SARDAR PATEL UNIVERSITY , VALLABH VIDYANAGAR
SYLLABUS FOR B.Sc. SEMESTER - 6
US06DMTH26(T)(NUMBER THEORY - 2)
TWO HOURS PER WEEK (2 CREDIT)
Effective from June 2020
Marks:-50 (External)

UNIT-1
Linear indeterminate equations and its solution ,General solution of Linear indeterminate equation with three unknown , Pythagoras (Shang-gao indeterminate) equation and its solution.

UNIT-2
Congruences : Definition and examples , Properties of congruences ,Necessary and sufficient condition for a positive integer can be divided by 3,9,4,7,11 or 13 .

UNIT-3
Complete residue system(mod m) and its properties , Reduced residue system(mod m) and its properties , Euler's theorem,Fermat's theorem , Properties of Euler's function .

UNIT-4
Congruence in one unknown , Solution of Linear congruence in one unknown and two unknown, Chinese theorem ,Solution of system of congruences.

Recommended texts :

C.Y.Hsiung, Elementary Theory of numbers, Allied publishers Ltd.(1992)

Reference Books:

1. D.Burton , elementary Number Theory, 6th Ed , Tata McGraw-Hill Edition,Indian reprint.
2. I.Niven And H.Zuckermar , An Introduction to the theory of Numbers, Wiley-Eastern Publication.
3. S.Barnard and J.N.Child , Higher Algebra, Mc Millan and Co. Ltd.
4. Neville Robinns, Beginning Number Theory , 2nd Ed.,Narosa Publishing House Pvt.Ltd. Delhi,2007

SARDAR PATEL UNIVERSITY
B.Sc.(MATHEMATICS) SEMESTER - IV
QUESTION BANK OF US06DMTH26
(Number Theory - 2)

....

Unit-1

1. (i)Prove that the indeterminate equation $ax + by = c$ has solution iff d/c, where $(a, b) = d$. 2
   (ii)If $x = x_0, y = y_0$ is a particular solution of $ax + by = c$ then prove that general solution can be written as $x = x_0 + \frac{b}{d}\,t$; $y = y_0 - \frac{a}{d}\,t$, where $t \in \mathbb{Z}$. 4

2. If $(a, b) = 1$ then prove that any solution of $ax + by = c$ can be written as $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$, where $x = x_0$; $y = y_0$ are particular a solution of $ax + by = c$. 4

3. Solve the equation $525x + 231y = 42$. 4

4. Find positive integer solution of following equation
   (i) $7x + 19y = 213$
   (ii) $19x + 20y = 1909$ 4
   (iii) $x^2 + xy - 6 = 0$ 2
   (iv) $7x + 19y = 213$ (v) $y - \frac{x + 3y}{x + 2} = 1$ 4

5. Find general solution of equation
   (i) $50x + 45y + 36z = 10$ 4
   (ii) $8x - 18y + 10z = 16$ 3
   (iii) $50x + 45y + 60z = 10$ 4

6. Find all relatively prime solution of $x^2 + y^2 = z^2$ with $0 < z < 30$. 3

7. Prove that the positive integer solution of $x^{-1} + y^{-1} = z^{-1}$, $(x, y, z) = 1$ has and must have the form $x = a(a + b)$, $y = b(a + b)$, $z = ab$, where a , $b > 0$, $(a, b) = 1$. 6

8. Prove that the general integer solution of $x^2 + y^2 = z^2$ with x , y , $z > 0$, $(x, y) = 1$ and y even is given by $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$, where$a$, $b > 0$, $(a, b) = 1$ and one of a,b is odd and the other is even. 6

9. Prove that the integer solution of $x^2 + 2y^2 = z^2$,(x,y)=1 can be expressed as $x = \pm(a^2 - 2b^2)$, $y = 2ab$, $z = a^2 + 2b^2$. 6

10. Prove that the integer solution of $x^{-2} + y^{-2} = z^{-2}$, $(x, y, z) = 1$ is given by $x = (a^4 - b^4)$, $y = 2ab(a^2 + b^2)$, $z = 2ab(a^2 - b^2)$, where $a > b > 0$, $(a, b) = 1$ and a,b both can not be odd or even . 6

11. Prove that a general integer solution of $x^2 + y^2 + z^2 = w^2$, $(x, y, z, w) = 1$ is given by $x = (a^2 - b^2 + c^2 - d^2)$, $y = 2ab - 2cd$, $z = 2ad + 2bc$, $w = a^2 + b^2 + c^2 + d^2$. 7

12. Prove that the equation $x^4 + y^4 = z^2$ has no solution with nonzero positive integers x , y , z . Hence prove that $x^4 - 4y^4 = z^2$ has no nonzero positive integer solution. 6
    OR : Prove that $x^4 + y^4 = z^2$ has no nonzero positive integer solution.

Unit-2

1. Define Congruent modulo n .

2. Prove that $a \equiv b(mod\ n)$ iff a and b have the same nonnegative remainder when divided by n. 3

3. Prove that congruent is an equivalent relation. 2

4. If $a_1 \equiv b_1 (mod\ n)$ and $a_2 \equiv b_2 (mod\ n)$,then prove the following:

   (a) $a_1 + a_2 \equiv b_1 + b_2 (mod\ n)$ 2

   (b) $ca_1 \equiv cb_1 (mod\ n)$, $\forall\ c \in \mathbb{Z}$. 2

   (c) $c + a_1 \equiv c + b_1 (mod\ n)$, $\forall\ c \in \mathbb{Z}$ 2

   (d) $a_1 a_2 \equiv b_1 b_2 (mod\ n)$ 2

   (e) ${a_1}^m \equiv {b_1}^m (mod\ n)$, $\forall\ m \in \mathbb{N}$, by using mathematical induction method. 3

5. If $ca \equiv cb(mod\ n)$ and $(c, n) = 1$ then prove that $a \equiv b(mod\ n)$ 3

6. Prove that $x^2 + y^2 = z^2$ has no prime solution. 3
   OR: Prove that Pythagoras equation has no prime solution.

7. Prove that a positive integer n is divided by 3 iff the sum of its digits is divisible by 3. 4
   OR : Prove that $3/n$ iff 3/(sum of digits of n) .

