Unit II : Congruences :

Congruences - Solutions of Congruences - The Chinese Remainder theorem - Prime power moduli - Prime modulus.

(Chapter II - Sections : 2.1 to 2.3, 2.6, 2.7)

Sunrise 6-40 AM Sunset 6-14 PM

Definition : 2.1

If an integer m, not zero, divides the difference a-b, then a is said to be Congruent to b modulo m.

Notation : $a \equiv b \pmod{m}$

Note : If a-b is not divisible by m then $a \not\equiv b \pmod{m}$

a-b is divisible by m iff a-b is divisible by -m

Generally we confine our attention to a +ve modulu

Assume modulus m as a positive integer throu' the present chapter

Theorem 2.1 : Let a, b, c, d denote integers. Then

(1) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$ and $a-b \equiv 0 \pmod{m}$ are equivalent statements.

(2) If $a \equiv b \pmod{m}$ & $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$

(3) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv (b+d) \pmod{m}$

(4) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, Then $ac \equiv bd \pmod{m}$

(5) If $a \equiv b \pmod{m}$ and $d \mid m$, $d>0$, then $a \equiv b \pmod{d}$

(6) If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{mc}$ for $c>0$.

Proof:

(1) $a \equiv b \pmod{m} \iff m \mid (a-b)$

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

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

$\iff b \equiv a \pmod{m}$

ie $\frac{a-b}{m} \in \mathbb{Z}$ ie $\frac{a-b}{m} = k$

$a - b = mk$

$a - mk = b$

$\frac{a}{m} - k = \frac{b}{m}$

$\frac{b}{m} = -k + \frac{a}{m}$

$k + \frac{b}{m} = \frac{a}{m}$

Example: $6 \equiv 2 \pmod{4}$

$\frac{6}{4}$ remainder ie 2

$a \equiv a \bmod c$

$\frac{a-a}{c} = 0$

(2) $a \equiv b \pmod m$ & $b \equiv c \pmod m$

$\Rightarrow m \mid a-b$ & $m \mid b-c$

$\Rightarrow a-b = k_1 m$ & $b-c = k_2 m$

$\frac{a-b}{m} = k_1 \in \mathbb{Z}$ & $\frac{b-c}{m} = k_2 \in \mathbb{Z}$

$\Rightarrow a-b+b-c = k_1 m + k_2 m$

$\Rightarrow a-c = (k_1+k_2)m$

$\Rightarrow a-c = km$

$\Rightarrow m \mid a-c$

$\Rightarrow a \equiv c \pmod m$

(3) $a \equiv b \pmod m$ & $c \equiv d \pmod m$

$\Rightarrow m \mid a-b$ & $m \mid c-d$

$\Rightarrow m \mid a-b+c-d$

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

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

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

$\Rightarrow m \mid a-b$, $m \mid c-d$

$\Rightarrow a-b = mx$, $c-d = my$; $x, y \in \mathbb{Z}$

$\Rightarrow a = b+mx$, $c = d+my$

$\Rightarrow ac = (b+mx)(d+my)$

$= bd + bmy + dmx + m^2xy$

$ac = bd + m[by + dx + mxy]$

$ac = bd + m y_1$, $y_1 = bd + dx + mxy$

$\Rightarrow ac - bd = my_1$

$\Rightarrow m \mid ac - bd$

$\Rightarrow ac \equiv bd \pmod m$

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

$\Rightarrow m \mid a - b$ $\qquad d \mid m$

$\Rightarrow a - b = mx$ $\qquad \Rightarrow m = dy$

$\Rightarrow a - b = dyx$ ←

$\Rightarrow a - b = dz$, $z = yx \in Z$

$\Rightarrow d \mid a - b$

$\Rightarrow a \equiv b \pmod d$

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

$\Rightarrow m \mid a - b$

$\Rightarrow a - b = mx$

$\Rightarrow ac - bc = mcx$

$\Rightarrow mc \mid ac - bc$

$\Rightarrow ac \equiv bc \pmod{mc}$

Sunrise 6-38 AM

Theorem 2.2 :

Sunset 6-15 PM

Let 'f' denote a polynomial with integral co-efficients. If $a \equiv b \pmod m$, then

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

Proof :

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_i \in \mathbb{Z}$, $a_n \neq 0$

$$f(a) = a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n$$

$$f(b) = a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$$

W.k.T $a \equiv b \pmod m$, $c \equiv d \pmod m$

$\Rightarrow ac \equiv bd \pmod m$ [$\because$ by property (4) of Theorem 2.1]

$a \equiv b \pmod m$, $a \equiv b \pmod m$

$\Rightarrow a^2 \equiv b^2 \pmod m$

$\Rightarrow a^3 \equiv b^3 \pmod m$

$\vdots$

$a^n \equiv b^n \pmod m$

$\because m \mid 0 \Rightarrow m \mid a_0 - a_0$

$\Rightarrow a_0 \equiv a_0 \pmod m$

Now, $a \equiv b \pmod m$

$\Rightarrow m \mid a-b$

$\Rightarrow m \mid a_1(a-b)$

$\Rightarrow m \mid a_1 a - a_1 b$

Sunrise 6-38 AM

$\Rightarrow a_1 a \equiv a_1 b \pmod{m}$

Now, $a^2 \equiv b^2 \pmod{m}$

$\Rightarrow m \mid a^2 - b^2$

$\Rightarrow m \mid a_2 (a^2 - b^2)$

$\Rightarrow m \mid a_2 a^2 - a_2 b^2$

$\Rightarrow a_2 a^2 \equiv a_2 b^2 \pmod{m}$

$\vdots$

$\Rightarrow a_n a^n \equiv a_n b^n \pmod{m}$

$\therefore a_0 + a_1 a + \cdots + a_n a^n \equiv (a_0 + a_1 b + \cdots + a_n b^n) \pmod{m}$

$f(a) \equiv f(b) \pmod{m}$

Theorem 2.3: (X) Cancellation Theorem

i) $ax \equiv ay \pmod{m}$ iff $x \equiv y \left(\mod \frac{m}{(a,m)} \right)$

ii) If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$

then $x \equiv y \pmod{m}$

iii) $x \equiv y \pmod{m_i}$ for $i = 1, 2 \cdots r$ iff

$x \equiv y \pmod{[m_1, m_2 \cdots m_r]}$

Proof:

i) Part I: Let $ax \equiv ay \pmod{m}$

$\Rightarrow m \mid ax - ay$

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

$\Rightarrow a(x-y) = km \quad , k \in \mathbb{Z}$

$\Rightarrow \frac{a}{d}(x-y) = \frac{km}{d}$ Let $d = (a, m)$

$\Rightarrow \frac{m}{d} \mid \frac{a}{d}(x-y)$

$\Rightarrow \frac{m}{d} \mid (x-y)$

$\Rightarrow x \equiv y \pmod{\frac{m}{d}}$

$\Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$

$\therefore ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$

Part II : Assume $x \equiv y \pmod{\frac{m}{(a,m)}}$

$\Rightarrow x \equiv y \pmod{\frac{m}{d}}$ $d = (a, m)$

$\Rightarrow \frac{m}{d} \mid (x-y)$

$\Rightarrow x - y = k\left(\frac{m}{d}\right)$

$\Rightarrow d(x-y) = km$

$\Rightarrow m \mid d(x-y)$

$\Rightarrow m \mid d(x-y) \cdot \frac{a}{d}$ $\left[\frac{a}{d}\right.$ as an integer as $d \mid a$ $\left.\begin{matrix} d \\ \text{divides} \\ a \end{matrix}\right]$

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

$\Rightarrow m \mid ax - ay$

$\Rightarrow ax \equiv ay \pmod{m}$

(ii) Given $(a, m) = 1$

$ax \equiv ay \pmod{m}$

$\Leftrightarrow x \equiv y \pmod{\frac{m}{(a,m)}}$ [$\because$ by (i)]

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

$\Rightarrow x \equiv y \pmod{m}$

(iii) Part (i)

Assume, $x \equiv y \pmod{m_1}$

$x \equiv y \pmod{m_2}$

⋮

$x \equiv y \pmod{m_r}$

i.e. $m_1 \mid x-y$; $x-y$ is a multiple of m_1

$m_2 \mid x-y$; " " " " " m_2

$\vdots$

$m_r \mid x-y$; " " " " " m_r

Thus, $m_1, m_2, \cdots m_r \mid x-y$

LCM $[m_1, m_2 \cdots m_r] \mid m_1, m_2, \cdots m_r$

$\therefore [m_1, m_2 \cdots m_r] \mid x-y$ [$\because$ by transitive property]

$\therefore x \equiv y \pmod{[m_1, m_2 \cdots m_r]}$

Part (ii) Conversely,

let $x \equiv y \pmod{[m_1, m_2 \cdots m_r]}$

$\Rightarrow [m_1, m_2 \cdots m_r] \mid x-y$

$\Rightarrow m_i \mid x-y \quad \forall\ i = 1, 2 \cdots r$

$\Rightarrow x \equiv y \pmod{m_i} \ \forall\ i = 1, 2 \cdots r.$

Theorem 2.4:

If $b \equiv c \pmod{m}$, Then $(b, m) = (c, m)$

P.T.O

Sunrise 6-37 AM

Proof:

Let $(b, m) = d_1$, $(c, m) = d_2$ ---------- (1)

Then $d_1 \mid b$, $d_1 \mid m$, $d_2 \mid c$, $d_2 \mid m$ ---------- (2)

Given, $b \equiv c \pmod{m}$

$m \mid b-c$ ---------- (3)

From (2) & (3) we have

$d_1 \mid b$, $\{ d_1 \mid m,\ m \mid b-c \}$

$\Rightarrow d_1 \mid b,\ d_1 \mid b-c$

$\Rightarrow d_1 \mid b-(b-c)$

$\Rightarrow d_1 \mid c$

Now, $d_1 \mid m,\ d_1 \mid c \Rightarrow d_1 \mid (c, m)$

$\Rightarrow d_1 \mid d_2$; $\because$ by (1) ---- (4)

$d_2 \mid c,\ d_2 \mid m,\ m \mid b-c$

$\Rightarrow d_2 \mid c,\ d_2 \mid b-c$

$\Rightarrow d_2 \mid c+b-c$

$\Rightarrow d_2 \mid b$

$d_2 \mid b,\ d_2 \mid m \Rightarrow d_2 \mid (b, m)$

$\Rightarrow d_2 \mid d_1$ ---------- (5)

(4) & (5) $\Rightarrow d_1 = d_2$

$\Rightarrow (b, m) = (c, m)$

Sunrise 6-36 AM

Sunset 6-17 PM

Definition 2.2: Residue

If $x \equiv y \pmod{m}$ then y is called a residue of x modulo m.

