Mini Quiz 3 - Parth Patel

I have attached an image of my calculator

I certify I have complied with the written Instructions Parth Patel

Start Time : 12:28
Submitted Time : 1:26
Elapsed Time : 58 min

1

a) $81 = 3^4$, $\phi(3^4) = (3^4 - 3^3) = 81 - 27 = \boxed{54}$

b) $77 = 7 \cdot 11$, $\phi(77) = (7-1)(11-1) = \boxed{60}$

c) $\gcd(9,33) = 3$, $\frac{33}{\gcd(9,33)} = 33/3 = \boxed{11}$

d) Since 31 is prime, $\phi(31) = 30$

$$5^{50000} = 5^{20} \cdot 5^{49980} = 5^{20} \cdot (5^{30})^{1666}$$

Since $5^{30} \equiv 1 \bmod 31$, $5^{20} {5^{30}}^{1666} \equiv_{31} 5^{20}$

$$5^{20} = 5^2 \cdot (5^3)^6$$

$$5^3 = 125 \equiv_{31} 1$$

Since $5^3 \equiv 1 \bmod 31$, $5^{20} = 5^2 5^{36} \equiv_{31} 5^2 \equiv 25$

Answer

$\boxed{25}$

2 $3^{27} \bmod 37$

$27 = 11011_2$

digit	pow	Z
1	$3 \equiv_{37} 3$	$3 \cdot 1 \equiv_{37} 3$
1	$3^2 \equiv_{37} 9$	$9 \cdot 3 \equiv_{37} 27$
0	$3^4 \equiv_{37} 7$	27
1	$3^8 \equiv_{37} 7^2 \equiv 12$	$12 \cdot 27 \equiv_{37} 28$
1	$3^{16} \equiv_{37} 12^2 \equiv 33$	$33 \cdot 28 \equiv_{37} 36$

Answr $\boxed{36}$

(3) Suppose $a \in \mathbb{Z}_N^*$

Suppose $f_a(x_1) = f_a(x_2)$

The $f_a(x_1) = ax_1 \bmod N$
$f_a(x_2) = ax_2 \bmod N$

The $ax_1 \equiv_N ax_2 \bmod N$

Therefore $N \mid ax_1 - ax_2 \implies N \mid a(x_1 - x_2)$

Either $n \mid a$ or $N \mid x_1 - x_2$

Since $\gcd(N, a) = 1$ $(a \in \mathbb{Z}_N^*)$, $N \mid x_1 - x_2$

Consider the set $\mathbb{Z}_N^*$.

$\max\{Z_n\} = N-1$, $\min\{Z_n\} = 0$

Thus $0 \le x_1 - x_2 \le N-1$

Since $N \mid x_1 - x_2$, ~~and Z~~ $0 \le x_1 - x_2 \le N-1$, $x_1 - x_2 = 0$

$\implies x_1 = x_2$

Therefore $f_a(x)$ is $\boxed{1:1}$

$$7 \cdot \{0, \ldots, 10\} \bmod 11$$

$$\equiv_{11} (7 \cdot 1)_{11} \cdot (7 \cdot 2)_{11} \cdot (7 \cdot 3)_{11} \cdot \ldots \cdot (7 \cdot 10)_{11}$$

$$\equiv_{11} 10!$$

$$\equiv_{11} \boxed{10}$$

4

a	b	q	r
60	7	8	4
7	4	1	3
4	3	1	1
3	1	3	0

Q

$$\begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} = \begin{pmatrix} 1 & -8 \\ -1 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -8 \\ -1 & 9 \end{pmatrix} = \begin{pmatrix} -1 & 9 \\ 2 & -17 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} -1 & 9 \\ 2 & -17 \end{pmatrix} = \begin{pmatrix} 2 & -17 \\ -7 & 60 \end{pmatrix}$$

$60(2) + 7(-17) = \boxed{1}$ ⇐ Ans 1

Iteratios: $O(\log n)$ ⇐ Ans 2

5 $N = 77 \Rightarrow p = 11, q = 7 \Rightarrow \phi(77) = (11-1)(7-1) = 60$

Since $\phi(77)x + ed = 1$, $60(2) + e(-17) = 1$

$d = -17$ 60 · 2 =

Since $d < 0$, $d \equiv -17 \equiv_{\phi(N)} \equiv 43$

Answer
$\boxed{d = 43}$

Could $e = 5$ be chosen? $\boxed{\text{NO}}$ $\gcd(60, 5) = 5 \neq 1$

6 $M = 13 \quad 17$

$13^{43} \bmod 77 = 41$
$17^{43} \bmod 77 = 73$

$M_d = 41 \quad 73 \Rightarrow$ "J" "I"