8. Prove that a positive integer n is divided by 9 iff the sum of its digits is divisible by 9. 4

9. Find a necessary and sufficient condition that a positive integer is divisible by 11. 4

10. Find a necessary and sufficient condition that a positive integer is divisible by 7. 4

11. Find a necessary and sufficient condition that a positive integer is divisible by 13. 4

12. Prove that every number containing more than two digits can be divided by 4 iff the number formed by last two digits can be divided by 4. 4

13. Is 765432 divided by 3,4,5,7,9,11,13 ? 2

14. Is 527590 divided by 11 ? 2

15. Is 237897 and 73912 are divided by 11 ? 2

16. Using divisibility test check whether 27720 is divisible by 2,3,4,5,7,9,11 or not .

17. If $a \equiv b(mod\ m)$; $a \equiv b(mod\ n)$ and $(m, n) = k$ then prove that $a \equiv b(mod\ k)$ 2

Unit- 3

1. Define complete residue system modulo m and reduced residue system modulo m with example . 2

2. Prove that a set of k integers $a_1, a_2, a_3 \ldots, a_k$ is a complete residue system modulo m iff
   (i) $k = m$ (ii)$a_i \neq a_j (mod\ m)$, $\forall\ i \neq j$. 3

3. If $a_1, a_2, a_3 \ldots, a_k$ is CRS modulo m and $(a, m) = 1$,then prove that
   $aa_1 + b, aa_2 + b, aa_3 + b, \ \ldots\ , aa_k + b$ forms a CRS mod m , where b is any integer. 2

4. Prove that a set of k integers $a_1, a_2, a_3, \ldots, a_k$ is a reduced residue system modulo m iff
   (i)$k = \Phi(m)$ (ii)$(a_i, m) = 1$, $\forall\ i$ (iii) $a_i \neq a_j (mod\ m)$, $\forall\ i \neq j$. 3

5. If a_1 , a_2 , a_3 , ... , $a_{\Phi(m)}$ is RRS modulo m and $(a, m) = 1$,then prove that
   (i) aa_1 , aa_2 , aa_3 , ... , $aa_{\Phi(m)}$ is RRS mod m. 2
   (ii) $aa_1 + b$, $aa_2 + b$, $aa_3 + b$, ... , $aa_{\Phi(m)} + b$ is not RRS mod m , where b is any integer. 1

6. Is $\{27, 80, 96, 113, 64\}$ a CRS modulo 5 ? Justify . 2

7. Check whether $\{26, 37, 48, 59, 10\}$ is a CRS modulo 5 or not. 2

8. Is $\{83, 84, 85, 86, 87, 88\}$ a CRS modulo 6 ? Justify. 2

9. State and prove Euler's theorem. 3
   OR : If $(a, p) = 1$, p is prime , then prove that $a^{p-1} \equiv 1(mod\ p)$.

10. State and prove Fermat's theorem. OR: State and prove Fermat's little theorem. 2

11. If $a^n \equiv 1(mod\ m)$ and d is order of a modulo m then prove that d/n . 2

12. Define Euler's function . Prove that Euler's function is multiplicative function. 5

13. Prove that Euler's function is multiplicative function and hence find $\phi(142296)$ 5
    OR :If $(a, b) = 1$ then prove that $\phi(ab) = \phi(a)\phi(b)$.

14. Find all positive integers m and n such that $\phi(mn) = \phi(m) + \phi(n)$. 5

15. Prove that $\Phi(p^k) = p^k - p^{k-1}$,where p is prime. 4
    OR : Prove that $\Phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$, where p is prime.

16. Find $\phi(128)$, $\phi(625)$, $\phi(81)$. 2

17. In usual notation prove that $\sum_{i=0}^{k} \Phi(p^i) = p^k$, where p is prime. 4

18. Find $\phi(32) + \phi(16) + \phi(8) + \phi(4) + \phi(2) + \phi(1)$ OR Find $\sum_{i=0}^{5} \Phi(2^i)$. 2

19. Find $\phi(243) + \phi(81) + \phi(27) + \phi(9) + \phi(3)$ 2

20. If $m = p_1^{m_1} p_2^{m_2} p_3^{m_3} \dots p_k^{m_k}$,where all p_i are primes then prove that 4
    $\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$.

21. Prove that $\phi(ab) = \frac{\phi(a)\phi(b)d}{\phi(d)}$, where $d = (a, b)$. 4

22. Prove that the sum of $\phi(m)$ positive integers less than m $m > 1$ and relatively prime to m is $\frac{m}{2}\phi(m)$. 4

23. If m is positive integer then prove that $\Phi(m) = m\sum_{d/m} \frac{\mu(d)}{d} = \sum_{d/m} \mu\left(\frac{m}{d}\right) d$. 5

24. Prove that $\sum_{d/m} \mu(d)\phi(d) = 0$ iff m is even. 5

25. Prove that m is prime iff $\phi(m) + S(m) = mT(m)$. 7

Unit- 4

1. Define Congruence in one unknown .

2. Prove that $ax + b \equiv 0(mod\ m)$,where (a,m)=1 has exactly one solution$x \equiv -a^{\phi(m)-1}\ b\ (mod\ m)$. 2

3. Prove that $ax + b \equiv 0(mod\ m)$, where$(a, m) = d$, $d > 1$ has solution iff d/b.Also prove that it has d solutions $x_i \equiv a + i\frac{m}{d}(mod\ m)$, $i = 0, 1, 2, \dots, d - 1$, of which $x \equiv a\left(mod\ \frac{m}{d}\right)$ is unique solution of $\frac{a}{d}x + \frac{b}{d} \equiv 0\left(mod\ \frac{m}{d}\right)$. 6

4. Prove that $ax + by + c \equiv 0(mod\ m)$ has solution iff d/c , where $d = (a, b, m)$. Also prove that it has md solutions. 4

5. Prove that the system of congruences , $x \equiv a(mod\ m)$; $x \equiv b(mod\ n)$ has solution iff $a \equiv b(mod\ (m, n))$. Also prove that system has unique solution with respect to modulo $[m, n]$. 5