Complete Residue System: (CRS)

A set $x_1, x_2, \ldots x_m$ is called a complete residue system modulo m if for every integer y there is one and only one $x_j \ni y \equiv x_j \pmod{m}$.

Note:

(i) There are infinitely many CRS modulo m.

eg:- $\{1, 2, \ldots m\}$, $\{0, 1, 2 \ldots m-1\}$

(ii) A set of 'm' integers forms a CRS modulo 'm' iff no two integers in the same set are Congruent modulo m.

Residue Class (Congruence class) modulo m:

Consider a fixed modulo $m > 0$, we denote by $\hat{a}$ or $[a]$, the set of all integers 'x' $\ni$ $x \equiv a \pmod{m}$

and $\hat{a}$ or $[a]$ is called the residue class of a modulo m.

ie $\hat{a} = \{x \mid x \equiv a \pmod{m}\}$

Example:

Let $m = 5$

$\hat{1} = [1] = \{x \mid x \equiv 1 \pmod 5\}$

$= \{1, 6, 11, 16, 21 \ldots -4, -9, -14 \ldots\}$

$\hat{2} = [2] = \{x \mid x \equiv 2 \pmod 5\}$

$= \{2, 7, 12, 17, 22, \ldots -3, -8, \ldots\}$

$\hat{3} = [3] = \{x \mid x \equiv 3 \pmod 5\}$

$= \{3, 8, 13, \ldots -2, -7, \ldots\}$

$\hat{4} = [4] = \{4, 9, 14 \ldots -1, -6, \ldots\}$

$\hat{5} = [5] = = \{5, 10, 15 \ldots 0, -5, -10 \ldots\}$

$\hat{1} \cup \hat{2} \cup \ldots \cup \hat{5} = \{\ldots -4, -3, -2, -1, 0, 1, 2, 3 \ldots\}$

The residue classes are mutually disjoint and their union is 'Z'.

Note: The elements of the residue class $\hat{a}$ are $\hat{a} = \{a + mq \mid q = 0, \pm 1, \pm 2 \ldots\}$

ie The A.P arithmetic progression

A person who sits restraining his working senses while contemplating sense objects deludes himself and is called a hypocrite. – Bhagavad Gita 3:6

$a-3m, a-2m, a-m, a, a+m, a+2m \ldots$

Sunrise 6-34 AM Sunset 6-17 PM

Definition 2.3: Reduced Residue System (RRS)

A reduced residue system modulo m is a set of integers r_i s.t $(r_i, m) = 1$, $r_i \equiv r_j \pmod m$ if $i \neq j$ and s.t $\forall$ x prime to m is congruent modulo m to some member r_i of the set.

i.e $x \equiv r_i \pmod m$

Euler's ϕ function (Totient):

The number of +ve integers $\leq n$ and are (coprime) relatively prime to 'n' is denoted by $\phi(n)$ called Euler's ϕ function.

Examples:

$\phi(1) = 1$; $\phi(2) = 1$; $\phi(3) = 2$; $\phi(4) = 2$

$\phi(5) = 4$; $\phi(6) = 2$; $\phi(7) = 6$.

n	$\phi(n)$	nos. coprime to n	
1	1	1	(1,1)
2	1	1	(1,2)
3	2	1, 2	(1,3) (2,3)
4	2	1, 3	(1,4) ~~(2,4)~~ (3,4)
5	4	1, 2, 3, 4	(1,5) (2,5) (3,5) (4,5)
6	2	1, 5	(1,6) ~~(2,6)~~ ~~(3,6)~~ ~~(4,6)~~ (5,6)
7	6	1, 2, 3, 4, 5, 6.	

Coprime: if they have no common prime factors

Sunrise 6-33 AM

Sunset

when n is prime (eg 2, 3, 5, 7 ...)

$\phi(n) = n-1$

Composite nos ?

$4 = 2 \times 2 = 2^2$ ∴ $\phi(4) = 4 \times (1 - \frac{1}{2})$

$= 4 \times (\frac{2-1}{2})$

$= 4 \times \frac{1}{2}$

$= 2$

$9 = 3^2$ ∴ $\phi(9) = 9 \times (1 - \frac{1}{3})$

$= 9 \times (\frac{3-1}{3})$

$= 9 \times \frac{2}{3}$

$= 6$

$15 = 3 \times 5$ $\phi(15) = 15 (1 - \frac{1}{3})(1 - \frac{1}{15})$

$= 8$

If 'p' is prime $\phi(p) = p-1$

CRS mod 5 = {0, 1, 2, 3, 4, 5}, {1, 2, 3, 4, 5}

RRS mod 5 = {1, 2, 3, 4}, $\phi(5) = 4$

If the modulus is 'm' then the set of CRS is $\{r_1, r_2 \dots r_m\}$

The set of RRS is $\{r_1, r_2 \dots r_{\phi(m)}\}$

Theorem 2.6: Let $(a, m) = 1$. Let $r_1, r_2, \dots r_n$ be a complete, or a reduced, residue system modulo m. Then $ar_1, ar_2, \dots ar_n$ is a complete, or a reduced, residue system, respectively, modulo m.

Proof:

Given $(a, m) = 1$, let $(r_i^\circ, m) = 1$

$(a, m) = (b, m) = 1 \Rightarrow (ab, m) = 1$

$(a, m), (r_i^\circ, m) \Rightarrow (ar_i^\circ, m) = 1$

Clearly $ar_1, ar_2 \dots ar_n$ and $r_1, r_2 \dots r_n$ are of same numbers.

To prove: $ar_i^\circ \not\equiv ar_j^\circ \pmod m$ and $(a, m) = 1$

Assume that suppose $ar_i^\circ \equiv ar_j^\circ \pmod m$

Then $r_i^\circ \equiv r_j^\circ \pmod m$ [$\because$ by Theorem 2.3]

But $r_i^\circ \not\equiv r_j^\circ \pmod m$

$\therefore \Rightarrow \Leftarrow$ to our assumption $ar_i \equiv ar_j \pmod m$ $i^\circ \neq j^\circ$

$\therefore ar_1, ar_2 \dots ar_m$ is CRS (or) RRS modulo m.

Notes 5 marks

Let us postpone the proof of this Theorem after Theorem 2.8.

20

Theorem 2.7: FERMAT'S THEOREM:

Let P be a prime if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

for every integer 'a', $a^p \equiv a \pmod{p}$.

Proof:

If 'p' is prime and $p \nmid a$ then $(a, p) = 1$

By Theorem 2.8,

$(a, p) = 1 \Rightarrow a^{\phi(p)} \equiv 1 \pmod{p}$ ——— (1)

But if p is prime, $\phi(p) = p - 1$

just previous page...

(1) $\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ or $a^p \equiv a \pmod{p}$

Theorem 2.8 Euler's Generalization of Fermat's Theorem.

If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof:

Let $r_1, r_2 \cdots r_{\phi(m)}$ be a RRS modulo m,

By Theorem 2.6;

Let $(a, m) = 1$, let $r_1, r_2 \cdots r_m$ be a Complete (or) RRS modulo 'm', then $ar_1, ar_2 \cdots ar_n$ is a Complete (or) a RRS respec modulo m

$\therefore ar_1, ar_2 \cdots ar_{\phi(m)}$ is also a RRS modulo m.

Hence Corresponding to each r_i°, There is and and only one $ar_j^\circ \ni r_i^\circ \equiv ar_j^\circ \pmod{m}$ ——— (1)

Further different 'r_i°' will have different Corresponding 'ar_j°'.

ie The numbers $ar_1, ar_2 \cdots ar_{\phi(m)}$ are just residues modulo m of $r_1, r_2 \cdots r_{\phi(m)}$ but need not be in the same order.

(1) $\Rightarrow ar_j^\circ \equiv r_i^\circ \pmod{m}$.

Taking product on both sides,

$$\prod_{j^\circ=1}^{\phi(m)} ar_j^\circ \equiv \prod_{i^\circ=1}^{\phi(m)} r_i^\circ \pmod{m}$$

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv \prod_{j^\circ=1}^{\phi(m)} r_j^\circ \pmod{m}$$

$$a^{\phi(m)} \prod_{j^\circ=1}^{\phi(m)} r_j^\circ \equiv \prod_{j^\circ=1}^{\phi(m)} r_j^\circ \pmod{m}$$

If $ax \equiv ay \pmod{m}$ & $(a,m) = 1$

Then $x \equiv y \pmod{m}$

↑

Then by Theorem 2.3 (ii)

we have $a^{\phi(m)} = 1 \pmod{m}$

Now prove Theorem 2.7.

