Devansh Shah
1914078
B2

ITC tutorial 9

Q1) $11^{999} \pmod{23}$

$(999)_{10} = (1111100111)_2$

1	1	1	1	1	0	0	1	1	1
11	20	7	10	19	16	3	7	10	19

$11^2 \bmod 23 = 121 \bmod 23 = 6$
$6 \times 11 \bmod 23 = 66 \bmod 23 = 20$

$20^2 \bmod 23 = 400 \bmod 23 = 9$
$9 \times 11 \bmod 23 = 99 \bmod 23 = \cancel{10}\ 7$

$7^2 \bmod 23 = 49 \bmod 23 = 3$
$3 \times 11 \bmod 23 = 33 \bmod 23 = 10$

$10^2 \bmod 23 = 100 \bmod 23 = 8$
$8 \times 11 \bmod 23 = 88 \bmod 23 = 19$

$19^2 \bmod 23 = 361 \bmod 23 = \cancel{8}16$
$16^2 \bmod 23 = \cancel{88}256 \bmod 23 = 3$

$3^2 \bmod 23 = 9 \bmod 23 = \cancel{16}9$
~~9^2 mod~~
$9 \times 11 \bmod 23 = 99 \bmod 23 = 7$

$\therefore (11)^{999} \bmod 23 = 1911$

Q2) Find value of x using chinese remainder theorem : 1) $x = 3 \mod 5$ 2) $x = 1 \mod 7$
3) $x = 6 \mod 8$

Ans) Here, $a_1 = 3$, $a_2 = 1$, $a_3 = 6$, $m_1 = 5$, $m_2 = 7$, $m_3 = 8$

$M = m_1 \times m_2 \times m_3 = 5 \times 7 \times 8 = 280$

$M_1 = \frac{M}{m_1} = \frac{280}{5} = 56$, $M_2 = \frac{M}{M_2} = \frac{280}{7} = 40$

$M_3 = \frac{M}{m_3} = \frac{280}{8} = 35$

$M_1 x_1 = 1 \mod 5$

$(56 \times 1) \% 5 = 1$ $(56 \times 2) \% 5 = 2$ $(56 \times 3) \% 5 = 3$

$\boxed{x_1 = 1}$

$M_2 x_2 = 1 \% 7$

$(40 \times 1) \% 7 = 5$

$(40 \times 2) \% 7 = 3$

$(40 \times 3) \% 7 = 1$

$\boxed{x_2 = 3}$

$M_3 x_3 = 1 \mod 8$

$(35 \times 1) \% 8 = 3$

$(35 \times 2) \% 8 = 6$

$(35 \times 3) \% 8 = 1$

$\boxed{x_3 = 3}$

$x = (M_1 x_1 a_1 + M_2 x_2 a_2 + M_3 x_3 a_3) \mod M$

$= (56 \times 1 \times 3 + 40 \times 3 \times 1 + 35 \times 3 \times 6) \% 280$

$= (168 + 120 + 630) \% 280$

$= 918 \% 280$

$\boxed{x = 78}$

PAGE No.
DATE / /

Q3) Find x such that $7x = 3 \bmod 10$

Ans) To find multiplicative inverse of $7 \pmod{10}$

$= 7^{\phi(10)-1} = 7^{4-1} = 7^3 = 343$

$= 3 \bmod 10$

$7x = 3 \bmod 10$ — ①

In equation ①, multiply both sides by 3

$21x = 9 \pmod{10}$

Now, $21 \pmod{10} = 1$, $9 \pmod{10} = 9$ so,

$x = 9 \pmod{10}$

$\therefore \underline{x = 9}$

To verify, $7 \times 9 = 63 = 3 \pmod{10}$

Q4) How many smaller positive integer are there than 969 and are relative prime with 969.

Ans) $\phi(n) = \phi(969)$

$969 = 3 \times 17 \times 19$

$\phi(969) = \phi(3 \times 17 \times 19)$

$= \phi(3) \times \phi(17) \times \phi(19)$

$= 3-1 \times 17-1 \times 19-1$

$\because \phi(p) = p-1$ if p is prime

$= 2 \times 16 \times 18$

$\phi(969) = 576$

$\therefore$ 576 positive integers smaller than 969 are relative prime with 969.