6. If $(a, m) = 1$ $a^{m-1} \equiv 1(mod\ m)$, and $a^n \not\equiv 1(mod\ m)$ for any proper divisor n of $m - 1$ then prove that m is prime . 3

7. Solve the equation 4
   (i) $12x + 15 \equiv 0(mod\ 45)$(ii) $18x \equiv 30(mod\ 42)$(iii) $9x \equiv 21(mod\ 30)$
   (iv) $103x \equiv 57(mod\ 211)$(v) $111x \equiv 75(mod\ 321)$ (vi) $863x \equiv 880(mod\ 2151)$
   (vii) $2x + 7y \equiv 5(mod\ 12)$ (viii) $6x + 15y \equiv 9(mod\ 18)$

8. State and prove Chinese remainder theorem . OR : State and prove Sun-Tsu theorem. 6

9. Solve the system of congruences 5
   (i) $x \equiv 2(mod\ 3)$; $x \equiv 3(mod\ 5)$; $x \equiv 2(mod\ 7)$.
   (ii) $x \equiv 1(mod\ 4)$; $x \equiv 3(mod\ 5)$; $x \equiv 2(mod\ 7)$
   (iii) $2x \equiv 1(mod\ 5)$; $3x \equiv 1(mod\ 7)$.
   (iv) $x \equiv -2(mod\ 12)$; $x \equiv 6(mod\ 10)$; $x \equiv 1(mod\ 15)$

10. Find order of 5 modulo 13 . 2

11. Find order of 2 modulo 7 . 2

NUMBER THEORY

Unit 4

....

✠ Congruence equation in one unknown

Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, then congruence equation in one unknown and of n^{th} order is of the form $f(x) \equiv 0 \ (mod \ m)$, $a_n \not\equiv 0 \ (mod \ m) \ (i.e. \ m \nmid a_m)$

★ $f(a) \equiv 0 \ (mod \ m)$, then we say that $x \equiv a \ (mod \ m)$ is solution of $f(x) \equiv 0 \ (mod \ m)$.

⁎ **Theorem 1 :** Prove that $ax + b \equiv 0 \ (mod \ m)$, where $(a, m) = 1$ has exactly one solution $x \equiv -a^{\phi(m)-1} \ b(mod \ m)$.

Proof :

Here,$(a, m) = 1 \ and \ ax + b \equiv 0 \ (mod \ m)$. ....(1)

Let $x_1, x_2, ..., x_m$ be a CRS modulo m.

$\Rightarrow ax_1, ax_2, ..., ax_m$ be also CRS modulo m.

$\Rightarrow ax_1 + b, ax_2 + b, ..., ax_m + b$ be also CRS modulo m.

Then, Exactly one of them say, $ax_k + b$

$$ax_k + b \equiv 0 \ (mod \ m).$$

$\therefore$ We say that equation (1) has exactly one solution.

Also, (a,m)=1

$\Rightarrow a^{\phi(m)} \equiv 1 \ (mod \ m)$ ($\because$ By Euler's Theorem)

$\Rightarrow a^{\phi(m)}x \equiv x \ (mod \ m)$ ....(2)

Also, by (1) $ax + b \equiv 0 \ (mod \ m)$.

$\Rightarrow ax \equiv -b \ (mod \ m)$

$\Rightarrow a^{\phi(m)-1} \ ax \equiv -a^{\phi(m)-1} \ b \ (mod \ m)$

$\Rightarrow a^{\phi(m)} \ x \equiv -a^{\phi(m)-1} \ b \ (mod \ m)$ ....(3)

by (2) and (3), we get

$$x \equiv -a^{\phi(m)-1} \ b \ (mod \ m) .$$

Hence Proved.

⁎ **Theorem 2 :** Prove that $ax + b \equiv 0(mod \ m)$, where $(a, m) = d, \ d > 1$ has solution if and only if $d \mid b$. Also prove that it has d solutions. $x_i \equiv a + i\frac{m}{d} \ (mod \ m), i = 0, 1, 2, ..., d-1.$ of which $x \equiv a \ (mod \ \frac{m}{d})$ is unique solution of

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \ (mod \ \frac{m}{d})$$

Proof :

Here, $(a, m) = d$ and $ax + b \equiv 0 \ (mod \ m) \Rightarrow m \mid ax + b$

Now, $(a, m) = d \Rightarrow \ d \mid m \ , \ d \mid a$

Now, $d \mid m \ \ \& \ \ m \mid (ax + b) \Rightarrow \ d \mid (ax + b). \ \Rightarrow \ d \mid ax.$

Thus, we have $d \mid ax \ \ \& \ \ d \mid (ax + b)$

$\Rightarrow d \mid (ax + b - ax)$

$\Rightarrow d \mid b$

Converse Part:
We have $d \mid b$ and $(a, m) = d. \Rightarrow \left(\frac{a}{d}, \frac{m}{d} \right) = 1.$
here, $\frac{b}{d} \in Z$
$\therefore \; \frac{a}{d}x + \frac{b}{d} \equiv 0 \; (mod \; \frac{m}{d})$ has solution.

$\Rightarrow ax + b \equiv 0 \; (mod \; m)$ has solution.
We have $ax + b \equiv 0 \; (mod \; m), \; d = (a, m)$ ....(1)
Here $d \mid b$, So Equation (1) has Solution.
Let $x = x_1$ is solution of equation (1)
i.e $ax_1 + b \equiv 0 \; (mod \; m)$ ....(2)

Claim : $x = x_1 + \frac{m}{d}t, \; t \in Z$ is also Solution of (1)

Now, $a\left(x_1 + \frac{m}{d}t\right) = ax_1 + \frac{a}{d}mt$

$$\Rightarrow ax_1 + \frac{a}{d}mt \equiv (-b) + 0 \; (mod \; m)$$

$$\Rightarrow a\left(x_1 + \frac{m}{d}t\right) + b \equiv 0 \; (mod \; m)$$

$\Rightarrow x = x_1 + \frac{m}{d}t$ is solution of (1), $t \in Z$

By Division Algorithm on t and d

$$t = qd + r, \quad 0 \leq r < d \;\; or \;\; 0 \leq r \leq d - 1$$

$$x = x_1 + \frac{m}{d}(qd + r)$$

$$\Rightarrow x = x_1 + mq + \frac{m}{d}r$$

$$\Rightarrow x \equiv x_1 + 0 + \frac{m}{d}r \; (mod \; m)$$

$$\Rightarrow x \equiv x_1 + \frac{m}{d}r \; (mod \; m), \quad 0 \leq r \leq d - 1$$