Corollary: Not Necessary

If $(a,m) = 1$, then $ax \equiv b \pmod{m}$ has solution $x = x_1$. All solutions are given by $x = x_1 + jm$, $j = 0, \pm 1, \ldots$

Proof: Given $(a,m) = 1$

By Theorem 2.8, $a^{\phi(m)} \equiv 1 \pmod{m}$

Take $x = a^{\phi(m)-1} b$

Satisfing $ax \equiv b \pmod{m}$ ——— ①

$a \cdot a^{\phi(m)-1} b = b \pmod{m}$

$a^{\phi(m)} b \equiv b \pmod{m}$

$a^{\phi(m)} \equiv 1 \pmod{m}$

Let x_1 be a solution of $ax \equiv b \pmod{m}$

ie $ax_1 \equiv b \pmod{m}$ ——— ②

① − ② $\Rightarrow$ $a(x - x_1) = 0 \pmod{m}$

$\therefore m \mid a(x - x_1)$

$\therefore m \mid a$ or $m \mid (x - x_1)$

$m \nmid a$ as $(a, m) = 1$

$\therefore m \mid x - x_1$

i.e. $x - x_1 = mj$, $j \in Z$

$x = x_1 + mj$, $j = 0, \pm 1, \pm 2 \ldots$

Theorem 2.9:

If $(a, m) = 1$ then there is an 'x' $\ni$ $ax \equiv 1 \pmod m$. Any two such 'x' are congruent (mod m). If $(a, m) > 1$ then there is no such 'x'.

Proof: If $(a, m) = 1$ then $ax + my = 1$ $x, y \in Z$

$\Rightarrow ax - 1 = my$

$ax - 1 \equiv 0 \pmod m$

$ax \equiv 1 \pmod m$

Conversely, if $ax \equiv 1 \pmod m$

then $\exists$ a 'y' $\ni$ $ax + my = 1$ so that

$(a, m) = 1$

By Theorem 2.3 thus if $ax_1 \equiv ax_2 \equiv 1 \pmod m$

then $(a, m) = 1$

$\rightarrow x_1 \equiv x_2 \pmod m$

Having created humanity along with sacrifice, the progenitor said at the beginning of creation. "By this (sacrifice) you shall attain all things; may such sacrifice be your wish - fulfilling cow of plenty." – Bhagavad Gita 3:10

If $(a, m) > 1$ there is no such 'x' will exist

Sunrise 6-32 AM

Examples:

1. If $(a, m) = 1$ Then the linear Congruence $ax \equiv 1 \pmod{m}$ has exactly one solution

$$2x \equiv 1 \pmod{5}$$

$$(2, 5) = 1$$

The CRS mod 5 is $\{0, 1, 2, 3, 4\}$

This Congruence has exactly one solution

$$x = 3$$

$$\begin{aligned} 2 \cdot 3 &= 1 \pmod{5} \\ 6 &= 1 \pmod{5} \\ 6 - 1 &= 0 \pmod{5} \\ 5 &= 0 \pmod{5} \end{aligned}$$

2. If $(a, m) = d$ and $d \nmid b$ then $ax \equiv b \pmod{m}$ has no solution.

$$2x \equiv 3 \pmod{4}$$

$$(2, 4) = 2, \quad 2 \nmid 3$$

CRS mod 4 is $\{0, 1, 2, 3\}$

$\therefore 2x \equiv 3 \pmod{4}$ has no solution

3. If $(a, m) = d$, and $d|b$ Then $ax \equiv b \pmod{m}$ has exactly 'd' solutions.

$2x \equiv 2 \pmod{4}$ (a = 2, b = 2, m = 4)

$d = (2, 4)$ & $d|2$ ie $2|2$.

CRS mod 4 is $\{0, 1, 2, 3\}$.

$x = 1$

$2 \cdot 1 \equiv 2 \pmod{4}$

$2 - 2 \equiv 0 \pmod{4}$

$0 \equiv 0 \pmod{4}$

$x = 3$

$2 \cdot 3 \equiv 2 \pmod{4}$

$6 - 2 \equiv 2 \pmod{4}$

$4 \equiv 0 \pmod{4}$

This has exactly 2 solutions 1 and 3.

Inverse of a Number in a Congruence:

An integer 'a' is said to be an inverse of 'b' if the integers belongs to CRS

Example: Take modulo 11

CRS of mod 11 is $\{0, 1, 2, 3 \cdots 10\}$.

$1 \cdot 1 = 1 \pmod{11}$

$2 \cdot 6 = 1 \pmod{11}$

$3 \cdot 4 = 1 \pmod{11}$

$4 \cdot 3 = 1 \pmod{11}$

$5 \cdot 9 = 1 \pmod{11}$

$6 \cdot 2 = 1 \pmod{11}$

$7 \cdot 8 = 1 \pmod{11}$

$8 \cdot 7 = 1 \pmod{11}$

$9 \cdot 5 = 1 \pmod{11}$

$10 \cdot 10 \cdot 1 \pmod{11}$

Nos:	1	2	3	4	5	6	7	8	9	10
Inverse:	1	6	4	3	9	2	8	7	5	10

Lemma 2.10: 2 m

Let 'p' be a prime number, Then $x^2 \equiv 1 \pmod{p}$ iff $x \equiv \pm 1 \pmod{p}$

Proof:

(i) Given $x^2 \equiv 1 \pmod{p}$

$\Rightarrow x^2 - 1 \equiv 0 \pmod{p}$

ie $(x-1)(x+1) \equiv 0 \pmod{p}$

$\therefore p \mid (x-1)(x+1)$

$\therefore p \mid x-1$ or $p \mid x+1$

ie $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$

$\Rightarrow x \equiv \pm 1 \pmod{p}$

(ii) Conversely, assume $x \equiv \pm 1 \pmod{p}$

$\Rightarrow x \equiv 1 \pmod{p}$, $x \equiv -1 \pmod{p}$

$\Rightarrow x - 1 \equiv 0 \pmod{p}$, $x + 1 \equiv 0 \pmod{p}$

$\Rightarrow x^2 - 1 \equiv 0 \pmod{p}$

$\Rightarrow x^2 \equiv 1 \pmod{p}$

Sunrise 6-30 AM

Theorem 2.11 : WILSON'S THEOREM

Sunset 6-18 PM

If 'p' is a prime, then $(p-1)! \equiv -1 \pmod{p}$ — (1)

Proof:

p is prime;

$p = 2$ $\quad (2-1)! \equiv -1 \pmod{2}$

$1 \equiv -1 \pmod{2}$

$2 \equiv 0 \pmod{2}$

∴ (1) is true for $p = 2$

$p = 3$ $\quad (3-1)! \equiv -1 \pmod{3}$

$2! \equiv -1 \pmod{3}$

$3 \equiv 0 \pmod{3}$

∴ (1) is true for $p = 3$

Let us take a prime number 'p' then the RRS of mod p is $\{1, 2, \ldots, p-1\}$

This set has exactly p-1 elements.

Finding the inverse of the elements of this set

Inverse of 1 is 1

" " p-1 is p-1 Refer Example

Now, There are p-3 elements

ie. 2, 3, ---- p-2

Since They belong to the RRS, each number is relatively prime to 'p'.

ie $(a, p) = 1 \quad \forall \quad x = 2, 3 \cdots p-2$

W.k.T the linear Congruence $ab \equiv 1 \pmod{p}$ has exactly one solution if $(a,p) = 1$ [$\because$ by the eg 1]

$\therefore$ Each and every element in $\{2, 3 \cdots p-2\}$ has one converse.

The product $2 \cdot 3 \cdot 4 \cdots p-2 \equiv 1 \pmod{p}$ ——— (2)

$p \equiv 0 \pmod{p}$
$p-1 \equiv -1 \pmod{p}$ but $p-1 \equiv -1 \pmod{p}$ ——— (3)

(2) & (3) $\Rightarrow 1 \cdot 2 \cdot 3 \cdots p-2 \cdot p-1 \equiv -1 \pmod{p}$

$\Rightarrow (p-1)! \equiv -1 \pmod{p}$

Theorem 2.12 : 5 m

Let 'p' be a prime then $x^2 \equiv -1 \pmod{p}$ —(1) has solutions iff $p = 2$ or $p \equiv 1 \pmod{4}$

Proof:

(i) Let $p = 2$ (or) $p \equiv 1 \pmod{4}$

To prove $x^2 \equiv -1 \pmod{p}$ has solution $p = 2$ in (1)

$x^2 \equiv -1 \pmod{2}$ ——— (2)

Solution of (2) is $x = 1$

$\therefore x^2 \equiv -1 \pmod{p}$ has solution if $p = 2$.

