 11\}$ is RRS (mod 12)

Sol Let $S = \{1, 5, 7, 11\}$ $m = 12$

Here $a_1 = 1, a_2 = 5, a_3 = 7, a_4 = 11$

To show (1) $(a_i, m) = 1$

$(1, 12) = 1$ $(7, 12) = 1$

$(5, 12) = 1$ $(11, 12) = 1$

i.e $(a_1, 12) = 1$
$(a_2, 12) = 1$
$(a_3, 12) = 1$
$(a_4, 12) = 1$

To show $a_i \not\equiv a_j \pmod m$, $\forall\ i \neq j$

Clearly $a_1 \not\equiv a_2 \pmod{12}$ i.e $1 \not\equiv 5 \pmod{12}$

$1 \not\equiv 7 \pmod{12}$

$1 \not\equiv 11 \pmod{12}$

$5 \not\equiv 7 \pmod{12}$

(5) if $(n, m) = 1$ then $n \equiv a_i \pmod m$

ex $m = 12$

Choose n such that $(n, 12) = 1$

Take $n = 13$

Then $13 \equiv a_i \pmod{12} \Rightarrow a_i = 1$

So for each n we can have a_i such that $(n, m) = 1$.

Linear congruence equation

$$ax \equiv b \pmod m, \quad a \neq 0 \qquad \text{---(1)}$$

Let x_0 be a solution of (1), we have

$$ax_0 \equiv b \pmod m$$

$\Rightarrow m \mid (ax_0 - b)$

$\Rightarrow \exists$ an integer y such that

$$ax_0 - b = my$$

$$\Rightarrow ax_0 - my = b \qquad \text{---(2)}$$

which is of the $ax + by = c$ (likewise linear Diophantine eqn)

Soln of (2) exists if $(a, m) \mid b \Rightarrow d \mid b$ if $d = g.c.d$ of a & m

If (x_0, y_0) be initial solution of (2) then its general soln is

$$x_1 = x_0 - \frac{-m}{d}t$$

$$\boxed{x_1 = x_0 + \frac{m}{d}t}$$

$$y_1 = y_0 + \frac{a}{d}t$$

$$\boxed{y_1 = y_0 + \frac{a}{d}t}, \quad t \in I$$

i.e $t = 0, \pm 1, \pm 2, \ldots$

Theorem Prove $ax \equiv b \pmod m$ has incongruent solutions if $d \mid b$ where $d = g.c.d$ of a & m.

Proof Given $ax \equiv b \pmod m$ —— (1)

let $d = (a, m)$ —— (2)

To prove (1) has incongruent solutions

Let (x_0, y_0) be a particular solution of (1)

(1) can be written as

$$ax - my = b \quad \text{—— (3)}$$

(3) has solution if $d \mid b$

put $x = x_0$, $y = y_0$, we have

$ax_0 - my_0 = b \Rightarrow (x_0, y_0)$ is a soln of (3)

general soln of (3) is

$$x_1 = x_0 - \frac{-m}{d}t$$

$$y_1 = y_0 + \frac{a}{d}t$$

$$\Rightarrow x_1 = x_0 + \frac{m}{d}t, \; y_1 = y_0 + \frac{m}{d}t, \; t \in I$$

Let $x = x_0, \; x_0 + \frac{m}{d}, \; x_0 + \frac{2m}{d}, \; x_0 + \frac{3m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$

are d solutions of (3)

To prove these are not congruent

suppose if possible

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod m \quad \text{for } 0 \le t_1 < t_2 \le d-1$$

$$\Rightarrow \frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod m$$

$$\Rightarrow t_1 \equiv t_2 \left(\mod \frac{m}{\frac{m}{d}}\right)$$

$$\Rightarrow t_1 \equiv t_2 \pmod d$$

$\Rightarrow d \mid t_1 - t_2 \Rightarrow d \mid t_2 - t_1 \quad t_2 - t_1 < d.$

which is not possible as

$\therefore$ All solutions are not congruent.

$$\left[\begin{array}{l} ac \equiv bc \pmod m \\ \Rightarrow a \equiv b \left(\mod \frac{m}{d}\right) \\ \text{where } d = (c, m) \end{array}\right]$$

Th. Let $ax \equiv b \pmod m$, $d = (a, m)$ & $d \mid b$ then $ax \equiv b \pmod m$ has exactly d solutions

Proof. Given $ax \equiv b \pmod m$ —— (1)

Let d = g.c.d of a and m

To prove (1) has exactly d incongruent Soln's.

We know $\left(x_0 + \frac{m}{d}t\right)$ is a solution of (1)

$t \in I$, $d \in I^+ \Rightarrow \exists\, q$ & r such that

$t = qd + r$ where $0 \le r < d$

OR

$0 \le r \le (d-1)$

Therefore,

$$x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}[qd + r]$$

$$= x_0 + mq + \frac{mr}{d}$$

ii $\left(x_0 + \frac{m}{d}t\right) \pmod m \equiv \left(x_0 + mq + \frac{mr}{d}\right) \pmod m$

$$\equiv \left(x_0 + \frac{mr}{d}\right) \pmod m$$

As $0 \le r < d$ i.e r has $(d-1)$ values and x_0 is another values

ii $ax \equiv b \pmod m$ has exactly d solutions.