Put $t = 0, 1, 2, ..., d - 1$

Consider set of d Solutions

$\left(x_1, x_1 + \frac{m}{d}, x_1 + 2\frac{m}{d}, ..., x_1 + (d-1)\frac{m}{d}\right)$ ....(3)

Taking $t_1, \; t_2 \in$ 0,1,2,....,d-1 such that

$$x_1 + t_1\frac{m}{d} \equiv x_1 + t_2\frac{m}{d} \; (mod \; m)$$

$$\Rightarrow t_1 \equiv t_2 \; (mod \; m) \;\; \Rightarrow \;\; m \mid (t_1 - t_2)$$

We Have, $d = (a, m) \Rightarrow d \mid m \ \ \& \ \ m \mid (t_1 - t_2)$

$\Rightarrow d \mid (t_1 - t_2)$

$\Rightarrow d \mid (|t_1 - t_2|)$

But $0 \leq t_1 - t_2 \leq d - 1$

This is Possible when $t_1 - t_2 = 0 \quad \Rightarrow \quad t_1 = t_2$

$\therefore$ Integers of set (3) are Incongruent Solution.

Hence Proved.

⁎ **Theorem 3:** Prove that $ax + by + c \equiv 0 \ (\ mod \ m \ )$ has solution. if and only if $d \mid c$. where, $d = (a, b, m)$ and also prove that it has total md solutions.

Proof:

First, let $ax + by + c \equiv 0 \ (\ mod \ m \ )$ has solution. ....(1)
Here, (a , b , m)=d, then

$\Rightarrow d \mid a \ , \ d \mid b \ , \ d \mid m.$
$\Rightarrow d \mid ax \ , \quad d \mid by \ , \quad d \mid m.$

Now, $d \mid m$ and by (1) $\Rightarrow \ m \mid (ax + by + c)$

$\Rightarrow d \mid ax + by + c$

Now, we have $d \mid ax, \ d \mid by, \ d \mid (ax + by + c)$

$\Rightarrow d \mid (ax + by + c - ax - by)$
$\Rightarrow d \mid c$

Converse Part:
If $d \mid c$ then we have to prove that $ax + by + c \equiv 0 \ (mod \ m)$ has solution.
Here, (a , b , m) = d,

Let $d_1 = (a, m)$, then $d = (d_1, b)$.
Since, $d \mid c$ and $d = (b, d_1)$.
so, $by + c \equiv 0 \ (mod \ d_1)$ has solution. ....(2) [by theorem (2)]

Clearly, Eq. (2) has total d solution.

By, Eq. (2) we say that $d_1 \mid by + c$.
$\Rightarrow by + c = c_1 d_1$ for some $c_1 \in Z$

we can write, $d_1 \mid c_1 d_1$, $(a, m) = d_1$, then by thm(2), we say that
$ax + c_1 d_1 \equiv 0 \ (\ mod \ m \ )$ has solution. ....(3)
clearly, Eq. (3) has d_1 solution.

Thus, $ax + by + c \ \equiv \ 0 \ (mod \ m)$ has solution.
Now, we prove that $ax + by + c \ \equiv \ 0 \ (mod \ m)$ has total 'md' solutions.

From Eq.(2) we say that,
$by + c \equiv 0 \ (mod \ d_1\ )$ has total 'd' solution with modulo d_1.

$$\therefore \frac{m}{d_1} \ by \ + \ \frac{m}{d_1} \ c \ \equiv \ 0 \ (mod \ \frac{m}{d_1} d_1) \text{ has solution.}$$

also, it has $\left(\frac{m}{d_1} b \ , \frac{m}{d_1} d_1 \ \right) = \frac{m}{d_1} \ (b, d_1) \ = \frac{m}{d_1} \ d$ solution with modulo m. ....(4)

Now, by Eq. (3),

$ax + c_1 d_1 \ \equiv \ 0 \ (mod \ m)$ has total 'd_1' solution with modulo m.

Hence, given Eq (1) has total $\frac{m}{d_1} d \times d_1$ solution.
i.e. total 'md' solutions.

Hence proved.

⋇ **Theorem 4 :** Prove that the system of congruences, $x \equiv a \ (mod \ m)$, $x \equiv b \ (mod \ n)$ has solution iff $a \equiv b \ (mod \ (m, n)\ )$.Also prove that system has unique solution with respect to modulo [m , n].

Proof:
Let x = c is solution of given system, then
$c \ \equiv \ a \ (\ mod \ m \ ), \ c \ \equiv \ b \ (\ mod \ n \ ).$
$\Rightarrow m \mid c - a, \ \ n \mid c - b$

Let (m , n) = d, then $d \mid m \ , \ \ d \mid n$
$\Rightarrow d \mid c - a, \quad d \mid c - b$

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

$\Rightarrow d \mid a - b$

$\Rightarrow a \ \equiv \ b(\ mod \ d \ ).$

Thus $a \ \equiv \ b \ (\ mod \ (m \ , \ n) \ )$

Converse Part

If $a \ \equiv \ b \ (\ mod \ (m \ , \ n) \ )$
$a \ \equiv \ b(\ mod \ d \ ).$ where d = (m , n).
$\Rightarrow \ d \mid a - b$

Thus, $d \mid a - b$ and (m , n) = d.
then, by theorem we say that
$my \ + \ (a - b) \ \equiv \ 0 \ (mod \ n)$ has solution say, y_1
$my_1 \ + \ (a - b) \ \equiv \ 0 \ (mod \ n)$
$\Rightarrow \quad a \ + \ my_1 \ \equiv \ b \ (mod \ n)$ ....(1)

we can write $m \mid my_1$

$\Rightarrow \quad m \mid a + my_1 - a$

$\Rightarrow \quad a + my_1 \equiv a \ (mod \ m)$ ....(2)

By (1) and (2),

$x = a + my_1$ is a solution of given system.

Hence, given system has solution.

