MA212 TUTORIAL 5 (NUMBER THEORY) [BHAGVA RANA]

LINEAR CONGRUENCES AND CHINESE REMAINDER THEORAM

U19CS012

1) Solve the following linear congruences

(a) $25x \equiv 15 \pmod{29}$

$\gcd(25, 29) = 1$ ∵ 29 is prime

∴ Solution Exist

① Adding -29 $\quad -4x \equiv -14 \pmod{29}$

② Dividing by -2 ($\gcd(2,29)=1$) $\quad 2x \equiv 7 \pmod{29}$

③ Multiplying by 15 $\quad 30x \equiv 105 \pmod{29}$

④ Adding -29 $\quad x \equiv 76 \pmod{29}$

⑤ Adding -58 on right $\quad \therefore x \equiv 18 \pmod{29}$

ANS : $x \equiv 18 \pmod{29}$

(b) $5x \equiv 2 \pmod{26}$

$\gcd(5, 26) = 1$ ∴ Solution Exist (5 is prime)

① Multiplying 5 on both sides

$$5 \times 5x \equiv 5 \times 2 \pmod{26}$$

$$25x \equiv 10 \pmod{26}$$

$$-1x \equiv 10 \pmod{26}$$

multipy both sides by (-1),

$$1x \equiv -10 \pmod{26}$$

$$1x \equiv 16 \pmod{26}$$

So, $\boxed{x \equiv 16 \pmod{26}}$

Therefore, the solution of linear congruence $5x \equiv 2 \pmod{26}$ is

$x = 16 + 26t$ for integer $t = 0$

Hence, the Unique solution is $\boxed{x = 16 \pmod{26}}$.

U19CS012

(c) $34x \equiv 60 \pmod{98}$

Here $a = 34$, $b = 60$, $n = 98$

$d = \gcd(a, n) = \gcd(34, 98) = 2$

$d \mid b$ [since $2 \mid 60$]

So, there will be 2 incongruent solutions modulo 98.

Reduce the congruence to form $\frac{ax}{d} = \frac{b}{d} \bmod \frac{n}{d}$

That is $17x \equiv 30 \bmod 49$ —— ①

① multiply both sides by 3

$3 \times 17x \equiv 3 \times 30 \bmod 49$

$51x \equiv 90 \bmod 49$

$2x \equiv 41 \bmod 49$

$2x \equiv (-8) \bmod 49$

② multiply both sides by 24,

$24 \times 2x \equiv 24(-8) \bmod 49$

$48x \equiv (-192) \bmod 49$

$(-1)x \equiv 4 \bmod 49$

③ multiply both sides by (−1)

$1x \equiv (-4) \bmod 49$

$1x \equiv 45 \bmod 49$

$x \equiv 45 \bmod 49$

The solution for congruence ①,

$x = 45 + 49t$

Therefore, the two incongruent solⁿ can be obtained by adding 49 to the constant & replacing $49t \to 98t$

ie. $x = 98t + 45$, $x = 98t + 94$ } are solution of $34x = 60 \pmod{98}$

Ans: $\boxed{x \equiv 45 \pmod{98}, \quad x \equiv 94 \pmod{98}}$ are solutions to given congruence.

U19CS012

(d) $140x \equiv 133 \pmod{301}$

$140 = 2^2.5.7$, $301 = 7 \times 43$, $\therefore \gcd(140, 301) = 7$
and $7 \mid 133$ $\therefore$ 7 congruent solution exist

$20x \equiv 19 \pmod{43}$ [divide by 7]
$40x \equiv 38 \pmod{43}$ [multiply by 2]
$43x - 40x = 43 - 38 \pmod{43}$
$3x \equiv 5 \pmod{43}$
$42x \equiv 70 \pmod{43}$ [multiply by 14]
$43x - 42x \equiv 86 - 70 \pmod{43}$
$x \equiv 16 \pmod{43}$

