Assignment -

Name - Keerthi P. Charanthimath
Roll No - 19MA20059

Q.1 (a) 98

$U = [2555 \quad 1 \quad 0] \qquad V = [98 \quad 0 \quad 1]$

W	U			V		
	2555	1	0	98	0	1
26	98	0	1	7	1	-26
14	7	1	-26	0	-14	0

$7 = 2555.1 + 98.(-26)$

Inverse of 98 in Z_{2555} does not exist as $\gcd(2555, 98) = 7 \neq 1$

b) 1972

$U = [2555 \quad 1 \quad 0] \qquad V = [1972 \quad 0 \quad 1]$

W	U			V		
	2555	1	0	1972	0	1
1	1972	0	1	583	1	-1
3	583	1	-1	223	-3	4
2	223	-3	4	137	7	-9
1	137	7	-9	86	-10	13
1	86	-10	13	51	17	-22
1	51	17	-22	35	-27	35
1	35	-27	35	16	44	-57
2	16	44	-57	3	-115	149
5	3	-115	149	1	619	-802
3	1	619	-802	0		

P.T.O

$1 = 2555.619 + 1972 \cdot (-802)$

$1972^{-1} \pmod{2555} = -802$

Q2:- $n \geq ab - a - b + 1$

$ax + by = n$ has soln if $n \geq ab - a - b + 1$

Let x^*, y^* be a soln to the above eqn

$\therefore ax^* + by^* = n$

Let p be any integer

$\therefore p^n = p^{ax^* + by^*} = (p^{x^*})^a \cdot (p^{y^*})^b$

$\therefore$ Every n^{th} power of an integer can be written as the product of an a-th power and b-th power.

Q 3:- We have to find if soln of $13x + 7y = 71$ exists

$13 \cdot 7 - 13 - 7 + 1 = 72$

Linear diophantine eqn: $ax + by = n$

It has a soln if $n \geq ab - a - b + 1$

$ab - a - b + 1 = 13 \cdot 7 - 13 - 7 + 1 = 72$

$71 < 72$

$\therefore 13x + 7y = 71$ does not have a solution.