Let $p \equiv 1 \pmod{4}$, p is prime

By Wilson's Theorem

$$(p-1)! \equiv -1 \pmod{p}$$

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv -1 \pmod{p}$$

$$\text{i.e } \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdots (p-1)\right) \equiv -1 \pmod{p}$$

$$\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)\left((p-1)(p-2) \cdots \left(\frac{p+1}{2}\right)\right) \equiv -1 \pmod{p}$$

$$\underbrace{\left(1 \cdot 2 \cdots \frac{p-1}{2}\right)}_{\frac{p-1}{2}}\underbrace{\left((p-1)(p-2) \cdots \left(p-\left(\frac{p-1}{2}\right)\right)\right)}_{p-j} \equiv -1 \pmod{p}$$

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \pmod{p} \quad \text{— (3)}$$

Here $j(p-j) = jp - j^2 \equiv -j^2 \pmod{p}$

$$\prod_{j=1}^{(p-1)/2} (-j^2) \equiv -1 \pmod{p}$$

$$(-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j^2 \equiv -1 \pmod{p} \quad \text{— (4)}$$

$$4(5-4) = 4 \equiv -16 \pmod{5}$$

$$4+16 \equiv 0 \pmod{5}$$

$$20 \equiv 0 \pmod{5}$$

64 × 9 = 576

$$\text{i.e } 4 \cdot (-j^2) \quad -[1 \; 4 \; 9 \; 16] \equiv -1 \bmod p \to 5$$

$j = 1 \cdots 4$

Therefore, without attachment to the fruits of your work, constantly engage in your duty as a warrior, for by acting without attachment one attains God consciousness. — Bhagavad Gita 3:19

$$-576 \equiv -1 \bmod p \to 5$$

$$-575 \equiv 0 \bmod p \to 5$$

Sunrise 6-29 AM

Sunset 6-

Given $p \equiv 1 \pmod 4$

$\therefore 4 \mid p-1 \Rightarrow p-1$ is a multiple of 4.

$\Rightarrow \frac{p-1}{2}$ " " " " 2

$\Rightarrow \frac{p-1}{2}$ is even

(4) $\Rightarrow \prod_{j=1}^{\frac{p-1}{2}} j^2 \equiv -1 \pmod p$

$\left(\prod_{j=1}^{\frac{p-1}{2}} j\right)^2 \equiv -1 \pmod p$

This is of the form $x^2 \equiv -1 \pmod p$

$\therefore$ If $p \equiv 1 \pmod 4$, the solution of $x^2 \equiv -1 \pmod p$ is $\left(\frac{p-1}{2}\right)!$

Conversely,

Assume that $x^2 \equiv -1 \pmod p$ has a solution where 'p' is prime.

To prove: $p = 2$ (or) $p \equiv 1 \pmod 4$

Assume $p \neq 2$ (or) $p \not\equiv 1 \pmod 4$

$\therefore p \equiv 3 \pmod 4$

Sunrise 6-28 AM

Sunset 6-18 PM

$\Rightarrow p = 3 + 4m$

$\Rightarrow p - 1 = 2 + 4m$

$\Rightarrow \frac{p-1}{2} = 1 + 2m$ ie odd

Given $x^2 \equiv -1 \pmod{p}$

$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

$x^{p-1} \equiv -1 \pmod{p}$

a $\Rightarrow\Leftarrow$ to our assumption

$\therefore p = 2$ (or) $p \equiv 1 \pmod{4}$

Sunrise 6-27 AM

Solution of Congruence

Sunset 6-18 p

Let $f(x)$ denote a polynomial with integrable coefficients

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

Let 'u' be an integer s.t

$$f(u) \equiv 0 \pmod{m}$$

$\Rightarrow$ u is the solution of the Congruence

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

If u is a solution of the Congruence $f(x) \equiv 0 \pmod{m}$ & and if $v \equiv u \pmod{m}$. then v is also a solution. (by Theorem 2.2)

whether or not an integer is a solution of a Congruence depends on the modulus m as well as on the polynomial $f(x)$.

$\therefore$ we say that $x \equiv u \pmod{m}$ is a solution of $f(x) \equiv 0 \pmod{m}$ meaning that every integer congruent to u modulo m, satisfies

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

Example: 1. The Congruence $x^2 - x + 4 \equiv 0 \pmod{10}$ has solution $x = 3$ and $x = 8$.

If $f(x) \equiv 0 \pmod{m}$ has a solution 'u' it has infinitely many solutions.

All integers 'x' $\Rightarrow$ $V \equiv U \pmod{m}$ are solutions in the above example.

$x = 13, 23, \ldots 18, 28 \ldots$ are the solutions of $x^2 - x + 4 = 0 \pmod{10}$.

2. Consider, $x^2 + 1 \equiv 0 \pmod{7}$

CRS is $\{0, 1, 2, 3, 4, 5, 6\}$

But $1 \equiv -6 \pmod{7}$ Given $x^2+1 \equiv 0 \pmod{7}$

$2 \equiv -5 \pmod{7}$ $x = 0$ $1 \not\equiv 0 \pmod{7}$

$3 \equiv -4 \pmod{7}$ $x = \pm 1$ $2 \not\equiv 0 \pmod{7}$

$4 \equiv -3 \pmod{7}$

$5 \equiv -2 \pmod{7}$

$6 \equiv -1 \pmod{7}$

$\therefore$ CRS $= \{0, \pm 1, \pm 2, \pm 3 \cdots \pm 6\}$

3. Consider $x^2 + 1 \equiv 0 \pmod{5}$

CRS is $\{0, 1, 2, 3, 4\}$

$1 \equiv -4 \pmod{5}$

$2 \equiv -3 \pmod{5}$

$3 \equiv -2 \pmod{5}$

$4 \equiv -1 \pmod{5}$

CRS is $\{0, \pm 1, +2, \cdots \pm 4\}$

Given, $x^2+1 \equiv 0 \pmod 5$

$x = 0, \quad 1 \not\equiv 0 \pmod 5$

$x = \pm 1, \quad 2 \not\equiv 0 \pmod 5$

$x = \pm 2, \quad 5 \not\equiv 0 \pmod 5$ ✓

$x = \pm 3, \quad 10 \not\equiv 0 \pmod 5$ ✓

$x = \pm 4 \quad 17 \not\equiv 0 \pmod 5$

$\therefore x^2+1 \equiv 0 \pmod 5$ has two solutions.

$x = \pm 2, \pm 3$

Definition: Let $r_1, r_2 \cdots r_m$ denote a CRS modulo m. The number of solutions of $f(x) \equiv 0 \pmod m$ is the number of r_i's $\ni f(r_i) \equiv 0 \pmod m$.

Degree of the Congruence:

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$

If $a_n \not\equiv 0 \pmod m$ the degree of the Congruence of $f(x) \equiv 0 \pmod m$ is 'n'

If $a_n \equiv 0 \pmod m$, let 'j' be the largest integers $\ni a_j \not\equiv 0 \pmod m$, then the degree of the Congruence is 'j'

If there is no such j, (ie) if all the co-efficients of $f(x)$ are multiples of m, no degree is assigned to the congruence.

Note: Degree of the congruence $f(x) \equiv 0 \pmod{m}$ is not the degree of the polynomial $f(x)$. Degree of the congruence depends on the modulus.

Example:

1. Consider $f(x) = 6x^3 + 3x^2 + 1$

$$f(x) \equiv 0 \pmod 5$$

$6x^3 + 3x^2 + 1 = a_n x^n + a_{n-1} x^{n-1} + a_0$

$a_n = 6 \quad x^n = x^3 \quad n = 3$

$a_n \not\equiv 0 \pmod m \quad 6 \not\equiv 0 \pmod m \Rightarrow 6 \not\equiv 0 \pmod 5$

$f(x) \equiv 0 \pmod m$ is 3

$6 \equiv 0 \pmod 2 \quad [\because 2 \mid 6-0]$

$a_n \equiv 0 \pmod m$ here $j = 2$ is the largest integer

$\therefore a_2 = 3 \not\equiv 0 \pmod 2$, Then the degree of the congruence is 2

Here Degree of polynomial $f(x)$ is 3.

2. Consider $f(x) = 7x^4 - 6x^3 + 3x^2 + 2$

Theorem 2.16 2m

If $d|m$, $d>0$ and if U is a Solution of $f(x) \equiv 0 \pmod m$ then U is a solution of $f(x) \equiv 0 \pmod d$

Proof:

If 'U' is a solution of $f(x) \equiv 0 \pmod m$

then $f(U) \equiv 0 \pmod m$

$\Rightarrow m | f(U)$

$\Rightarrow f(U) = mx \quad , \quad x \in Z$

Given $d|m \Rightarrow m = dx_1 \quad , \quad x_1 \in Z$

$f(U) = mx$

$= d x_1 x$

$= d(x_1 x) \quad x_1, x \in Z$

$\therefore d | f(U)$

$\therefore U$ is the solution of $f(x) \equiv 0 \pmod d$

Converse is not true.

Congruence of degree one:

Any congruence of degree one can be put in the form $ax \equiv b \pmod m$, $a \not\equiv 0 \pmod m$

Note:

If $(a, m) = 1$, then $ax \equiv b \pmod m$ has exactly one solution say $x \equiv x_1 \pmod m$

Let $(a, m) = g$, then $ax \equiv b \pmod m$ has a solution then $b \equiv aU \pmod m$ and hence

$$b \equiv aU \equiv 0 \pmod g$$

If $g \nmid b$, then $ax \equiv b \pmod m$ has no solution.

If $g \mid b$, then $ax \equiv b \pmod m$ has many solutions.

The solutions are

$$x = x_1 + t\left(\frac{m}{g}\right) \pmod m \qquad 0 \le t \le g-1.$$

Theorem 2.19 Prove Chinese Remainder Theorem.

Let 'm' and 'n' denote any two positive relatively prime integers, then $\phi(mn) = \phi(m).\phi(n)$

Proof:

Let $\phi(m) = r$ ——— (1)

Then $\exists\ a_1, a_2 \cdots a_r$ relatively prime to 'm'.

ie $(a, m) = 1$, $i = 1, 2 \cdots r$ ——— (2)

$\{a_1, a_2 \cdots a_r\}$ is the RRS modulo m.

Let $\phi(n) = s$ ——— (3)

Sunrise 6-23 AM

Then $\forall\ b_1, b_2 \cdots b_s$ relatively prime to n.

