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	

$\therefore$ 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

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

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

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

Scanned by CamScanner

$a = 0$

Q6 $C = (P \times k) \bmod 26$

(1) Plaintext: h → 07 Encryption: $(07 \times 07) \bmod 26 = 49 \bmod 26$

$= 23 \rightarrow X$

(2) Plaintext: e → 04, Encryption: $(04 \times 07) \bmod 26 = 28 \bmod 26 = 02 \rightarrow C$

(3) Plaintext: l → 11, Encryption: $(11 \times 07) \bmod 26 = 77 \bmod 26 = 25 \rightarrow Z$

(4) Plaintext: l → 11, Encryption: $(11 \times 07) \bmod 26 = 77 \bmod 26 = 25 \rightarrow Z$

(5) Plaintext: o → 14, Encryption: $(14 \times 07) \bmod 26 = 98 \bmod 26 = 20 \rightarrow U$

∴ "hello" is encoded using the key 07 by Multiplicative Cipher to "XCZZU"

Q7 ~~Plaintext:~~ $C = (P \times K_1 + K_2) \bmod 26$ $K_1 = 07, K_2 = 02$

Plaintext: h → 07, Encryption: $(07 \times 07 + 02) \bmod 26 = 51 \bmod 26 = 25 \Rightarrow Z$

Plaintext: e → 04, Encryption: $(04 \times 07 + 02) \bmod 26 = 30 \bmod 26 = 4 \Rightarrow E$

Plaintext: l → 11, Encryption: $(11 \times 07 + 02) \bmod 26 = 79 \bmod 26 = 1 \rightarrow B$

Plaintext: l → 11, Encryption: $(11 \times 07 + 02) \bmod 26 = 79 \bmod 26 = 1 \rightarrow B$

Plaintext: o → 14, Encryption: $(14 \times 07 + 02) \bmod 26 = 100 \bmod 26 = 22 \rightarrow W$

∴ "hello" is encoded using the key pair 7, 2 by Affine Cipher to "ZEBBW"

Q8 If $a|b$

$b = ma$ where m is some integer ($m \in Z$) —(1)

If $a|c$

$c = na$ where n is some integer ($n \in Z$) —(2)

Adding ~~from~~ (1) & (2)

$b+c = ma + na = (m+n)a$ [If $m \in Z, n \in Z$, $(m+n) \in Z$]

$\therefore a | b+c$

Hence option C

Option A is also true
$a|b$ & $a|c$
then $a|bc$
$a|b$ then $b = ap$ $bc = (ap)c = a(pc)$ so $a|bc$

Q9 We need to find gcd (6, 15)

gcd (6, 15) = 3

Q10 gcd (252, 198) = 18

$\therefore 252x + 198y = 18$ [$x, y \in Z$]

From the given options, A satisfies the above equation

$252 \times 4 - 198 \times 5 = 1008 - 990 = 18$

$\therefore$ Solution is (A)

Q11

(a) $2x \equiv 5 \pmod 7$ $[ax \equiv b \pmod m]$

$\gcd(a,m) = d = \gcd(2,7) = 1$

& $d | b$ i.e $1|5$

$\therefore$ Solution exists & no. of solutions $= d = 1$

$\therefore$ Let $x_0 = 0, 1, 2, 3 \ldots$

Putting $x_0 = 6$

$2 \times 6 \equiv 5 \pmod 7$

$12 \equiv 5 \pmod 7$

$\therefore$ $\boxed{x_0 = 6}$ is the solution

(b) $6x \equiv 5 \pmod 8$ $[ax \equiv b \pmod m]$

$\gcd(a,m) = \gcd(6,8) = 2$

But $2|5$ is false

$\therefore$ $\boxed{\text{No Solution exists}}$

(c) $19x \equiv 30 \pmod{40}$ $[ax \equiv b \pmod m]$

$\gcd(a,m) = \gcd(19,40) = 1$

& $d|b$ i.e $1|30$

$\therefore$ Solⁿ exists & no. of solutions $= d = 1$

Let ~~Put~~ $x_0 = 0, 1, 2.$

Putting $x_0 = 10$

$19 \times 10 \equiv 30 \bmod (40)$

$190 \equiv 30 \bmod 40$

is true

$\therefore$ $\boxed{\text{Sol}^n \text{ is } 10}$

Q12 (a) $234x \equiv 60 \pmod{762}$ $[ax \equiv b \pmod{m}]$

$\gcd(a, m) = \gcd(234, 762)$

$= 6$

& $6 | 60$

$\therefore$ No of Solutions $= \gcd(a, m) = 6$

(b) $128x \equiv 833 \pmod{1001}$

$\gcd(a, m) = \gcd(128, 1001)$

$= 1$

& $1 | 833$

$\therefore$ No. of Solutions $= \gcd(a, m) = 1$