Tutorial-2

Page No.
Date

1) $39x + 15y = 270$
$\quad\quad a \quad\quad b \quad\quad c$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
2	39	15	9	1	0	1	0	1	-2
1	15	9	6	0	1	-1	1	-2	3
1	9	6	3	1	-1	2	-2	3	-5
2	6	3	0	-1	2	-5	3	-5	13
	3	0		2	-5		-5	13	

↓ gcd ↓ s ↓ t

check :- $39 \times 2 + 15 \times (-5) = 3$

$78 - 75 = 3$

$\boxed{3 = 3}$

↑ d

Since, 3 divides 270, Hence there exist infinite soln.

Particular soln :-

$x_0 = (c/d)s \quad , \quad y_0 = (c/d)t$

$= 90(2) \quad\quad = 90(-5)$

$\boxed{x_0 = 180} \quad\quad \boxed{y_0 = -450}$ Ans

General soln :-

$x = x_0 + k(b/d) = 180 + k(5)$

$y = y_0 - k(a/d) = -450 - k(13)$ } Ans.

2) $256x \equiv 442 \bmod (60)$

q	r_1	r_2	r	t_1	t_2	t
	60	256	60	0	1	0
4	256	60	16	1	0	1
3	60	16	12	0	1	-3
1	16	12	4	1	-3	4
3	12	4	0	-3	4	-15
	4	0		4	-15	

↓ gcd

Since, 4 does not divide 442. Hence, no sol^n exist.

ii) $232x + 42 \equiv 248 \pmod{50}$

$232x + 42 - 42 \equiv 248 - 42 \pmod{50}$

$232x \equiv 206 \pmod{50}$

q	r_1	r_2	r	t_1	t_2	t
0	50	232	50	0	1	0
4	232	50	32	1	0	-3
1	50	32	18	0	-3	3
1	32	18	14	-3	3	-6
1	18	14	4	3	-6	9
3	14	4	2	-6	9	-33
2	4	2	0	9	-33	75
	2	0		-33	75	

↓ gcd

Since $2 \mid 206$. Hence, there exist 2 sol^n.

$232x \equiv 206 \pmod{50}$

$116x \equiv 103 \pmod{25}$

$x = (103 \times 116^{-1}) \bmod 25$

$\hookrightarrow (-33 \bmod 25) = -8 \bmod 25 = 17$

$x_0 = (103 \times 17) \bmod 25 = 1751 \bmod 25$

$= 1$ sol^n

$x_1 = x_0 + k(m/d) = 1 + 1 \times (50/2) = 26$. } Ans.

3) $IP = x^8 + x^4 + x + 1$

$P_1 = x^5 + x^2 + x$

$P_2 = x^7 + x^4 + x^3 + x^2 + x$

			Red^n
$x^0 \otimes P_2$	$x^7 + x^4 + x^3 + x^2 + x$	$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes P_2$	$x \otimes (x^7 + x^4 + x^3 + x^2 + x)$ $= x^8 + x^5 + x^4 + x^3 + x^2$	$x^5 + x^3 + x^2 + x + 1$	Yes
$x^2 \otimes P_2$	$x \otimes (x^5 + x^3 + x^2 + x + 1)$	$x^6 + x^4 + x^3 + x^2 + x$	No
$x^3 \otimes P_2$	$x \otimes (x^6 + x^4 + x^3 + x^2 + x)$	$x^7 + x^5 + x^4 + x^3 + x^2$	No
$x^4 \otimes P_2$	$x \otimes (x^7 + x^5 + x^4 + x^3 + x^2)$ $= x^8 + x^6 + x^5 + x^4 + x^3$	$x^6 + x^5 + x^3 + x + 1$	Yes
$x^5 \otimes P_2$	$x \otimes (x^6 + x^5 + x^3 + x + 1)$	$x^7 + x^6 + x^4 + x^2 + x$	No

$$x^8 + x^4 + x + 1 \;\overline{)\; x^8 + x^5 + x^4 + x^3 + x^2 \;(\; 1}$$

$$x^8 + x^4 + x + 1$$

$$x^5 + x^3 + x^2 + x + 1$$

$$P_1 \otimes P_2 = (x^7 + x^6 + x^4 + x^2 + x) + (x^6 + x^4 + x^3 + x^2 + x) + (x^5 + x^3 + x^2 + x + 1)$$