$(b_j, n) = 1 \quad j = 1, 2 \cdots s$ ——— (4)

$\{b_1, b_2 \cdots b_s\}$ is the RRS modulo 'n'. Consider the Number 'mn'.

Assume $(x, mn) = 1 \Rightarrow (x, m) = 1$ & $(x, n) = 1$

$\therefore x$ is an element of the RRS mod 'mn'

$\therefore (x, m) = 1, (x, n) = 1 \Rightarrow x \equiv a_i \pmod m$

$\Rightarrow x \equiv b_j \pmod m$

By chinese remainder theorem,

For each 'a_i' & 'b_j' we can find a solution these are 'rs' solutions.

ie $\forall$ 'rs' no's relatively prime with 'mn'

$\phi(mn) = rs = \phi(m)\,\phi(n)$, where $(m, n) = 1$

Example: $m = 4, \quad n = 9$

$\phi(m) = \phi(4) = \phi(2^2) = 2^2 - 2 = 2$

$\phi(n) = \phi(9) = \phi(3^2) = 3^2 - 3 = 6$

$\phi(m)\,\phi(n) = 2 \cdot 6 = 12$ ——— (1)

$\phi(mn) = 36$

CRS mod 36 is $\{0, 1, 2 \cdots 35\}$.

The No of integers which is less than 36 & prime to 36 is $\phi(m) = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$ ie 12 nos

$\phi(36) = 12$ ——— (2)

Thus, knowing oneself to be superior to the intellect, control the mind with intellect. In this way, O mighty-armed one, destroy the unconquerable enemy in the form of desire. – Bhagavad Gita 3:43

(1) & (2) $\quad \phi(mn) = \phi(m)\,\phi(n)$

Sunrise 6-23 AM

Chinese Remainder Theorem

Sunset 6-20

Let $m_1, m_2 \cdots m_r$ denote 'r' positive integers that are relatively prime in pairs and let $a_1, a_2 \cdots a_r$ denote any 'r' integers. Then the congruence $x \equiv a_i \pmod{m_i}$ $i = 1, 2 \cdots r$ have common solutions. If x_0 is one such solution. Then an integer 'x' satisfies the congruences $x \equiv a_i \pmod{m_i}$ iff 'x' is of the form $x = x_0 + km$ for some integer k. Here $M = m_1 m_2 \cdots m_r$

Proof: Given $x \equiv a_i \pmod{m_i}$ $i = 1, 2 \cdots r$

ie
$$\left.\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}\right\} \quad \text{---- (1)}$$

Also, $(m_i, m_j) = 1$ $i \neq j$

Then $\frac{M}{m_1}, \frac{M}{m_2} \cdots \frac{M}{m_r}$ are integers.

$$\left(\frac{M}{m_1}, m_1\right) = 1, \left(\frac{M}{m_2}, m_2\right) = 1, \cdots \left(\frac{M}{m_r}, m_r\right) = 1 \quad \text{---- (2)}$$

W.K.T $ax \equiv b \pmod{m}$ has a solution if $(a, m) = 1$

$\frac{M}{m_1} x_1 \equiv 1 \pmod{m_1}$ has a solution

$\frac{M}{m_2} x_2 \equiv 1 \pmod{m_2}$ " " "

⋮

$\frac{M}{m_r} x_r \equiv 1 \pmod{m_r}$ " " " — (3)

Also $\frac{M}{m_1} x_1 \equiv 0 \pmod{m_2}$

$\frac{M}{m_1} x_1 \equiv 0 \pmod{m_3}$

⋮

$\frac{M}{m_1} x_1 \equiv 0 \pmod{m_r}$ — (4)

Similarly $\frac{M}{m_2} x_2 \equiv 0 \pmod{m_1}$

$\frac{M}{m_2} x_2 \equiv 0 \pmod{m_3}$

⋮

$\frac{M}{m_2} x_2 \equiv 0 \pmod{m_r}$

$$\frac{M}{m_2} x_2 \equiv 0 \pmod{m_1}$$

$$\frac{M}{m_2} x_2 \equiv 0 \pmod{m_2}$$

$$\vdots$$

$$\frac{M}{m_{n-1}} x_{n-1} \equiv 0 \pmod{m_{n-1}} \quad \text{---- (4)}$$

Consider a Number,

Let $X = \frac{M}{m_1} x_1 a_1 + \frac{M}{m_2} x_2 a_2 + \cdots + \frac{M}{m_n} x_n a_n$

$\Rightarrow X = \frac{M}{m_1} x_1 a_1 +$ multiple of m_1

$\Rightarrow X - \frac{M}{m_1} x_1 a_1 =$ multiple of m_1

$\Rightarrow X - \frac{M}{m_1} x_1 a_1 \equiv 0 \pmod{m_1}$

$\Rightarrow X \equiv \frac{M}{m_1} x_1 a_1 \pmod{m_1}$ ---- (5)

but $\frac{M}{m_1} x_1 \equiv 1 \pmod{m_1}$ (by (3))

$\therefore \quad X \equiv a_1 \pmod{m_1}$

$\therefore$ X is a solution of $x \equiv a_1 \pmod{m_1}$

IIIly, we can prove that X is a solution of

$x \equiv a_2 \pmod{m_2}$

and so on.

Hence X is the solution of the system (1)

If x_0 and x_1 are two solutions of (1)

$x_0 \equiv a_i \pmod{m_i}$

$x_1 \equiv a_i \pmod{m_i} \qquad i = 1, 2 \cdots r$

$x_0 - x_1 \equiv 0 \pmod{m_i}$

$\Rightarrow \quad x_0 \equiv x_1 \pmod{m_i}$

$\Rightarrow \quad x_0 \equiv x_1 \pmod{M} \qquad [\because \text{by (iii) of 2.3}]$

Theorem 2.17

Let $(a, m) = g$ Then $ax \equiv b \pmod{m}$ has no solution if $g \nmid b$. If $g \mid b$ it has 'g' solution

$x = \left(\frac{b}{g} x_0 + t \frac{m}{g} \right) t = 0, 1, 2 \cdots g-1$, where

x_0 is any solution of $\frac{a}{g} \equiv 1 \pmod{\frac{m}{g}}$

Sunrise 6-20 AM

Proof:

Sunset 6-20 PM

Given $(a, m) = g$ and $ax \equiv b \pmod{m}$ ——— (1)

$\Rightarrow m \mid ax - b$

$\Rightarrow ax - b = mk, \quad k \in Z$

$\Rightarrow ax - mk = b$ ——— (2)

(i) Let $g \nmid b$

$\because (a, m) = g \Rightarrow g \mid a, \; g \mid m$

$\Rightarrow g \mid ax, \; g \mid mk$

$\Rightarrow g \mid ax - mk$

$\Rightarrow g \mid b$

a $\Rightarrow \Leftarrow$ to the fact $g \nmid b$

$\therefore ax \equiv b \pmod{m}$ has no solutions if $g \nmid b$.

(ii) Let $ax \equiv b \pmod{m}$ and $(a, m) = g$.

Then $\left(\frac{a}{g}, \frac{m}{g}\right) = 1$ ——— (3)

Given $g \mid b$

Dividing (1) by g,

$$\frac{a}{g} x \equiv \frac{b}{g} \pmod{\frac{m}{g}} \quad \text{——— (4)}$$

There is a solution x_0 then for

$\frac{a}{g} x \equiv 1 \pmod{\frac{m}{g}}$ [$\because$ by (3)]

$$\Rightarrow \frac{a}{g} x_0 \equiv 1 \pmod{\frac{m}{g}} \quad \text{---------- (5)}$$

Multiplying (4) by x_0.

$$\frac{a}{g} \times x_0 \equiv \frac{b}{g} x_0 \pmod{\frac{m}{g}}$$

$$x \equiv \frac{b}{g} x_0 \pmod{\frac{m}{g}} \quad [\because \text{by (5)}]$$

$$\Rightarrow \frac{m}{g} \mid x - \frac{b}{g} x_0$$

$$\Rightarrow x - \frac{b}{g} x_0 = \frac{m}{g} t \quad , \quad t \in Z$$

$$\Rightarrow x = \frac{b}{g} x_0 + \frac{m}{g} t \quad , \quad t = 0, 1, 2 \cdots g-1$$

and all other values are Congruent to mod m giving the same set of values as $t = 0, 1, 2 \cdots g-1$

Example :

Find the general solution of $5x \equiv 2 \pmod 7$

This is of the form $ax \equiv b \pmod m$

Here $a = 5$, $b = 2$, $m = 7$

$(a, m) = (5, 7) = 1$

$5x - 2 \equiv 0 \pmod 7$

$\Rightarrow 7 \mid 5x - 2$

$\Rightarrow 5x - 2 = 7y$, $y \in Z$

$\Rightarrow 5x - 2 = 7y$

$\Rightarrow 5x = 7y + 2$

$\Rightarrow x = \frac{7y + 2}{5}$

when $y = 4$, $x = 6$

$\therefore x \equiv 6 \pmod 7$ is the solution of the given Congruence.

We can also apply Euclidean algorithm to find this.

Two problem from the other notes ... ☺

Sunrise 6-17 AM

Prime Power Module

Sunset 6-20 PM

The problem of solving a congruence has reduced to that of solving a congruence where modulus is a power of a single prime.