$\therefore$ $x = 16 + 43t$, $\therefore$ such that $t = 0, 1, 2, 3, 4, 5, 6$

ANS:
$\boxed{\therefore \; x \equiv 16, 59, 102, 145, 188, 231, 274 \pmod{301}}$

2.) Using congruences, solve the Diophantine equations:

(a) $4x + 51y = 9$

$4x \equiv 9 \pmod{51}$
$52x \equiv 117 \pmod{51}$ (multiplied by 13)
$x \equiv 15$ [subtract $51x$, 102] (51×2)
$\therefore \boxed{x = 15 + 51t}$

$51y \equiv 9 \pmod{4}$
$17y \equiv 3 \pmod{4}$ ($\gcd(51, 4) = 1$, divide by 3)
$17y - 16y \equiv 3 \pmod{4}$
$y \equiv 3 \pmod{4}$
$\boxed{\therefore \; y = 3 + 4s}$

U19CS012

$\therefore\ 4x + 51y = 4(15+51t) + 51(3+4s) = 9$

$= 60 + 204t + 153 + 204s$

$(-204) = 204t + 204s$

$t + s = -1$

$[s = -1 - t]$

ANS: $\therefore$ $\boxed{\begin{aligned} x &= 15 + 51t \\ y &= 3 + 4(-1-t) = -1 - 4t \end{aligned}}$

(b) $5x - 53y = 17$

$5x \equiv 17 \pmod{53}$

$55x \equiv 187$ (mult. by 11)

$55x - 53x \equiv (187 - 3.53) \pmod{53}$

$2x \equiv 28 \pmod{53}$

$x \equiv 14 \pmod{53}$ $\quad$ (gcd (2, 53) = 1 , divide by 2)

$\therefore \boxed{x = 14 + 53t}$

$-53y \equiv 17 \pmod 5$

$-53y + 50y \equiv 17 \pmod 5$

$-3y \equiv 17 \pmod 5$

$-9y \equiv 51 \pmod 5$ $\quad$ (multiply by 3)

$y = 51 \pmod 5$ $\quad$ (add by 10y)

$\therefore \boxed{y = 51 + 5s}$

$\therefore\ 5x - 53y = 5(14+53t) - 53(51+5s)$

$17 = 70 + 265t - 2703 - 265s$

$2650 = 265t - 265s$

$10 = t - s$, $\quad$ $[s = t - 10]$

$\therefore\ y = 51 + 5(t-10) = 5t + 1$

ANS: $\therefore$ $\boxed{\begin{aligned} x &= 14 + 53t \\ y &= 1 + 5t \end{aligned}}$

U19CS012

3.) Solve the following sets of simultaneous congruences :

(a) $x \equiv 5 \pmod{11}$

$x \equiv 14 \pmod{29}$

$x \equiv 15 \pmod{31}$

$N = 11 \cdot 29 \cdot 31 = 9889$

$N_1 = 29 \cdot 31 = 899$, $N_2 = 11 \cdot 31 = 341$, $N_3 = 11 \cdot 29 = 319$

$899\,x \equiv 1 \pmod{11}$	$341x \equiv 1 \pmod{29}$	$319\,x \equiv 1 \pmod{31}$
$899x - 81 \cdot 11\,x \equiv 1$	$341x - 62 \cdot 29x \equiv 1$	$319x - 310x \equiv 1$
$899x - 891\,x \equiv 1$	$341x - 348\,x \equiv 1$	$9x \equiv 1$
$8x \equiv 1$	$-7x \equiv 1$	$63\,x \equiv 7$
$32x \equiv 4$	$-28\,x \equiv 4$	$x \equiv 7$
$32x - 33x \equiv 4$	$x \equiv 4$	
$x \equiv -4 \pmod{11}$		

$\therefore\ x_1 = -4, \quad x_2 = 4, \quad x_3 = 7$

$\therefore\ a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$

$5 \cdot 899\,(-4) + 14 \cdot 341 \cdot (4) + 15 \cdot 319\,(7) = 34{,}611$

ANS

$\therefore\ x \equiv 34{,}611 = 34{,}611 - 3 \cdot 9889 = \boxed{4944 \pmod{9889}}$

