Tutorial Sheet - 8

Solution

Ques-1 :- To find the last two digits of 9^{9^9}, we need to calculate

$$9^{9^9} \pmod{100}.$$

$$9^2 \equiv 81 \pmod{100}$$

$$9^3 \equiv 29 \pmod{100}$$

$$9^3 \times 9^3 = 9^6 \equiv 41 \pmod{100}$$

$$9^3 \times 9^6 = 9^9 \equiv 89 \pmod{100}$$

Now,

$$9^{9^9} \equiv 89^9 \pmod{100}$$

$\because$

$$89 \equiv -11 \pmod{100}$$

$$89^9 \equiv (-11)^9 \pmod{100}$$

or

$$89^9 \equiv (-11)^3 (-11)^3 (-11)^3 \pmod{100}$$

$$\equiv -31 \times 31 \times 31 \pmod{100}$$

$$\equiv -91 \pmod{100}$$

$$\equiv 9 \pmod{100}$$

Hence

$$\boxed{9^{9^9} \equiv 9 \pmod{100}}$$

Ques-2 :- Given a is an odd integer.

To prove $a^2 \equiv 1 \pmod 8$, we will Mathematical induction. [Here, $a = 2n+1$]

for $a = 1$ i.e. $n = 0$.

$$1^2 \equiv 1 \pmod 8$$

which is true.

Now, let us assume that for $a = 2k+1$, it is true. i.e. $(2k-1)^2 \equiv 1 \pmod 8$ —— ①

Now, we will prove that above will be true for $n = k+1$ also.

i.e. $(2k+1)^2 \equiv 1 \pmod 8$

[$\because$ $(2k+1)^2 = (2k-1)^2 + 8k$.]

$$\Rightarrow (2k-1)^2 + 8k \equiv 1 \pmod 8$$

$$1 + 0 \equiv 1 \pmod 8$$

[Using eqⁿ (1)]

Hence, $\boxed{a^2 \equiv 1 \pmod 8}$

Ques-3 :- (a) $9 + 8 \pmod{10}$

$= 17 \pmod{10}$

$= 7 \pmod{10}$

(b) $85 - 28 \pmod{20} = 57 \pmod{20} = 17 \pmod{20}$

OR

$= [85 \pmod{20} - 28 \pmod{20}] \pmod{20}$

$= 5 - 8 \pmod{20}$

$= -3 \pmod{20}$ or $17 \pmod{20}$

(c) $91 \times 89 \pmod{30}$

$= [91 \pmod{30} \times 89 \pmod{30}] \pmod{30}$

$= (1 \times -1) \pmod{30}$

$= -1 \pmod{30}$

$= 29 \pmod{30}$

Ques-4:- (a) $\because$ $a \equiv b \pmod{n}$

$\Rightarrow$ $a - b = k \cdot n$ —— (1)

and $c \equiv c \pmod{n}$

$\Rightarrow$ $c - c = 0 \cdot n$ —— (2)

Adding (1) & (2),

$(a-b) + (c-c) = k \cdot n + 0 \cdot n$

or $(a+c) - (b+c) = k \cdot n$

or $\boxed{a + c \equiv b + c \pmod{n}}$

Multiplying (1) & (2),

$ac = (kn + b)(0 \cdot n + c)$

$= kc \cdot n + bc$

$ac - bc = kc \cdot n$

$ac - bc = k_1 \cdot n$ [where $kc = k_1$]
$\downarrow$
an integer.

$\boxed{ac \equiv bc \pmod{n}}$

(b) To prove this part we use induction argument.

i.e. for $k = 1$,

$$a \equiv b \pmod{n}$$

which is true.

We will assume it is true for some fixed k.

And, $\because$ $a \equiv b \pmod{n}$

$$a^k \equiv b^k \pmod{n}$$

$\Rightarrow$ $a a^k \equiv b b^k \pmod{n}$ [Using the prop. if $a \equiv b \pmod{n}$ & $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$]

$\Rightarrow$ $a^{k+1} \equiv b^{k+1} \pmod{n}$

Hence, the induction steps proves that

$$a^k \equiv b^k \pmod{n}$$

Ques-5 :- (a)

$$1475 = 1 \times 1200 + 275$$
$$1200 = 4 \times 275 + 100$$
$$275 = 2 \times 100 + 75$$
$$100 = 1 \times 75 + \boxed{25}$$
$$75 = 3 \times 25 + 0$$

Hence 25 is the GCD of 1475 and 1200.