Steps to be followed to solve the congruence of the form $f(x) \equiv 0 \pmod{p^h}$

Step 1: Consider the given congruence as

$$f(x) \equiv 0 \pmod{p^{h+1}}$$

Step 2: Find the solution of the congruence

$$f(x) \equiv 0 \pmod{p^h}$$

Step 3: Let $x = c$ be one of the solution of

$$f(x) \equiv 0 \pmod{p^h}$$

Then the solution of the given congruence

$$f(x) \equiv 0 \pmod{p^{h+1}}$$

corresponding to 'c' one as follows.

Condition	Solution
1. $f'(c) \not\equiv 0 \pmod{p}$	There is only one solution $c + p^h q$, $0 \le q < p$ where q is given by $f'(c)\,q \equiv \frac{-f(c)}{p^h} \pmod{p}$

2. $f'(c) \equiv 0 \pmod{p}$ and $f(c) \equiv 0 \pmod{p^{h+1}}$ — There are p solutions $c + p^h q$ where $q = 0, 1, 2 \cdots h$

3. $f'(c) \equiv 0 \pmod{p}$ and $f(c) \not\equiv 0 \pmod{p^{h+1}}$ — There is no solution.

Problem 1: Solve $x^2 + x + 7 \equiv 0 \pmod{27}$

Solution: $x^2 + x + 7 \equiv 0 \pmod{27}$

$x^2 + x + 7 \equiv 0 \pmod{3^3} \equiv 0 \pmod{p^{h+1}}$

$x^2 + x + 7 \equiv 0 \pmod{p^h} \equiv 0 \pmod{3^{2+1}}$

$\equiv 0 \pmod{3^2}$ $3^2 = 9 : 0, 1, 2 \cdots 8$

CRS is $\{0, \pm 1, \pm 2, \pm 3, \pm 4\}$ or $0, \pm 1, \pm 2 \cdots \pm 4$

Solutions are

1) Take $x = 1$

$f(1) = 1^2 + 1 + 7 = (9)$

$f'(1) = 2x + 1 = 2(1) + 1 = 3$

$f'(1) \equiv 0 \pmod{p}$

$3 \equiv 0 \pmod{3}$ ✓

Next, $f(c) \equiv 0 \pmod{p^{h+1}}$

$(9) \equiv 0 \pmod{27}$ not true

$27 \nmid 9 - 0$

Condition 3, ∴ There is no solution.

2) Take $x = 4$

$f(4) = x^2 + x + 7 = 4^2 + 4 + 7 = 27$

$f'(4) = 2x + 1 = 8 + 1 = 9$

$f'(c) \equiv 0 \pmod{p}$

$9 \equiv 0 \pmod{3}$

$3 \mid 9 - 0$ is true.

$f(c) \equiv 0 \pmod{p^{h+1}}$

$27 \equiv 0 \pmod{27}$

$27 \mid 27$

Hence there are p solutions ie 3 solutions

$c + p^h q$ where $q = 0, 1, 2, \ldots h$

$4 + 3^2 \cdot 0 \quad h = 0$ $\boxed{h = 2.}$

$= 4$

$c + p^h q, \quad h = 1$

$4 + 3^2 \cdot 1$

$= 4 + 9 = 13$

$c + p^h q, \quad h = 2$

$4 + 3^2 \cdot 2$

$= 4 + 9 \times 2$

$= 22$

Hence the solutions of $x^2 + x + 7 \equiv 0 \pmod{27}$ are 4, 13, 22.

Prime Modulus :

Now, we reduce the problem of solving $f(x) \equiv 0 \pmod m$ to the last stage, Congruence with prime modulo.

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ where p is prime. $a_n \not\equiv 0 \pmod p$

Theorem 2.24 :

If the degree 'n' of $f(x) \equiv 0 \pmod p$ is greater than or equal to 'p', then either every integer is a solution of $f(x) \equiv 0 \pmod p$

proof :

For any x, by Fermat's Theorem

$$x^{p-1} \equiv 1 \pmod p$$

$$x^p x^{-1} \equiv 1 \pmod p$$

$$x^p \equiv x \pmod p$$

$$x^p - x \equiv 0 \pmod p \quad \text{——— (1)}$$

If 'U' is a solution of (1) then

$$U^p - U \equiv 0 \pmod p \quad \text{——— (2)}$$

Using division algorithm, we get

$$f(x) = (x^p - x)\, q(x) + r(x) \quad \text{——— (3)}$$

where $q(x)$ is the quotient and $r(x)$ is a remainder.

Also, $q(x)$ is a polynomial with integer co-efficient with degree less than 'p' & $r(x) = 0$???

Since 'U' is a solution of $f(x)$ from (3)

$f(U) = (U^p - U)\, q(U) + r(U)$

But $U^p - U \equiv 0 \pmod p$ [$\because$ by (2)]

$f(U) = r(U)$

If $r(x) = 0$ every co-efficient in $r(x)$ is divisible by 'p' Then every integer is the solution of $f(x) \equiv 0 \pmod p$.

Problem:

Reduce the Congruence to equivalent Congruence of degree ≤ 6, $x^{11} + x^8 + 5 \equiv 0 \pmod 7$

Solution: By Fermat's Theorem

$$x^{p-1} \equiv 1 \pmod p$$

$$x^{7-1} \equiv 1 \pmod p \equiv 1 \pmod 7$$

$$x^7 \equiv x \pmod 7 \quad \text{or}$$

$$x^7 - x \equiv 0 \pmod 7 \qquad \text{——— (1)}$$

$\therefore$ $x^{11} + x^8 + 5$ by $x^7 - x$

$$x^7 - x \;\big)\; x^{11} + x^8 + 5 \;\big(\; x^4 + x$$

$$-x^{11} \pm x^5$$

$$x^8 + x^5 + 5$$

$$x^8 - x^2$$

$$x^5 + x^2 + 5$$

A liberated sould established in knowledge, who is free from attachment and acts only in sacrifice, dissipates all his karma. – Bhagavad Gita 4:23

$\therefore f(x) = (x^7 - x)(x^4 + x) + (x^5 + x^2 + 5)$

The reduced equivalent congruence

ie $x^5 + x^2 + 5 \equiv 0 \pmod 7$ ——— (2)

Now, solve this equation

CRS mod 7 ie $\{0, \pm 1, \pm 2, \pm 3\}$

$x = 0$ in (2) $5 \not\equiv 0 \pmod 7$

$x = 1$ " " $7 \equiv 0 \pmod 7$

$x = -3$ $-229 \not\equiv 0 \pmod 7$

$\therefore x \equiv 1 \pmod 7$ is the solution of the given congruence.

Theorem 2.25 10 marks

If the degree 'n' of $f(x) \equiv 0 \pmod p$ is greater than or equal to p $(\geq p)$ (*), of $f(x) \equiv 0 \pmod p$ or there is a polynomial $g(x)$ having integral co-efficients with leading Coefficients 1 $\not\equiv$ $g(x) \equiv 0 \pmod p$ is of degree less than 'p' and the solutions

* then every congruence is a solution

Sunrise 6-14 AM Sunset 6-21 PM

of $g(x) \equiv 0 \pmod p$ are precisely those of $f(x) \equiv 0 \pmod p$.

Proof: Given $n \geq p$

Divide $f(x)$ by $x^p - x$ Then

$$f(x) = (x^p - x)\, q(x) + r(x) \quad \text{——— (1)}$$

$q(x)$ – is a polynomial with integer coefficient.

$r(x)$ – is either zero or a polynomial with integral co-efficient and degree of $r(x) < p$.

By Fermat's Theorem Since every integer is a solu of $x^p \equiv x \pmod p$

$a^p - a \equiv 0 \pmod p$ for every integer 'a'

$a^p \equiv a \pmod p$

$p \mid a^p - a$

$f(a) \equiv r(a) \pmod p$ by (1) ∀ integer 'a'

$p \mid f(a) - r(a)$

∴ The solution of $f(x) \equiv 0 \pmod p$ are the same as the solution of $r(x) \equiv 0 \pmod p$

Case (i):

If $r(x) = 0$ or if every coefficient of $r(x)$ are divisible by 'p' Then every integer is a solution of $f(x) \equiv 0 \pmod p$ & so $f(a) \equiv 0 \pmod p$ ∀ integer 'a'

Hence every integer is a solution of $f(x) \equiv 0 \pmod p$

(case ii)

Other possibility is that $r(x)$ is a polynomial of degree $m < p$ with at least one co-efficient not divisible by p.

Let $r(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$

Let k be the largest suffix $\ni b_k \nmid p$

ie $(b_k, p) = 1$

In this case, we can find an integer b $\ni$ $bb_k \equiv 1 \pmod{p}$ ——— (3)

we get

$$r(x) = m(p) + b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + b_0$$

[$m(p)$ is a multiple of p]

$$\therefore br(x) = m(p) + (bb_k)x^k + (bb_{k-1})x^{k-1} + \cdots + bb_1 x + bb_0$$

$$br(x) \equiv (x^k + bb_{k-1}x^{k-1} + \cdots + bb_0) \pmod{p}$$ by (3)

Take

$$g(x) = x^k + bb_{k-1}x^{k-1} + \cdots + bb_0$$

$$\therefore b_{r(x)} \equiv g(x) \pmod{p} \quad \text{——— (4)}$$

Since $r(x) \equiv 0 \pmod{p}$

$br(x) \equiv 0 \pmod{p}$

$h r(x) \equiv 0 \pmod{p}$ are the same and so they are the solution of $g(x) \equiv 0 \pmod{p}$

Also the solution of $f(x) \equiv 0 \pmod{p}$ are the same as the solution of $r(x) \equiv 0 \pmod{p}$

Hence $f(x) \equiv 0 \pmod{p}$ & $g(x) \equiv 0 \pmod{p}$ have precisely the same solution.