(b) $2x \equiv 1 \pmod 5$; $4x \equiv 2$, $4x - 5x = -x$,	$x \equiv -2 \pmod 5$
$3x \equiv 9 \pmod 6$:	$x \equiv 3 \pmod 2$
$4x \equiv 1 \pmod 7$; $8x \equiv 2$, $8x - 7x = x$	$x \equiv 2 \pmod 7$
$5x \equiv 9 \pmod{11}$: $10x \equiv 18$, $10x - 11x = -x$	$x \equiv -18 \pmod{11}$

$N = 5 \cdot 2 \cdot 7 \cdot 11 = 770$ $\quad N_1 = 2 \cdot 7 \cdot 11 = 154$ $\quad N_3 = 5 \cdot 2 \cdot 11 = 110$

$N_2 = 5 \cdot 7 \cdot 11 = 385$ $\quad N_4 = 5 \cdot 2 \cdot 7 = 70$

U19CS012

$154\, x_1 \equiv 1 \pmod 5$ $\qquad$ $385\, x_2 \equiv 1 \pmod 2$

$x_1 = -1$ $\qquad$ $x_2 \equiv 1$

$110\, x_3 \equiv 1 \pmod 7$ $\qquad$ $70\, x_4 \equiv 1 \pmod{11}$

$110\, x_3 - 7.15\, x_3 = 5x_3 \equiv 1$ $\qquad$ $70\, x_4 - 66\, x_4 \equiv 1$

$15\, x_3 \equiv 3$ $\qquad$ $12\, x_4 \equiv 3$

$x_3 \equiv 3$ $\qquad$ $x_4 \equiv 3$

$\therefore\ a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + a_4 N_4 x_4 =$
$(-2)(154)(-1) + (3)(385)(1) + 2.(110)(3) + (-18)(70)(3)$
$= -1657$

$\therefore\ X = -1657 + \cancel{3.770}\ 3.770$
$= \boxed{653 \pmod{770}}$

4) Find the smallest integer $a > 2$, such that

$2 | a, \quad 3 | a+1, \quad 4 | a+2, \quad 5 | a+3, \quad 6 | a+4$

This is equivalent to:

$a \equiv 0 \pmod 2$	or	$a \equiv 0 \pmod 2$	[1]
$a+1 \equiv 0 \pmod 3$		$a \equiv -1 \pmod 3$	[2]
$a+2 \equiv 0 \pmod 4$		$a \equiv -2 \pmod 4$	[3]
$a+3 \equiv 0 \pmod 5$		$a \equiv -3 \pmod 5$	[4]
$a+4 \equiv 0 \pmod 6$		$a \equiv -4 \pmod 6$	[5]

Note that $\gcd(2,4) = 2$, so eliminate [1]

$\because$ [3] is true, [1] is automatically true

Also, $\gcd(3,6) \neq 1$, Multiply [2] by 2 and get

$(a+1).2 = 0.2 \pmod{3.2}$ or

$2a+2 = 0 \pmod 6$

Combine this with [5] and get

$2a+2 \equiv 0 \equiv a+4 \pmod 6$

$\therefore\ a \equiv 2 \pmod 6$

If this is true, then [2] & [5] will be true

U19CS012

$\therefore$ So, for we have $a \equiv -2 \pmod 4$ [1]'

$a \equiv -3 \pmod 5$ [2]'

$a \equiv -2 \pmod 6$ [3]'

Note that $\gcd(4,6) \neq 1 \therefore$ combine ~~[1]'~~

[1]' becomes $3a \equiv -6 \pmod{12}$

[3]' becomes $2a \equiv 4 \pmod{12}$

$\therefore 3a + 12 \equiv -6 + 12 \equiv 6 \pmod{12}$

$2a + 2 \equiv 4 + 2 \equiv 6 \pmod{12}$

$\therefore 3a + 12 \equiv 2a + 2 \pmod{12}$

$a \equiv -10 \pmod{12}$

$\therefore$ The system reduce to:

$a \equiv -3 \pmod 5$

$a \equiv -10 \pmod{12}$

$\therefore N = 5 \cdot 12 = 60$, $N_1 = 12$, $N_2 = 5$

$\therefore 12x_1 \equiv 1 \pmod 5$

$24x_1 \equiv 2$

$24x_1 - 25x_1 \equiv -x_1 \equiv 2$

$\therefore x_1 \equiv -2$

$5x_2 \equiv 1 \pmod{12}$

$25x_2 \equiv 5$

$25x_2 - 24x_2 \equiv x_2 \equiv 5$

$\therefore a_1 N_1 x_1 + a_2 N_2 x_2 =$

$(-3)(12)(-2) + (-10)(5)(5) = 72 - 250 = -178$

$\therefore a \equiv -178 \pmod{60}$ or $a \equiv 2 \pmod{60}$

ANS: $\therefore a \equiv 62 \pmod{60}$ $\boxed{\therefore a = 62}$

U19CS012

5.) A band of 17 pirates stole a stack of gold coins. When they try to divide the fortune, into equal portions, 3 coins remained. In the ensuing brawl, over who should get the extra coins, One pirate was killed. The wealth was redistributed, but this an equal division left 10 coins. Again an Argument developed in which another pirate was killed. But now the total fortune was evenly distributed, among the survivors. What was the least number of coins that could have been stolen.

$$\left.\begin{aligned} x &\equiv 3 \pmod{17} \\ x &\equiv 10 \pmod{16} \\ x &\equiv 0 \pmod{15} \end{aligned}\right\} \quad 17, 16, 15 \text{ are relatively prime}$$

$N = 17.16.15 = 4080$

$N_1 = 16.15 = 240$

$N_2 = 17.15 = 255$

$N_3 = 17.16 = 272$

$240 x_1 \equiv 1 \pmod{17}$

$240 x_1 - 14.17 x_1 = 2x_1$

$2x_1 = 1 ; \quad 18 x_1 = 9 9$

$\therefore x_1 = 9 \pmod{17}$

$255 x_2 \equiv 1 \pmod{16}$

$255 x_2 - 16.16\, x_2 = -x_2$

$\therefore x_2 = -1 \pmod{16}$

$N_3 x_3 \equiv 1 \pmod{15}$

{ irrelevant since $a_3 = 0$ }

$\therefore \; a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 3.240.9 + 10.255.(-1) + 0$

$= 3930$

Ans: $\boxed{\therefore \quad 3930 \text{ coins}}$ { Least number of coins stolen }

U19CS012

6.) A certain integer between 1 and 1200 leaves the remainder 1, 2, 6 when divided by 9, 11, 13 respectively. What is the integer?

6.) $x \equiv 1 \pmod 9$

$x \equiv 2 \pmod{11}$ and $1 < x < 1200$

$x \equiv 6 \pmod{13}$

9, 11, 13 are relatively prime, so can use Chinese remainder theorem

$N = 9.11.13$

$N_1 = 11.13 = 143$ $N_2 = 9.13 = 117$ $N_3 = 9.11 = 99$

$143 x_1 \equiv 1 \pmod 9$

$143 x_1 - 9.15 x_1 = 8x_1$

$8x_1 - 9x_1 = -x_1 \equiv 1$

$[x_1 \equiv -1]$

$117 x_2 \equiv 1 \pmod{11}$

$117 x_2 - 121 x_2 \equiv -4x_2$

$-12 x_2 \equiv 3$

$-x_2 \equiv 3$

$[x_2 \equiv -3]$

$99 x_3 \equiv 1 \pmod{13}$

$99x_3 - 8.13 x_3 \equiv -5x_3$

$-15x_3 \equiv 3$

$-2x_3 \equiv 3$

$-12x_3 \equiv 18$

$\boxed{x_3 \equiv 18}$

$\therefore$ $a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 =$

$1.143.(-1) + 2.(117).(-3) + 6.99(18)$

$= 9847$

$9847 - 7.1287 = 838$

ANS: $\therefore$ $\boxed{\text{838 is required integer}}$

U19CS012

7.> Find an integer having remainder 1, 2, 5, 5 when divided by 2, 3, 6, 12 respectively.