19MA20059

Q 4:- (a) $25x \equiv 55 \pmod{95}$

$\gcd(25, 95) = 5 \nmid 1$

$5/55$

$5x \equiv 11 \pmod{19}$

$\gcd(5, 19) = 1$

$1 = 19u + 5v$

~~$U = [19, 1,$~~

$U = [\ 19 \quad 1 \quad 0\ ] \qquad V = [\ 5 \quad 0 \quad 1\ ]$

W	U			V		
	19	1	0	5	0	1
3	5	0	1	4	1	-3
1	4	1	-3	1	-1	4
4	1	-1	4		0	

$1 = 19.(-1) + 5(4)$

$\therefore 5^{-1} \pmod{19} = 4$

$4.5x \equiv 4.11 \pmod{19}$

$20x \equiv 44 \pmod{19}$

$20x \equiv 6 \pmod{19}$

$-18x \equiv -13 \pmod{19}$

$\boxed{x \equiv 6 \pmod{19}}$ Soln

$5x \equiv 30 - 11 \pmod{19}$

(b) $1972x = 363 \pmod{2555}$

from ques 1,

$1972^{-1} \pmod{2555} = -802$

$-802.1972x = -802.363 \pmod{2555}$

P.T.O

19MA20059

$-158154.4x \equiv -291126 \pmod{2555}$

$2555(619)x - 158154.4x \equiv 2555(114) - 291126 \pmod{2555}$

$\boxed{x \equiv 144 \pmod{2555}}$ Ans

$1972x = 283968 \equiv 363 \pmod{2555}$

Q5:- $x \equiv 12 \pmod{25}$
$x \equiv 9 \pmod{26}$
$x \equiv 23 \pmod{27}$

$M = 17550$

$M_1 = 702 \quad M_2 = 675 \quad M_3 = 650$

$M_1 y_1 = 1 \pmod{25}$
$702u + 25v = 1$

$U = [702 \quad 1 \quad 0] \qquad V = [25 \quad 0 \quad 1]$

$1 = 702(-12) + 25(337)$
$702^{-1} \pmod{25} = -12 = y_1$

W	U			V		
	702	1	0	25	0	1
28	25	0	1	2	1	-28
12	2	1	-28	1	-12	337
2	1	-12	337	0		

$M_2 y_2 = 1 \pmod{26}$

$U = [675 \quad 1 \quad 0] \qquad V = [26 \quad 0 \quad 1]$

19MA20059

W	U			V		
	675	1	0	26	0	1
25	26	0	1	25	1	-25
1	25	1	-25	1	-1	26
25	1	-1	26		0	

$1 = 675(-1) + 26(26)$

$675^{-1} \pmod{26} = -1 = y_2$

$U \equiv [650 \quad 1 \quad 0] \qquad V = [23 \quad 0 \quad 1]$

$M_3 y_3 = 1 \pmod{27}$

$650u + 23v = 1$

$U = [650 \quad 1 \quad 0] \qquad V = [23 \quad 0 \quad 1]$

$1 = 650(-4) + 23(-113)$

$650^{-1} \pmod{27} = 4 = y_3$

W	U			V		
	650	1	0	23	0	1
28	23	0	1	6	1	-28
3	6	1	-28	5	-3	85
1	5	-3	85	1	4	-113
5	1	4	-113		0	

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{17550}$

$= 12 \cdot 702 \cdot (-12) + 9 \cdot 675(-1) + 23(650)4 \pmod{17550}$

$= -47363 \pmod{17550}$

$x \equiv 5287 \pmod{17550}$

p.T.O

Q 6 :- $22^{1437} \pmod{53}$

$22 \equiv 22 \pmod{53}$

$22^2 \equiv 484 \equiv 7 \pmod{53}$

$22^4 \equiv 49 \pmod{53}$

$22^8 \equiv 2401 \pmod{53} \equiv 16 \pmod{53}$

$22^{16} \equiv 256 \pmod{53} \equiv 44 \pmod{53}$

$22^{32} \equiv 1936 \pmod{53} \equiv 28 \pmod{53}$

$22^{64} \equiv 784 \pmod{53} \equiv 42 \pmod{53}$

$22^{128} \equiv 1764 \pmod{53} \equiv 15 \pmod{53}$

$22^{256} \equiv 225 \pmod{53} \equiv 13 \pmod{53}$

$22^{512} \equiv 169 \pmod{53} \equiv 10 \pmod{53}$

$22^{1024} \equiv 100 \pmod{53} \equiv 47 \pmod{53}$

$1437 \sim [1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1]$ base 2 (bit positions 10 9 8 7 6 5 4 3 2 1 0)

$1437 = 2^{10}.1 + 2^8.1 + 2^7 + 2^4 + 2^3 + 2^2 + 1$

$1437 = 1024 + 256 + 128 + 16 + 8 + 4 + 1$

$22^{1437} = 22^{1024} \cdot 22^{256} \cdot 22^{128} \cdot 22^{16} \cdot 22^{8} \cdot 22^{4} \cdot 22^{1}$

$= 47 \cdot 13 \cdot 15 \cdot 44 \cdot 16 \cdot 49 \cdot 22$

$\equiv 33 \pmod{53}$

$\gcd(22, 53) = 1$

$22^{52} \equiv 1 \pmod{53}$

$1437 = 52 \cdot 27 + 33$

$22^{1437} = 22^{52 \cdot 27} \cdot 22^{33} \equiv 1^{27} \cdot 22^{33}$

$\therefore 22^{1437} \equiv 22^{33} \pmod{53}$

$22^{33} \pmod{53}$

$33 = 32 + 1$

$22^{33} = 22^{32} \cdot 22$

$\equiv 28 \cdot 22 \pmod{53}$
$\equiv 33 \pmod{53}$

$\therefore 22^{1437} \equiv 33 \pmod{53}$

Q 7:- $n = 81$

$n = 3^4$

$Z_3^* = \{1, 2\} \Rightarrow \phi(3) = 2$

$2^2 \equiv 1 \pmod{3}$

$\therefore$ 2 → primitive root (mod 3)
5 → primitive root (mod 9)
5 → primitive root (mod 81)

No. of primitive roots $= \phi(\phi(81))$

$\phi(81) = \phi(3^4) = 81\left(1-\frac{1}{3}\right) = 54$

$\phi(54) = \phi(2 \cdot 3^3) = 54\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 18$

18 primitive roots
order of 5 → 54

$Z_{54}^* = \{1, 5, 7, 11, 13, 17 \ldots\}$
primitive roots: $\{5^1, 5^5, 5^7 \ldots\}$

Q 8:- (a) $\text{ord}_{11}(5)$

$\phi(11) = 10 = 2 \times 5$

$\therefore \text{ord}_{11}(5) = 2$ or 5 or 10

P.T.O

$5^2 \equiv 3 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$5^{10} \equiv 1 \pmod{11}$
$\therefore \text{ord}_{11}(5) = 5$

(b) $\text{ord}_{17}(2)$
$\phi(17) = 16 = 2^4$
$\therefore \text{ord}_{17}(2) = 2 \text{ or } 2^2 \text{ or } 2^3 \text{ or } 2^4$

$2^2 \equiv 4 \pmod{17}$
$2^4 \equiv 16 \pmod{17}$
$2^8 \equiv 1 \pmod{17}$

$\therefore \text{ord}_{17}(2) = 8$

(c) $\text{ord}_{427}(21)$
$\gcd(21, 427) = 7$
$\therefore$ 21 & 427 are not relatively prime.
$\text{ord}_{427}(21$ does not exist.