Theorem 2.26:

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ be a polynomial of degree 'n' with integral coefficient $\neq a_n \not\equiv 0 \pmod{p}$ where p is a prime, then the polynomial congruence $f(x) \equiv 0 \pmod{p}$ has atmost 'n' roots.

(or)

The congruence $f(x) \equiv 0 \pmod{p}$ of degree 'n' has atmost 'n' solutions

Proof:

The proof is by induction on 'n', the degree of the congruence.

when $n = 0$, $f(x) = a_0$

$\not\equiv 0 \pmod{p}$

Hence the Congruence has no solutions.

when $n=1$, $f(x) = a_1 x + a_0 \equiv 0 \pmod{p}$

Since 'p' is prime and $a_1 \not\equiv 0 \pmod{p}$

$$(a_1, p) = 1$$

∴ The Congruence has exactly one solution Thus the theorem holds for $n=0$ & $n=1$.

Refer defn at March 12

Let us assume that the theorem be true for all polynomials of degree $n-1$.

Assume, $f(x) \equiv 0 \pmod{p}$ has $n+1$ solutions $x_0, x_1, \ldots x_n$ with $x_i \not\equiv x_j \pmod{p}$ $i \neq j$

$$\Rightarrow f(x_k) \equiv 0 \pmod{p}, \quad k = 0, 1, 2, \ldots n.$$

$$\therefore f(x) = a_n x^n + \cdots + a_1 x + a_0$$

$$f(x_k) = a_n x_k^n + \cdots + a_1 x_k + a_0$$

$$f(x_0) = a_n x_0^n + \cdots + a_1 x_0 + a_0$$

$$f(x) - f(x_0) = a_n (x^n - x_0^n) + a_{n-1} (x^{n-1} - x_0^{n-1}) + \cdots + a_1 (x - x_0)$$

$$= (x - x_0)\, g(x)$$

where $g(x)$ is a polynomial of degree $n-1$ with leading coefficient 'a_n'.

$f(x_k) - f(x_0) = (x_k - x_0)\, g(x_k)$

Since $f(x_k) \equiv 0 \pmod p$

& $f(x_0) \equiv 0 \pmod p$

ie $(x_k - x_0)\, g(x_k) \equiv 0 \pmod p$

Since $x_k \not\equiv x_0 \pmod p \quad k \neq 0$

$\Rightarrow x_k - x_0 \not\equiv 0 \pmod p \quad k \neq 0$

ie $g(x_k) \equiv 0 \pmod p$ for $k = 1, 2 \cdots n$

$\because k \neq 0.$

This shows that $g(x) \equiv 0 \pmod p$ of degree $n-1$ has 'n' roots.

a $\Rightarrow \in$ to our assumptions ie $n+1$ solutions

Hence the theorem is true for given polynomial congruence.

$\therefore f(x) \equiv 0 \pmod p$ of degree 'n' has atmost 'n' roots.

Corollary : 2.27

If $b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0 \equiv 0 \pmod p$ has more than 'n' solutions then all the coefficients b_i's are divisible by 'p'.

Theorem 2.29 :

The congruence $f(x) \equiv 0 \pmod{p}$ of degree n, with leading coefficient $a_n = 1$ has n solutions iff $f(x)$ is a factor of $x^p - x$ modulo p, ie iff $x^p - x = f(x)\,q(x) + p\,s(x)$, where $q(x)$ & $s(x)$ have integral coefficients, $q(x)$ has degree $p-n$ and leading coefficient 1 and where either $s(x)$ is a polynomial of degree less than n or $s(x)$ is zero.

Proof :

Case i : Given $f(x) \equiv 0 \pmod{p}$ is a polynomial congruence of degree 'n'.

If it has 'n' solutions then $n \leq p$. ∵ Defn 2.4 by Ref 2.2

Divide $x^p - x$ by $f(x)$, we get

$$x^p - x = f(x)\,q(x) + r(x), \text{ where}$$

$r(x) = 0$ or it is a polynomial of degree $< n$ — (x)

Let a be any root of $f(x) \equiv 0 \pmod{p}$

$$\therefore f(a) \equiv 0 \pmod{p} \quad \text{——— (1)}$$

Also $a^p - a \equiv 0 \pmod{p}$ ——— (2)

Corresponding to the root a, $f(x) \equiv 0 \pmod{p}$ we have $a^p - a = f(a)\,q(a) + r(a)$

Sunrise 6-11 AM

Sunset 6-21 PM

① & ② ⇒

$r(a) \equiv 0 \pmod p$

∴ 'a' is the root of $r(x) \equiv 0 \pmod p$

If $r(x) \neq 0$ then it is a polynomial of degree $< n$ and having 'n' solutions by ④?

Each of the 'n' solutions of $f(x) \equiv 0 \pmod p$ is a solution of $r(x) \equiv 0 \pmod p$

∴ all the coefficients of $r(x)$ are divisible by 'p'.

i.e $r(x) = p \cdot s(x)$

Hence $x^p - x = f(x) q(x) + p \cdot s(x)$

Case (ii):

If $x^p - x = f(x) q(x) + p \cdot s(x)$

$\Rightarrow f(a) q(a) = a^p - a$

$\equiv 0 \pmod p$ ∀ integer 'a'

∴ $f(x) q(x) \equiv 0 \pmod p$ has p solutions.

∴ (By fermat Theorem)

This congruence has leading term x^p.

The leading term of $f(x)$ is x^n by hypothesis.

∴ The leading " " $q(x)$ is x^{p-n}

Then by Theorem 2.26, the congruences $f(x) \equiv 0 \pmod p$ and $q(x) \equiv 0 \pmod p$ have

at most n solutions and $p-n$ solutions respectively. Let the solutions be $u_1, u_2 \ldots u_k$ where $k \leq p-n$

If 'n' is any of the remaining $p-k$ solutions then $(q(a), p) = 1$ and

$$f(u) \cdot g(u) \equiv 0 \pmod{p}$$

So $f(u) \equiv 0 \pmod{p}$ has atmost $p-k \geq p-(p-n) = n$ solutions.

But the polynomial Congruence has atmost 'n' solution combining those two findings, we get the polynomial Congruence $f(x) \equiv 0 \pmod{p}$ has exactly 'n' solutions.

Note:

If $a_n \neq 1$, we can find an coleger $\bar{a}_n$ s.t $a_n \bar{a}_n \equiv 1 \pmod{p}$ but $g(x) = \bar{a}_n f(x) - (a_n \bar{a}_n - 1)x^n$ then

$g(x) \equiv 0 \pmod{p}$ has the same solutions as $f(x) \equiv 0 \pmod{p}$ and

$g(x)$ has leading co-efficient

Sunrise 6-09 AM

Corollary 2.30:

Sunset 6-21 PM

If $d \mid p-1$ then $x^d \equiv 1 \pmod{p}$ has d solutions.

Proof:

Choose 'e' $\rightarrow$ $de = p-1$

Since $(y-1)(1+y+\cdots+y^{e-1}) = y^e - 1$

In taking $y = x^d$

we see that

$$x(x^d-1)(1+x^d+\cdots+x^{d(e-1)}) = x(x^{de}-1)$$
$$= x(x^{p-1}-1)$$
$$= x^p - x.$$

Identical Congruences:

Consider 2 polynomials $f(x)$ & $g(x)$ with integral co-efficients.

They are said to be identical modulo 'm'.

If the corresponding co-efficient are congruent modulo 'm'.

Then the polynomials

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

are identical if $a_i \equiv b_i \pmod{m}$ $\forall i$

In this case we write $f(x) \equiv g(x) \pmod m$ and call it an identical Congruence.

Example:

If $f(x)$ and $g(x)$ are identical then the solution $f(x)$ are same as that of $g(x)$.

Problems:

1. find $\phi(720)$

$$\phi(720) = 2 \times 360$$
$$= 2 \times 2 \times 180$$
$$= 2 \times 2 \times 2 \times 90$$
$$= 2 \times 2 \times 2 \times 2 \times 45$$
$$= 2 \times 2 \times 2 \times 2 \times 9 \times 5$$
$$= 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 5$$
$$= 2^4 \times 3^2 \times 5$$

$$\phi(n) = n \prod_{j=1}^{n} (1 - 1/p_j) \qquad p_1 = 2,\ p_2 = 3,\ p_3 = 5$$

$$\phi(720) = 720 (1 - 1/2)(1 - 1/3)(1 - 1/5)$$
$$= 192.$$

Sunrise 6-07 AM

Sunset 6-21 PM

2. Find $\phi(25200)$

3. Find the integer that satisfies $x \equiv 1 \pmod 4$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

Solution:

By Chinese Remainder Theorem

$x \equiv a_i \pmod{m_i}$ $i = 1, 2, 3$

$a_1 = 1$ $m_1 = 4$ $M = m_1 \cdot m_2 \cdot m_3$

$a_2 = 2$ $m_2 = 5$ $= 4 \times 5 \times 7$

$a_3 = 3$ $m_3 = 7$ $= 140$

$$x = \frac{M}{m_1} x_1 a_1 + \frac{M}{m_2} x_2 a_2 + \frac{M}{m_3} x_3 a_3$$

Now, $\frac{M}{m_1} x_1 \equiv 1 \pmod{m_1}$

$\frac{M}{m_2} x_2 \equiv 1 \pmod{m_2}$

$\frac{M}{m_3} x_3 \equiv 1 \pmod{m_3}$

$\frac{140}{4} x_1 \equiv 1 \pmod 4 \Rightarrow 35 x_1 \equiv 1 \pmod 4$

$\Rightarrow 3 x_1 \equiv 1 \pmod 4$

$\Rightarrow x_1 = 3$

$\frac{140}{5} x_2 \equiv 1 \pmod 5$

$28 x_2 \equiv 1 \pmod 5$

$3 x_2 \equiv 1 \pmod 5$

$\Rightarrow x_2 = 2$

$\frac{140}{7} x_3 \equiv 1 \pmod 7$

$20 x_3 \equiv 1 \pmod 7$

$6 x_3 \equiv 1 \pmod 7$

$\Rightarrow x_3 = 6$

$X = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 2 \cdot 6$

$= 35 \cdot 3 + 28 \cdot 6 + 20 \cdot 12$

$= 513$

$X \equiv 513 \pmod{140}$

$X \equiv 93 \pmod{140}$

4. Solve the set of Congruences

$x \equiv 1 \pmod 4 \quad x \equiv 0 \pmod 3 \quad x \equiv 5 \pmod 7$

Sunrise 6-06 AM Sunset 6-22 PM

5. Find all integers that give the remainder 1, 2, 3 when divided by 3, 4, 5 respectively.

Hint: $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 4$

$x \equiv 3 \pmod 5$

6. Find the number when given remainder $2/3$, $4/5$ and $6/7$

Hint: $2/3 \Rightarrow x \equiv 2 \pmod 3$

7. Solve $20x \equiv 30 \pmod 4$

Solution: This is of the form $ax \equiv b \pmod m$

$a = 20$, $b = 30$, $m = 4$

$d = (a, m) = (20, 4) = 4$

ie $d \nmid b$

∴ This Congruence has no solution.

8. Solve $4x \equiv 5 \pmod 6$

9. Solve $15x \equiv 24 \pmod{35}$

10. Solve $x^2+x+7 \equiv 0 \pmod{15}$

Solution:

Given $x^2+x+7 \equiv 0 \pmod{15}$ ——— (1)

$15 = 3 \times 5$

(1) can be splitted into two congruences

ie $\left.\begin{aligned} x^2+x+7 &\equiv 0 \pmod 3 \\ x^2+x+7 &\equiv 0 \pmod 5 \end{aligned}\right\}$ ——— (2)

Solution of (2) will give the solution of (1) by Chinese Remainder Theorem.

(i) Consider $x^2+x+7 \equiv 0 \pmod 3$

CRS $= \{0, 1, 2\}$

when $x=0 \Rightarrow 7 \not\equiv 0 \pmod 3$

$x=1 \Rightarrow 9 \equiv 0 \pmod 3$

$x=2 \Rightarrow 13 \not\equiv 0 \pmod 3$

$\therefore x=1$ is a solution of congruence.

(ii) Consider $x^2+x+7 \equiv 0 \pmod 5$

CRS $= \{0, 1, 2, 3, 4\}$

when $x=0$, $7 \not\equiv 0 \pmod 5$

$x=1$, $9 \not\equiv 0 \pmod 5$

$x=2$, $13 \not\equiv 0 \pmod 5$

$x=3$, $19 \not\equiv 0 \pmod 5$

$x=4$, $27 \not\equiv 0 \pmod 5$

There is no solution to this Congruence

$\therefore$ (1) has no solution.

11. Solve $x^2 + x + 7 \equiv 0 \pmod{189}$

Refer the other notes.

12. Find the smallest odd number, show that $3 \mid n$, $5 \mid n+2$, $7 \mid n+4$.

Solution:

$3 \mid n \Rightarrow n \equiv 0 \pmod 3$

$5 \mid n+2 \Rightarrow n+2 \equiv 0 \pmod 5 \Rightarrow n \equiv -2 \pmod 5$

$7 \mid n+4 \Rightarrow n+4 \equiv 0 \pmod 7 \Rightarrow n \equiv -4 \pmod 7$

ie $a_1 = 0 \quad a_2 = -2 \quad a_3 = -4$

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

$M = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105$

By problem (6) $x_1 = 2, \; x_2 = 6, \; x_3 = 8$

$X = -732$

$x \equiv -732 \pmod{105}$

$\equiv -102 \pmod{105}$

$\equiv 3 \pmod{105}$

$\therefore$ The smallest odd Number 3.

13 Solve $15x \equiv 0 \pmod{35}$

Solution: This is of the form

$$ax \equiv b \pmod{m}$$

$a = 15$, $b = 0$, $m = 35$

$d = (a, m) = (15, 35) = 5$

$d \mid b$ ie $d \mid 0$.

This Congruence has $d = 5$ solutions

$$15x \equiv 0 \pmod{35}$$

$$15x - 0 = 35y$$

$$15x - 35y = 0.$$

This is of the form $bx + cy = g$

$$15x \equiv 0 \pmod{35}$$

This is reduced to $3x \equiv 0 \pmod{7}$

$\therefore$ CRS mod 7 is $\{0, 1, 2, \cdots 6\}$

To the above CRS, solution is 0, as There is no multiples of 7.

Consider the mod value 35

The congruence has 5 solutions

$\therefore$ The multiples of 7 is 0, 7, 14, 21, 28.

14. Solve $15x \equiv 25 \pmod{35}$

15. Solve $353x \equiv 254 \pmod{400}$

16. Verify whether the following congruence has solution $x^2 \equiv -1 \pmod{p}$.

$x^2 \equiv -1 \pmod{p}$ has a solution iff $p = 2$ or $p \equiv 1 \pmod{4}$ (Refer back)

Solution:

(i) $p = 7 \neq 2 \Rightarrow 7 \not\equiv 1 \pmod{4}$

$\therefore$ The congruence has no solution.

(ii) $p = 5 \neq 2 \Rightarrow 5 \equiv 1 \pmod{4}$

This congruence has solution.

CRS mod 5 (mod p) is $\{0, 1, 2, 3, 4\}$

$\Rightarrow x^2 + 1 \equiv 0 \pmod{5}$

when $x = 2 \Rightarrow 4 + 1 = 5 \equiv 0 \pmod{5}$

$x = 3 \Rightarrow 9 + 1 = 10 \equiv 0 \pmod{5}$

Hence $x = 2, 3$ are two solutions of the given congruence.

17. Solve $24x \equiv 20 \pmod{28}$
$10x \equiv 6 \pmod{32}$ } —— (1)

Solution:

(1) $\Rightarrow$ $6x \equiv 5 \pmod{7}$ —— (2)

$5x \equiv 3 \pmod{16}$ —— (3)

Find the coverse $ab \equiv 1 \pmod{m}$

(2) $\Rightarrow$ $6k_1 \equiv 1 \pmod{7}$

CRS modulo 7 is $\{0, 1, 2 \cdots 6\}$

Solution is $k_1 = 6$

[$\because$ $6 \times 6 \equiv 1 \pmod{7}$

$36 - 1 \equiv 0 \pmod{7}$]

(3) $\Rightarrow$ $5k_2 \equiv 1 \pmod{16}$

CRS modulo 16 is $\{0, 1, 2 \cdots 15\}$.

Solution is $k_2 = 13$.

[$\because$ $5 \times 13 \equiv 1 \pmod{16}$

$65 - 1 \equiv 0 \pmod{16}$]

(2) $\times 6$ $\Rightarrow$ $6 \times 6x \equiv 5 \times 6 \pmod{7}$

$36x \equiv 30 \pmod{7}$

$x \equiv 2 \pmod{7}$ [$\because \frac{30}{7}$ Rem 2]

(5) $\times 13 \Rightarrow 5 \times 13\, x \equiv 13 \times 3 \pmod{16}$

$65x \equiv 39 \pmod{16}$

$x \equiv 7 \pmod{16}$ $\left(\because \frac{39}{16} \text{ Rem } 7\right)$

Apply CRT

$x \equiv 2 \bmod 7 \; ; \; x \equiv 7 \pmod{16}$

$x \equiv a_i \pmod{m_i}$

$a_1 = 2 \; ; \; m_1 = 7$

$a_2 = 7 \; ; \; m_2 = 16$

$M = m_1 m_2 = 7 \times 16 = 112$

$X = \frac{M}{m_1} x_1 a_1 + \frac{M}{m_2} x_2 a_2$

$\frac{M}{m_1} x_1 \equiv 1 \pmod{m_1} \Rightarrow \frac{112}{7} x_1 \equiv 1 \pmod 7$

$\Rightarrow 16 x_1 \equiv 1 \pmod 7$

$\Rightarrow \boxed{x_1 = 4}$

$\frac{M}{m_2} x_2 \equiv 1 \pmod{m_2} \Rightarrow \frac{112}{16} x_2 \equiv 1 \pmod{16}$

$\Rightarrow 7 x_2 \equiv 1 \pmod{16}$

$\Rightarrow \boxed{x_2 = 7}$

and is steadfast and sense controlled sees

$$X = \frac{112}{7} 4 \times 2 + \frac{112}{16} 7 \times 7$$

$$= 16 \times 8 + 7 \times 49$$

$$= 471$$

$$x \equiv 471 \pmod{112}$$

$$x \equiv 23 \pmod{112}$$

18. Determine whether the system $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$, $x \equiv 5 \pmod{84}$ has a solution and find them all if they exist.

19. Solve the set of Congruence

Repeat (3)

$x \equiv 1 \pmod{4}$; $x \equiv 0 \pmod{3}$; $x \equiv 5 \pmod{7}$

20. Verify whether the following

(i) $x^2 \equiv -1 \pmod{7}$ (ii) $x^2 \equiv 1 \pmod{5}$

21. Solve the Congruence $x^3 + 2x - 3 \equiv 0 \pmod{45}$

22. Solve $x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod{7}$