7.> $x \equiv 1 \pmod 2$ [2] { divisors not relatively prime, so simplify }

$x \equiv 2 \pmod 3$ [3]

$x \equiv 5 \pmod 6$ [6]

$x \equiv 5 \pmod{12}$ [12]

$\gcd(3,6) \neq 1$, so multiply [3] by 2

$\therefore 2x \equiv 4 \pmod 6$

$x \equiv 5 \pmod 6$

$\therefore 2x - 4 \equiv x - 5 \pmod 6$, or

$x \equiv -1 \pmod 6$ [6']

$\therefore$ if [6'] is true, then so is [6] and [3]

But [6'] is same as $x \equiv -1 + 6 = 5 \pmod 6$, which is [6]

$\therefore$ can drop [3] ✓

$\gcd(6, 12) \neq 1$, so multiply [6] by 2

$\therefore 2x \equiv 10 \pmod{12}$

$x \equiv 5 \pmod{12}$

$\therefore x \equiv 5 \pmod{12}$, which is [12]

$\therefore$ if [12] is true, so if [6], so is [3]

$\therefore$ can drop [3] ✓ and [6] ✓

$\Rightarrow \therefore x \equiv 1 \pmod 2$ [2]

$x \equiv 5 \pmod{12}$ [12]

But $\gcd(2, 12) \neq 1$ $\therefore$ multiply [2] by 6

$\therefore 6x \equiv 6 \pmod{12}$

$x \equiv 5 \pmod{12}$

$\therefore 5x \equiv 1 \pmod{12}$

$7 \cdot 5x \equiv 7 \rightarrow 35x \equiv 7$

$35x - 36x \equiv -x \equiv 7$

$x \equiv -7 + 12 = 5$

$\therefore x \equiv 5 \pmod{12}$

$\therefore x = 5 + 12k$

since we want $x > 12$

we choose $x = 5 + 12(1)$

ANS: $\boxed{x = 17}$

U19CS012

Q 8.) Let t_n denote the n^{th} triangular number. For which values of n, does t_n divide $t_1^2 + t_2^2 + t_3^2 + \dots + t_n^2$

We will use the identity

$$t_1^2 + t_2^2 + t_3^2 + \dots t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30 \quad \text{—} (1)$$

$$\therefore t_n \mid t_1^2 + t_2^2 + \dots + t_n^2$$

[Can be proved using Mathematical Induction]

$$\iff \frac{(3n^3 + 12n^2 + 13n + 2)}{30} \text{ is an integer}$$

i.e. $(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{30}$ or

$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod{2.3.5}$ or

$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod 2$ [2]

$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod 3$ [3]

$(3n^3 + 12n^2 + 13n + 2) \equiv 0 \pmod 5$ [5]

Since unique solutions are $\equiv \pmod{30}$ by "Chinese Remainder Theorem"

For [2], $3n^3 - 2n^3 + 12n^2 - 6.2n^2 + 13n - 2.6n + 2.2 =$

$n^3 + n = n(n^2+1) \equiv 0 \pmod 2$

If $n \to$ even $n(n^2+1) \to$ even & $n(n^2+1) \equiv 0 \pmod 2$

$n \to$ odd $n^2 \to$ odd $n^2+1 \to$ even $\therefore n(n^2+1) \equiv 0 \pmod 2$

So, [2] put restriction on n.