Now, we prove that system has unique solution.

Suppose, x_1 and y_1 are two solutions of given system,then

$x_1 \equiv a \ (\ mod \ m \ ), \quad x_1 \equiv b \ (\ mod \ n \ )$

. &

$y_1 \equiv a \ (\ mod \ m \ ), \quad y_1 \equiv b \ (\ mod \ n \ )$

$\Rightarrow \quad x_1 \equiv y_1 \ (\ mod \ m \ ), \quad x_1 \equiv y_1 \ (\ mod \ n \ )$

$\Rightarrow \quad m \mid x_1 - y_1, \quad n \mid x_1 - y_1$

$\Rightarrow \quad [m, n] \mid x_1 - y_1$

$\Rightarrow \quad x_1 \equiv y_1 \ (\ mod \ [m, n] \ )$

Thus, system has Unique solution with respect to modulo [m , n].

Remark : If $a^{m-1} \equiv 1 \ (mod \ m)$ and d is the order of a modulo m, then $d \mid n$.

⁎ **Theorem 5 :** If $(a, m) = 1$, $a^{m-1} \equiv 1 \ (mod \ m)$ and $a^n \not\equiv 1 \ (mod \ m)$ for any proper divisor n of m-1 then prove that m is prime.

Proof :

From the above remark, We know that m-1 is the order of a modulo m.

By Euler's Theorem $\Rightarrow \ a^{\phi(m)} \equiv 1 \ (mod \ m)$

Hence, $\phi(m) \geq m - 1$,

But for any integers $m > 1$, we must have $\phi(m) \leq m - 1$,

Thus $\phi(m) = m - 1$, i.e m is prime.

Hence Proved.

⁎ **Theorem 6 :** State and Prove Chinese Remainder Theorem.

or

State and Prove Sun-Tsu Theorem.

Statement :

Let $m_1, m_2, ..., m_k$ be pairwise relatively prime positive integers.

The system of congruences $x \equiv a_i \ (mod \ m_i), \forall i = 1, 2, ..., k$ has unique solution.

$$x \equiv \sum_{i=1}^{k} \frac{m}{mi} xia_i \ (mod \ m)$$

where $m = m_1 \cdot m_2 ......m_k, \quad \dfrac{m}{m_i} x_i \equiv 1 \ (mod \ m_i)$

Proof :

Let $m = m_1 m_2.....m_k$, then

$\dfrac{m}{m_i} = m_1 m_2.....m_{i-1} m_{i+1}.....m_k,$

Clearly , $\left(\dfrac{m}{m_i}, m_i \right) = 1 \ \forall i$ ....(1)

$\therefore$ By Theorem (1), we can write

$\dfrac{m}{m_i} \ x \equiv \ 1 \ (mod \ m_i)$ has solution say x_i.

Thus, $\dfrac{m}{m_i} x_i \equiv 1 \ (mod \ m_i) \ \forall i = 1, 2, ..., k$ ....(2)

By equation (1), we say that

$$m_j \mid \frac{m}{m_i} \quad , \forall j \neq i$$

$$\Rightarrow \frac{m}{m_i} \equiv 0 \ (mod \ m_j), \quad \forall j \neq i.$$

$$\Rightarrow \frac{m}{m_i} a_i x_i \equiv 0 \ (mod \ m_j), \quad \forall j \neq i.$$

$$\Rightarrow \sum_{i=1}^{k} \frac{m}{mi} aix_i \equiv 0 \ (mod \ m_j), \quad \forall j \neq i.$$

$$\Rightarrow \sum_{i=1}^{k} \frac{m}{mi} aix_i \equiv \frac{m}{m_j} a_j x_j \ (mod \ m_j), \ \forall j = 1, 2, ..., k.$$

$$\Rightarrow \sum_{i=1}^{k} \frac{m}{mi} aix_i \equiv a_j \ (mod \ m_j), \ \forall j = 1, 2, ..., k. \qquad \text{(By equation (2))}$$

Thus, $\sum_{i=1}^{k} \dfrac{m}{mi} aix_i$ is solution of given system.

Hence, $x \equiv \sum_{i=1}^{k} \dfrac{m}{mi} aix_i \ (mod \ m_j), \ \forall j = 1, 2, ..., k.$

$\Rightarrow x \equiv \sum_{i=1}^{k} \dfrac{m}{mi} aix_i \ (mod \ m)$ is a required solution.

♦ Now, We Prove Uniqueness

If y is another solution of given congruences then

$y \equiv a_i \ (mod \ m_i) \ and \ x \equiv a_i \ (mod \ m_i) \quad i = 1, 2, ..., k$

$\Rightarrow y \equiv x \ (mod \ m_i). \ \forall i = 1, 2, .., k.$

$\Rightarrow y \equiv x \ (mod \ m_1 \cdot m_2.....m_k)$

$\Rightarrow y \equiv x \ (mod \ m)$

Hence, Given system has Unique Solution.

Solve the equation.

(1) $111x \equiv 75\ (mod\ 321)$
Sol.
Here, compare the given eq. with $ax + b \equiv 0\ (mod\ m)$

$$a = 111, \quad b = -75, \quad m = 321$$
$$(a, m) = (111, 321) = 3 \ \text{ and } \ 3 \mid (-75)$$

$\therefore$ Given eq. has solution, it has 3 solution.

$$111x \equiv 75\ (mod\ 321)$$

$$\begin{aligned}
&\Rightarrow\ 37x \equiv 25\ (mod\ 107)\\
&\Rightarrow\ 107 \mid 37x - 25\\
&\Rightarrow\ 37x - 25 - 107y = 0, \quad y \in Z\\
&\Rightarrow\ 37(x - 3y - 1) + 4y + 12 = 0\\
&\Rightarrow\ 37u + 4y + 12 = 0, \text{ where } u = x - 3y - 1\\
&\Rightarrow\ u = 0, \quad y = (-3)
\end{aligned}$$

Now, from eq of u

$$\Rightarrow\ x = (-8)$$

$\therefore x \equiv (-8)\ (mod\ 107)$
$\therefore x \equiv 99\ (mod\ 107)$
$\therefore x_0 = 99$ is Perticular Solution.