Q 10 :- (a) $g = 3$, $n = 566 = 2 \cdot 283 = 2p$

$$\phi(566) = \phi(2 \cdot 283) = 566\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{283}\right)$$

$\phi(566) = 282 = 2 \cdot 141 = 2 \cdot 3 \cdot 47$
$\text{ord}_{566}(3)$ is 2 or 3 or 47 or 141 or 282

$3^2 \equiv 9 \pmod{566}$
$3^4 \equiv 81 \pmod{566}$
$3^8 \equiv 335 \pmod{566}$
$3^{16} \equiv 157 \pmod{566}$

$3^{32} \equiv 311 \pmod{566}$
$3^{64} \equiv 501 \pmod{566}$
$3^{128} \equiv 263 \pmod{566}$
$3^{256} \equiv 117 \pmod{566}$

$47 = 32 + 8 + 4 + 2 + 1$
$3^{47} \equiv 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^2 \cdot 3^1 \pmod{566}$
$\equiv 311 \cdot 81 \cdot 9 \cdot 335 \cdot 3 \pmod{566}$
$\equiv 239 \pmod{566}$

$141 = 128 + 8 + 4 + 1$
$3^{141} \equiv 3^{128} \cdot 3^8 \cdot 3^4 \cdot 3^1 \pmod{566}$
$\equiv 263 \cdot 335 \cdot 81 \cdot 3 \pmod{566}$
$\equiv 565 \pmod{566}$

$282 = 256 + 16 + 8 + 2$
$3^{282} \equiv 3^{256} \cdot 3^{16} \cdot 3^8 \cdot 3^2 \pmod{566}$
$\equiv 117 \cdot 157 \cdot 335 \cdot 9 \pmod{566}$
$\equiv 1 \pmod{566}$

$\therefore \text{ord}_{566}(3) = 282 = \phi(566)$
$\therefore$ 3 → primitive root $\pmod{566}$

(b) $\text{ord}_{566}(a) = 12$
$12 \nmid 282$ ∴ There does not exist any integer a, such that $\phi_{566}(a) = 12$

(c) $n = 283$
$\phi n = 282$.
$\text{ord}_{283}(a) = 94$

$3^2 \equiv 9 \pmod{283}$
$3^4 \equiv 81 \pmod{283}$
$3^8 \equiv 52 \pmod{283}$
$3^{16} \equiv 157 \pmod{283}$
$3^{32} \equiv 28 \pmod{283}$
$3^{64} \equiv 218 \pmod{283}$

P. T. O.

ord 283 (3)

$282 = 256 + 16 + 8 + 2$

$3^{282} = 3^{256} \cdot 3^{16} \cdot 3^{8} \cdot 3^{2} \pmod{283}$

$3^{128} \equiv 263 \pmod{283}$

$3^{256} \equiv 117 \pmod{283}$

$3^{282} \equiv 117 \cdot 157 \cdot 52 \cdot 9 \pmod{283}$

$\equiv 141 \cdot 281 \pmod{283}$

$\equiv 1 \pmod{283}$

$\therefore$ 3 → primitive root of 283

$$\text{ord}_{283}(3^j) = \frac{\text{ord}_{283}(3)}{\gcd(j, 282)} = 94$$

$$\frac{282}{\gcd(j, 282)} = 94 \qquad \text{ord}_{283}(27) = 94$$

$\gcd(j, 282) = 3$

$282 = 2 \times 3 \times 47 \quad 1 \leq j \leq 282$

$j = 3, 3\times3, 5\times3, 7\times3, 9\times3$

138 integers

Q 9:- $n = 81$

$n = 81 = (3)^4$ which is of the form p^k where p is odd prime and $k \in \mathbb{Z}^+$

$\therefore$ primitive roots module $n = 81$ will exists

19MA20059

# of primitive roots $= \phi(\phi(81))$

$= \phi\left[81 \times \left(1-\frac{1}{3}\right)\right]$

$= \phi(54)$

$= 54 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$

# of primitive roots = 18

(b) First finding primitive root for $p = 3$

$\phi(p) = \phi(3) = 2$

Now $a^k \equiv 1 \bmod (p)$

for a to be primitive root modulo p least value of k should be $\phi(p) = 2$

for $a = 2$ $\quad 2 \pmod 3 = 2$

$2^2 \pmod 3 = 1$

$\therefore$ 2 is a primitive root for $p = 3$

Now by rules of primitive root we can say that $2+3$ will be primitive root mod p^2

5 is a primitive root mod 9

Now $\because$ 5 is a primitive root mod ^{2}

We can say that

5 is a primitive root mod 3^k

put $k = 4$

$\Rightarrow$ 5 is a primitive root mod 3^4

$\Rightarrow$ **5 is a primitive root mod 81**

(c) $\mathbb{Z}\phi(n)^* = \{ i \in \mathbb{Z}\phi(n) \mid \gcd(i, \phi(n)) = 1 \}$

P.T.O.

$$Z_{54}^* = \{ i \in Z_{54} \mid \gcd(i, 54) = 1 \}$$

$$= \{ 1, 5, 7, 11, 13, 17, 19, 23, \ldots \}$$

Set of primitive roots of mod $n = 81$ $= \{ \alpha^i \bmod 81 \mid i \in Z_{54}^* \}$

where $\alpha = 5$

So another primitive root of $5^2 \bmod 81 = 25$