Tutorial 9 Solution

Q1) Given $GCD(a,b) = ax+by$ where x and y are integers.

If $d = GCD(a,b)$, then $d = ax+by$.

Dividing both sides by d, we get

$$1 = \frac{a}{d}x + \frac{b}{d}y$$

Hence, $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime. Proved

Q2) (a) Given $a \equiv b \pmod{m}$

$\Rightarrow m \mid (a-b)$

$\Rightarrow m \mid c(a-b)$

$\Rightarrow m \mid (ac-bc)$

$\Rightarrow ac \equiv bc \pmod{m}$ Proved

(b) Given $a \equiv b \pmod{m}$

$\Rightarrow m \mid (a-b)$

$\Rightarrow m \mid (a-b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1})$

$\Rightarrow m \mid (a^k - b^k)$

$\Rightarrow a^k \equiv b^k \pmod{m}$ Proved

Q3 (a) GCD (1475, 1200) using Euclidean Algorithm

q	r	s	t
1	1475	1200	275
4	1200	275	100
2	275	100	75
1	100	75	25
3	75	25	0
	25	0	

∴ GCD (1475, 1200) = 25 Ans.

(b) GCD (766, 1235) using Euclidean Algorithm.

q	r	s	t
0	766	1235	766
1	1235	766	469
1	766	469	297
1	469	297	172
1	297	172	125
1	172	125	47
2	125	47	31
1	47	31	16
1	31	16	15
1	16	15	1
15	15	1	0

∴ GCD(766,1235)=1 Ans.

$3^{28} = (3^2)^{14} = 9^{14}$

In addition, $9 \equiv 4 \pmod 5$

We know that if $a \equiv b \pmod m$,

then $a^k \equiv b^k \pmod m$ for all $k \geq 1$

Thus, $9 \equiv 4 \pmod 5 \Rightarrow 9^{14} \equiv 4^{14} \pmod 5$

Moreover, $4^{14} = (4^2)^7 = 16^7$ and $16 \equiv 1 \pmod 5$

$16 \equiv 1 \pmod 5 \Rightarrow 16^7 \equiv 1^7 \pmod 5$

$\Rightarrow 16^7 \equiv 1 \pmod 5$

We know that if $a \equiv b \pmod m$ and $b \equiv c \pmod m$,

then $a \equiv c \pmod m$.

Thus $3^{28} \equiv 1 \pmod 5$

Hence, the remainder is 1.

5) ⓐ $(14+7) \bmod 15 = 21 \bmod 15 = 6$ Ans.

ⓑ $(7-11) \bmod 13 = -4 \bmod 13 = 9$ Ans.

ⓒ $(123 \times -10) \bmod 19 = -1230 \bmod 19 = 5$ Ans.