Hence, Required Solution are

$$x = x_0 + \frac{m}{d}t\ , \qquad 0 \le t \le d - 1$$
$$x = 99 + 107t\ , \qquad t = 0, 1, 2$$

i.e $x \equiv$ 99, 203, 315 (mod 321) are required Solution.

(2) $6x + 15y \equiv 9\ (mod\ 18)$
Sol.
Here, (6,15,18)=3 and $3 \mid (-9)$,
$\therefore$ Given eq. has solution, it has $18 \cdot 3 = 54$ solution.

$$6x + 15y \equiv 9\ (mod\ 18)$$

$$\begin{aligned}
&\Rightarrow\ 2x + 5y \equiv 3\ (mod\ 6)\\
&\Rightarrow\ 6 \mid 2x + 5y - 3\\
&\Rightarrow\ 2x + 5y - 3 - 6z = 0, \quad z \in Z\\
&\Rightarrow\ 2(x + 2y - 3z - 1) + y - 1 = 0\\
&\Rightarrow\ 2u + y - 1 = 0, \text{ where } u = x + 2y - 3z - 1\\
&\Rightarrow\ y = 1 - 2u
\end{aligned}$$

Now, from eq of u

$$\Rightarrow\ x = 5u + 3z - 1$$

Hence The Required Solutions are,

$x \equiv 5u + 3z - 1 \ (mod\ 18), \quad y \equiv 1 - 2u \ (mod\ 18)$
where, z=0 to 5 and u= 0 to 8.

H.W:

(3) $12x + 15 \equiv 0 \ (mod\ 45)$
Sol.
Here, compare the given eq. with $ax + b \equiv 0 \ (mod\ m)$

$$a = 12, \quad b = 15, \quad m = 45$$
$$(a, m) = (12, 45) = 3 \ \text{ and } \ 3 \mid 15$$

$\therefore$ Given eq. has solution, it has 3 solution.

$$12x + 15 \equiv 0 \ (mod\ 45)$$
$$\Rightarrow \ 4x + 5 \equiv 0 \ (mod\ 15)$$
$$\Rightarrow \ 15 \mid 4x + 5$$
$$\Rightarrow \ 4x + 5 - 15y = 0, \quad y \in Z$$
$$\Rightarrow \ x = 10, \quad y = 3$$

$\therefore x_0 = 10$ is Perticular Solution.

Hence, Required Solution are

$$x = x_0 + \frac{m}{d}t \ , \qquad 0 \leq t \leq d - 1$$
$$x = 10 + 15t \ , \qquad t = 0, 1, 2$$

i.e $x \equiv$ 10, 25, 40 (mod 45) are required Solution.

(4) $18x \equiv 30 \ (mod\ 42)$
Sol.
Here, compare the given eq. with $ax + b \equiv 0 \ (mod\ m)$

$$a = 18, \quad b = -30, \quad m = 42$$
$$(a, m) = (18, 42) = 6 \ \text{ and } \ 6 \mid (-30)$$

$\therefore$ Given eq. has solution, it has 6 solution.

$$18x \equiv 30 \ (mod\ 42)$$
$$\Rightarrow \ 3x \equiv 5 \ (mod\ 7)$$
$$\Rightarrow \ 7 \mid 3x - 5$$
$$\Rightarrow \ 3x - 5 - 7y = 0, \quad y \in Z$$
$$\Rightarrow \ x = 4, \quad y = 1$$

$\therefore x_0 = 4$ is Perticular Solution.

Hence, Required Solution are

$$x = x_0 + \frac{m}{d}t \;, \qquad 0 \le t \le d-1$$
$$x = 4 + 7t \;, \qquad t = 0, 1, 2, 3, 4, 5$$

i.e $x \equiv$ 4,11,18,25,32,39 (mod 42) are required Solution.

(5) $9x \equiv 21 \ (mod \ 30)$
Sol.
Clearly,

$$(9, 30) = 3 \;\text{ and }\; 3 \mid -21$$

$\therefore$ Given Eq. has solution, it has 3 solution.
Here,

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

$$\begin{aligned}
&\Rightarrow 3x \equiv 7 \ (mod \ 10) \\
&\Rightarrow \ 10 \mid 3x - 7 \\
&\Rightarrow \ 3x - 7 - 10y = 0, \quad y \in Z \\
&\Rightarrow \ x = 9, \quad y = 2
\end{aligned}$$

$\therefore x_0 = 9$ is Perticular Solution.

Hence, Required Solution are

$$x = x_0 + \frac{m}{d}t \;, \qquad 0 \le t \le d-1$$
$$x = 9 + 10t \;, \qquad t = 0, 1, 2$$

i.e $x \equiv$ 9, 19, 29 (mod 30) are required Solution.

(6) $103x \equiv 57 \ (mod \ 211)$
Sol.
Clearly,

$$(103, 211) = 1 \;\text{ and }\; 1 \mid (-57)$$

$\therefore$ Given Eq. has solution, it has one solution.
Here,

$$\begin{aligned}
&103x \equiv 57 \ (mod \ 211) \\
&\Rightarrow 211 \mid 103x - 57 \\
&\Rightarrow 103x - 57 = 211y, \;\; y \in Z \\
&\Rightarrow 103x - 211y - 57 = 0 \\
&\Rightarrow 103(x - 2y) - 5y - 57 = 0, \\
&\Rightarrow 103u - 5y - 57 = 0 \text{ where, } \quad u = x - 2y \;.......(1) \\
&\Rightarrow 5(20u - y - 11) + 3u - 2 = 0 \\
&\Rightarrow 5v + 3u - 2 = 0 \qquad \text{where, } v = 20u - y - 11 \;.......(2) \\
&\text{so,} \qquad v = 1, \; u = -1
\end{aligned}$$

$$\text{by, (2) } v = 20u - y - 11 \Rightarrow y = -32$$
$$\text{by, (1) } u = x - 2y \Rightarrow x = -65$$

$x \equiv -65 \ (mod\ 211\ )$
$\therefore x \equiv 146 \ (mod\ 211\ )$ is required solution.

(7) $863x \equiv 880 \ (mod\ 2151)$
Sol.
Clearly,

$$(863, 2151) = 1 \quad \text{and} \quad 1 \mid (-880)$$

$\therefore$ Given Eq. has solution, it has one solution.