For [3], $3n^3 - 3n^3 + 12n^2 - 3.4n^2 + 13n - 3.4n + 2 =$

$n + 2 \equiv 0 \pmod 3$

$\therefore \boxed{n \equiv 1 \pmod 3}$

P.T.O →

U19CS012

For [5], $3n^3 + 12n^2 - 5.2n^2 + 13n - 5.2n + 2 =$

$3n^3 + 2n^2 + 3n + 2 =$

$n^2(3n+2) + (3n+2) = (n^2+1)(3n+2) \equiv 0 \pmod 5$

$\therefore (n^2+1) \equiv 0 \pmod 5$

or $(3n+2) \equiv 0 \pmod 5$

Problem reduces to

$n \equiv 1 \pmod 3$
$(n^2+1) \equiv 0 \pmod 5$
$(3n+2) \equiv 0 \pmod 5$

$3n+2 \equiv 0 \pmod 5$

$3n \equiv -2 \quad 6n \equiv -4$

$n \equiv -4, \quad n \equiv 1$

$\therefore n \equiv 1 \pmod 5$

$n \equiv 1 \pmod 5 \Rightarrow 3n \equiv 3 \pmod{15}$

$n \equiv 1 \pmod 3 \Rightarrow 5n \equiv 5 \pmod{15}$

$\therefore 5n - 3n = (5-3) \pmod{15}$

$2n = 2 \pmod{15}$

$\boxed{n \equiv 1 \pmod{15}}$

$n^2+1 \equiv 0 \pmod 5$

$n^2 = -1, \quad n^2 \equiv 4$

$n \equiv 2$ or $n \equiv -2$

$\therefore n \equiv 2 \pmod 5$

or $n \equiv 3 \pmod 5$

$n \equiv 2 \pmod 5 \Rightarrow 3n = 6 \pmod{15}$

$n \equiv 1 \pmod 3 \Rightarrow 5n = 5 \pmod{15}$

$\therefore 5n - 3n \equiv 5 - 6, \quad 2n \equiv -1$

$2n = -1 + 15$

$2n \equiv 14$

$\boxed{\therefore n \equiv 7 \pmod{15}}$

ANS:
$\therefore n \equiv 1$ or 7 or $13 \pmod{15}$

$n \equiv 3 \pmod 5 \Rightarrow 3n \equiv 9 \pmod{15}$

$n \equiv 1 \pmod 5 \Rightarrow 5n \equiv 5 \pmod{15}$

$5n - 3n \equiv 5 - 9 = -4, \quad 2n \equiv -4$

$n \equiv -2, \quad n \equiv -2 + 15$

$\boxed{n \equiv 13 \pmod{15}}$

VISION

U19CS012

9.) Find the solutions of the system of congruences

$$3x + 4y \equiv 5 \pmod{13} \quad -[1]$$
$$2x + 5y \equiv 7 \pmod{13} \quad -[2]$$

multiply [1] by 5: $15x + 20y \equiv 25 \pmod{13}$ — [1']

multiply [2] by 4: $8x + 20y \equiv 28 \pmod{13}$ — [2']

[1'] - [2'] $\Rightarrow$

$$7x \equiv -3 \pmod{13}$$
$$\therefore 14x \equiv -6$$
$$14x - 13x \equiv -6 + 13$$
$$\boxed{x \equiv 7 \pmod{13}} \quad -[3']$$

Substitute [3'] into [1] :

$$3x \equiv 21 \pmod{13} \quad [3']$$
$$3x \equiv 5 - 4y \pmod{13} \quad [1]$$
$$\therefore 21 \equiv 5 - 4y \pmod{13}$$
$$16 \equiv -4y$$
$$48 \equiv -12y$$
$$48 - 3.13 \equiv -12y + 13y$$
$$9 \equiv y \pmod{13}$$

ANS :

$$\boxed{\begin{array}{l} \therefore x \equiv 7 \pmod{13} \\ y \equiv 9 \pmod{13} \end{array}}$$

—x—

SUBMITTED BY :

BHAGYA VINOD RANA

U19CS012

II nd yr - (CSE)