OR

q	r	s	t
1	1475	1200	275
4	1200	275	100
2	275	100	75
1	100	75	25
3	75	25	0
	$\boxed{25}$	0	

(b) 766 , 1235

$$1235 = 1 \times 766 + 469$$
$$766 = 1 \times 469 + 297$$
$$469 = 1 \times 297 + 172$$
$$297 = 1 \times 172 + 125$$
$$172 = 1 \times 125 + 47$$
$$125 = 2 \times 47 + 31$$
$$47 = 1 \times 31 + 16$$
$$31 = 1 \times 16 + 15$$
$$16 = 1 \times 15 + 1$$
$$15 = 15 \times 1 + 0$$

Hence GCD of 766 and 1235 is 1.

Ques-6 :- (a)

$$272 = 2 \times 119 + 34 \quad \text{—— (1)}$$
$$119 = 3 \times 34 + 17 \quad \text{—— (2)}$$
$$34 = 2 \times 17 + 0 \quad \text{—— (3)}$$

$$GCD(272, 119) = 17$$

$$17 = 119x + 272y$$

To find x & y,

$$17 = 119 - 3 \times 34 \quad \text{[from (2)]}$$
$$17 = 119 - 3 \times (272 - 2 \times 119) \quad \text{[from (1)]}$$
$$17 = 7 \times 119 - 3 \times 272$$

or $\boxed{17 = 119(7) + 272(-3)}$

Hence $x = 7$ and $y = -3$

(b) GCD (1769, 2378)

$$2378 = 1 \times 1769 + 609 \quad \text{———— (1)}$$
$$1769 = 2 \times 609 + 551 \quad \text{———— (2)}$$
$$609 = 1 \times 551 + 58 \quad \text{———— (3)}$$
$$551 = 9 \times 58 + \boxed{29} \quad \text{———— (4)}$$
$$58 = 2 \times 29 + 0$$

$\Rightarrow$ GCD (1769, 2378) = 29

Now find x & y s.t.

$$29 = 1769x + 2378y$$

$$29 = 551 - 9 \times 58 \quad \text{[Using (4)]}$$
$$29 = 551 - 9 \times (609 - 1 \times 551) \quad \text{[Using (3)]}$$
$$29 = 10 \times 551 - 9 \times 609$$
$$29 = 10 \times (1769 - 2 \times 609) - 9 \times 609 \quad \text{[Using 2]}$$
$$29 = 10 \times 1769 - 29 \times 609$$
$$29 = 10 \times 1769 - 29\,(2378 - 1 \times 1769) \quad \text{[Using (1)]}$$
$$\boxed{29 = 1769\,(39) + 2378\,(-29)}$$

$\Rightarrow$ $x = 39$ and $y = -29$.

Ques-7 :- (a) $18x \equiv 30 \pmod{42}$

Since GCD (18, 42) = 6 and $6 | 30$

$\Rightarrow$ given linear congruence have 6 sol^{n}s. and can be written as

$$3x \equiv 5 \pmod 7$$

$x_0 \equiv 4 + (42/6)\,t \equiv 4 + 7t \pmod{42}$ [$t = 0, 1, 2, 3, 4, 5$]

$x = 4, 11, 18, 25, 32, 39.$

(b) $9x \equiv 21 \pmod{30}$

Since $\gcd(9,30) = 3$ and $3 | 21$, Hence there must be three incongruent solutions:

$$3x \equiv 7 \pmod{10}$$

$$x \equiv 9 + (30/3)t \equiv 9 + 10t \quad , \quad t = 0, 1, 2$$

$$x = 9, 19, 29.$$

Ques-8 :- $Z_{15} = \{0, 1, 2, 3, ----, 14\}$

Multiplicative inverse,

$ab \equiv 1 \pmod{15}$ where $a, b \in Z_{15}$

$$1 \times 1 \equiv 1 \pmod{15}$$
$$2 \times 8 \equiv 1 \pmod{15}$$
$$4 \times 4 \equiv 1 \pmod{15}$$
$$7 \times 13 \equiv 1 \pmod{15}$$
$$11 \times 11 \equiv 1 \pmod{15}$$
$$14 \times 14 \equiv 1 \pmod{15}$$

3, 5, 6, 9, 10, 12 will not have their multiplicative inverse in Z_{15} as these integers are not relatively prime to 15.

Ques-9 :- $C = P * K \pmod{26}$

1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L

13	14	15	16	17	18	19	20	21	22	23	24
M	N	O	P	Q	R	S	T	U	V	W	X

25	26
Y	Z

Now, given $k = 5$

9 14 4 9 1
I N D I A

$\therefore \quad C = P \times k \pmod{26}$

$P = $ I N D I A

9 14 4 9 1

$P \times k = C = 9\times5 \quad 14\times5 \quad 4\times5 \quad 9\times5 \quad 1\times5 \pmod{26}$

$C = 19 \quad 18 \quad 20 \quad 19 \quad 5$

S R T S E

$\boxed{C = SRTSE}$