Here,

$$\begin{aligned}
& 863x \equiv 880 \ (mod\ 2151) \\
\Rightarrow\ & 2151 \mid 863x - 880 \\
\Rightarrow\ & 863x - 2151y - 8800 \\
\Rightarrow\ & 863(x - 2y - 1) - 425y - 17 = 0 \\
\Rightarrow\ & 863u - 425y - 17 = 0 \quad \text{where, } \ u = x - 2y - 1 \qquad ....(1) \\
\Rightarrow\ & 425(2u - y) + 13u - 17 = 0 \\
\Rightarrow\ & 425v + 13u - 17 = 0 \quad \text{where, } \ v = 2u - y \qquad ....(2) \\
\Rightarrow\ & 13(32v + u) + 9v - 17 = 0 \\
\Rightarrow\ & 13w + 9v - 17 = 0 \qquad \text{where, } \ w = 32v + u \\
\Rightarrow\ & w = 2\ , \quad v = -1
\end{aligned}$$

Now, $w = 32v + u \quad \Rightarrow \quad u = 34$
By, (2) $y = 69$
By, (1) $x = 173$
$\Rightarrow x \equiv 173 \ (mod\ 2151)$ is required solution.

(8) $2x + 7y \equiv 5 \ (mod\ 12)$
Sol.
Here, $\quad$ (2,7,12)=1 and $1 \mid (-5)$,
$\therefore$ Given eq. has solution, it has 12 solution.

$$2x + 7y \equiv 5 \ (mod\ 12)$$

$$\begin{aligned}
\Rightarrow\ & 12 \mid 2x + 7y - 5 \\
\Rightarrow\ & 2x + 7y - 5 - 12z = 0 \\
\Rightarrow\ & 2(x - 3y - 2 - 6z) + y - 1 = 0 \\
\Rightarrow\ & 2u + y - 1 = 0, \text{ where } u = x + 3y - 2 - 6z \\
\Rightarrow\ & y = 1 - 2u
\end{aligned}$$

Now, from eq of u

$$\Rightarrow \ x = 7u + 6z - 1$$

Hence The Required Solutions are,
$x \equiv 7u + 6z - 1 \ (mod\ 12), \qquad y \equiv 1 - 2u \ (mod\ 12)$
where, z=0,1 and u= 0 to 5.

Solve the system of congruences.

(1) $x \equiv 2\ (mod\ 3)$; $x \equiv 3\ (mod\ 5)$; $x \equiv 2\ (mod\ 7)$
Sol.

$$\begin{gathered} x \equiv 2\ (mod\ 3) \\ x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \end{gathered}$$

By Sun-Tsu Theorem ,

$$\begin{gathered} a_1 = 2, \quad a_2 = 3, \quad a_3 = 2 \\ m_1 = 3, \quad m_2 = 5, \quad m_3 = 7 \\ m = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105 \\ \frac{m}{m_i} x_i \equiv 1\ (mod\ m_i); \quad i = 1, 2, 3 \end{gathered}$$

$$\begin{gathered} 35x_1 \equiv 1\ (mod\ 3) \\ 21x_2 \equiv 1\ (mod\ 5) \\ 15x_3 \equiv 1\ (mod\ 7) \end{gathered}$$

$$\begin{gathered} \therefore 3 \mid 35x_1 - 1; \quad 5 \mid 21x_1 - 1; \quad 7 \mid 15x_1 - 1 \\ \Rightarrow x_1 = 2; \quad x_2 = 1; \quad x_3 = 1 \end{gathered}$$

Now,

$$x \equiv \sum_{i=1}^{3} \frac{m}{mi} aix_i\ (mod\ m)$$

$$\begin{aligned} &x \equiv [35 \cdot 2 \cdot 2 + 21 \cdot 3 \cdot 1 + 15 \cdot 2 \cdot 1]\ (mod\ 105), \\ &x \equiv 233\ (mod\ 105), \\ &x \equiv 23\ (mod\ 105), \ \text{ which is req solution.} \end{aligned}$$

(2) $2x \equiv 1\ (mod\ 5)$; $3x \equiv 1\ (mod\ 7)$
Sol.
We can write,

$$2x \equiv 1\ (mod\ 5) \ \Rightarrow \ 5 \mid 2x - 1 \ \Rightarrow \ x \equiv 3\ (mod\ 5)$$

and also,

$$3x \equiv 1\ (mod\ 7) \ \Rightarrow \ 7 \mid 3x - 1 \ \Rightarrow \ x \equiv 5\ (mod\ 7)$$

Therefore, Given system is equivalent to,

$$\begin{gathered} x \equiv 3\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \end{gathered}$$

By Sun-Tsu Theorem ,

$$\begin{gathered} a_1 = 3, \quad a_2 = 5, \\ m_1 = 5, \quad m_2 = 7, \\ m = m_1 m_2 = 5 \cdot 7 = 35 \\ \frac{m}{m_i} x_i \equiv 1\ (mod\ m_i); \quad i = 1, 2 \end{gathered}$$

$$\begin{gathered} 7x_1 \equiv 1\ (mod\ 5) \\ 5x_2 \equiv 1\ (mod\ 7) \end{gathered}$$

$$\begin{gathered} \therefore 5 \mid 7x_1 - 1; \quad 7 \mid 5x_1 - 1 \\ \Rightarrow x_1 = 3; \quad x_2 = 3 \end{gathered}$$

Now,

$$x \equiv \sum_{i=1}^{2} \frac{m}{mi} a i x_i \ (mod\ m)$$

$$\begin{aligned} &x \equiv [7 \cdot 3 \cdot 3 + 5 \cdot 5 \cdot 3] \ (mod\ 35), \\ &x \equiv 138 \ (mod\ 35), \\ &x \equiv 33 \ (mod\ 35), \ \text{ which is req solution.} \end{aligned}$$

H.W:

(3) $x \equiv 1 \ (mod\ 4) \quad ; \quad x \equiv 3 \ (mod\ 5) \quad ; \quad x \equiv 2 \ (mod\ 7)$

Sol.

$$\begin{aligned} x &\equiv 1 \ (mod\ 4) \\ x &\equiv 3 \ (mod\ 5) \\ x &\equiv 2 \ (mod\ 7) \end{aligned}$$

By Sun-Tsu Theorem ,

$$a_1 = 1, \quad a_2 = 3, \quad a_3 = 2$$
$$m_1 = 4, \quad m_2 = 5, \quad m_3 = 7$$
$$m = m_1 m_2 m_3 = 4 \cdot 5 \cdot 7 = 140$$
$$\frac{m}{m_i} x_i \equiv 1 \ (mod\ m_i); \quad i = 1, 2, 3$$
$$35x_1 \equiv 1 \ (mod\ 4)$$
$$28x_2 \equiv 1 \ (mod\ 5)$$
$$20x_3 \equiv 1 \ (mod\ 7)$$
$$\therefore 4 \mid 35x_1 - 1; \quad 5 \mid 28x_1 - 1; \quad 7 \mid 20x_1 - 1$$
$$\Rightarrow x_1 = 3; \quad x_2 = 2; \quad x_3 = 6$$

Now,

$$x \equiv \sum_{i=1}^{3} \frac{m}{mi} a i x_i \ (mod\ m)$$

$$\begin{aligned} &x \equiv [35 \cdot 1 \cdot 3 + 28 \cdot 3 \cdot 2 + 20 \cdot 2 \cdot 6] \ (mod\ 140), \\ &x \equiv 513 \ (mod\ 140), \\ &x \equiv 93 \ (mod\ 140), \ \text{ which is req solution.} \end{aligned}$$

(4) $x \equiv -2 \ (mod\ 12) \ ; \quad x \equiv 6 \ (mod\ 10) \ ; \quad x \equiv 1 \ (mod\ 15)$

Sol.

$$\text{Here, } (m_i, m_j) \neq 1, \quad \forall\ i\ , j$$

$\therefore$ we can not apply Sun Tsu theorem directly.

Here, $x \equiv -2 \ (mod\ 12) \Rightarrow \ 12 \mid x + 2$

$$\Rightarrow 4 \mid x + 2\ , \ \ 3 \mid x + 2$$

$\Rightarrow \; x \equiv -2 (mod\ 4) \quad \& \quad x \equiv -2\ (mod\ 3)$

Now,

$x \equiv 6\ (mod\ 10)$ is equivalent to $x \equiv 6\ (mod\ 2)$ and $x \equiv 6\ (mod\ 5)$

& $x \equiv 1\ (mod\ 15)$ is equivalent to $x \equiv 1\ (mod\ 3)$ and $x \equiv 1\ (mod\ 5)$

Thus, given system is equivalent to

$x \equiv -2\ (mod\ 4)$ i.e. $x \equiv 2\ (mod\ 4)$
$x \equiv -2\ (mod\ 3)$ i.e. $x \equiv 1\ (mod\ 3)$
$x \equiv 6\ (mod\ 2)$ i.e. $x \equiv 0\ (mod\ 2)$
$x \equiv 6\ (mod\ 5)$ i.e. $x \equiv 1\ (mod\ 5)$

Since, $x \equiv 2\ (mod\ 4)$ & $x \equiv 0\ (mod\ 2)$ are satisfied by $x = 2$
$\therefore x \equiv 2\ (mod\ [\ 2, 4\ ]\ )$
$\therefore x \equiv 2\ (mod\ 4)$

Hence, the Given system is equivalent to,

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

Now, by Sun-Tsu Theorem ,

$$a_1 = 2, \quad a_2 = 1, \quad a_3 = 1$$
$$m_1 = 4, \quad m_2 = 3, \quad m_3 = 5$$
$$m = m_1 m_2 m_3 = 4 \cdot 5 \cdot 7 = 60$$
$$\frac{m}{m_i} x_i \equiv 1\ (mod\ m_i); \quad i = 1, 2, 3$$
$$15x_1 \equiv 1\ (mod\ 4)$$
$$20x_2 \equiv 1\ (mod\ 3)$$
$$12x_3 \equiv 1\ (mod\ 5)$$
$$\therefore 4 \mid 15x_1 - 1; \quad 3 \mid 20x_1 - 1; \quad 5 \mid 12x_1 - 1$$
$$\Rightarrow x_1 = 3; \quad x_2 = 2; \quad x_3 = 3$$

Now,

$$x \equiv \sum_{i=1}^{3} \frac{m}{mi} aix_i\ (mod\ m)$$

$$x \equiv [15 \cdot 2 \cdot 3 + 20 \cdot 1 \cdot 2 + 12 \cdot 1 \cdot 3]\ (mod\ 60),$$
$$x \equiv 166\ (mod\ 60),$$
$$x \equiv 46\ (mod\ 60), \text{ which is req solution.}$$

Que: Find The order of 5 modulo 13.

Sol.
Let x be order of 5 modulo 13
Then we can write $5^x \equiv 1 \ (mod \ 13)$
Here, $\phi(13) = 12$ so $1, 2, 3, 4, 6 \ or \ 12$ (divisors of 12) can be order of 5 modulo 13
we check them one by one,
clearly, $5^1 = 5$, $5 \not\equiv 1 \ (mod \ 13)$
$5^2 = 25$, $25 \not\equiv 1 \ (mod \ 13)$
$5^3 = 125$, $125 \not\equiv 1 \ (mod \ 13)$
$5^4 = 625$, $625 \equiv 1 \ (mod \ 13)$
$\therefore$ 4 is order of 5 modulo 13.

H.W: Find The order of 2 modulo 7.
(Ans= 3)

Sol.
Let x be order of 2 modulo 7
Then we can write $2^x \equiv 1 \ (mod \ 7)$
Here, $\phi(7) = 6$ so $1, 2, 3 \ or \ 6$ (divisors of 6) can be order of 2 modulo 7
we check them one by one,
clearly, $2^1 = 2$, $2 \not\equiv 1 \ (mod \ 7)$
$2^2 = 4$, $4 \not\equiv 1 \ (mod \ 7)$
$2^3 = 8$, $8 \equiv 1 \ (mod \ 7)$
$\therefore$ 3 is order of 2 modulo 7.

.

- Dipali M. Mistry