$$= x^7 + x^5 + x^2 + x + 1. \quad \text{Ans}$$

Page No.
Date

4) $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

$M = m_1 \times m_2 \times m_3$
$= 3 \times 5 \times 7 = 105$

$M_1 = 35$, $M_2 = 21$, $M_3 = 15$

$M_1^{-1} = 35^{-1} \bmod 3$, $M_2^{-1} = 21^{-1} \bmod 5$, $M_3 = 15^{-1} \bmod 7$

$= 2$ $= 1$ $= 1$

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= (140 + 63 + 30) \bmod 105$
$x = 233 \bmod 105 = 23.$

$x = 23$. Ans

$\phi(1) = 0$

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

$\phi(m \times n) = \phi(m) \times \phi(n)$ if m & n are rel. prime

$\phi(p^e) = p^e - p^{e-1}$

$a^{p-1} = 1 \bmod p$

$a^p = a \bmod p$

$a^{-1} \bmod p = a^{p-2} \bmod p$

$a^{\phi(m)} \equiv 1 \bmod n$

$a^{k \times \phi(m)+1} \equiv a \bmod n$

$a^{-1} \bmod n = a^{\phi(m)-1} \bmod n$

Ex: $44^{-1} \bmod 667 = 44^{665} \bmod 667 = 244$ Ans

$44^{665} \bmod 667$

i	x_i	$y \equiv 1$	$a = 44$
0	1	44	602
1	0		223
2	0		371
3	1	316	239
4	1	153	426
5	0		52
6	0		36
7	1	172	629
8	0		110
9	1	244	

244 Ans

Page No.
Date

$y = a \times y \bmod n$

$a = a^2 \bmod n$

In $17364^{41} \bmod 2134$

i	x_i	$y = 1$	$a = 17364$
			2038
0	1	292	680
1	0		1456
2	0		874
3	1	486	2038
4	0		
5	1	292	

292 Ans

q	r_1	r_2	r	t_1	t_2	t
x	x^4+x+1	x^3+x+1	x^2+1	0	1	x
x	x^3+x+1	x^2+1	1	1	x	$1+x^2$
x^2+1	x^2+1	1	0	x	$1+x^2$	x
	1	0		$1+x^2$	x	

gcd

(multiplicative inverse).

$$x^3+x+1 \overline{)\, x^4+x+1 \,(\, x}$$
$$x^4+x^2+x$$
$$x^2+1$$

$$x^2+1 \overline{)\, x^3+x+1 \,(\, x}$$
$$x^3+x$$
$$1$$

$$1 \overline{)\, x^2+1 \,(\, x^2+1}$$
$$x^2$$
$$1$$
$$1$$
$$0$$

$$(1+x^2)^2 = x^4+1+2x^2$$

$$x^4+1+x^4+x^0+1 = x$$

$8^{-1} \bmod 15$

Page No.
Date

$9^{5} \% 15$

$= 9^{10} \cdot 9^{1}$

$\Rightarrow 1023 \times 2^{1}$

$a = 2, \quad m = 1023, \quad k = 1$

since, $k-1 = 0$; so it'll never enter loop.

Hence, it is composite.

7) $2047 - 1 = 2046$

2	2046
3	1023
	341

$T = a^{m} \bmod n$

$T = T^{2} \bmod n$

if $(T = 1)$ composite

$T = -1$ prime

Page No.
Date

8) $IR = x^4 + x + 1$

0	0	0000
g^0	1	0001
g^1	g	0010
g^2	g^2	0100
g^3	g^3	1000
g^4	$g+1$	0011
g^5	$g(g+1) = g^2+g$	0110
g^6	g^3+g^2	1100
g^7	$g^4+g^3 = g^3+g+1$	1011
g^8	$g^4 \times g^4 = g^2+g+g+1 = g^2+1$	0101
g^9	g^3+g	1010
g^{10}	$g^4+g^2 = g^2+g+1$	0111
g^{11}	g^3+g^2+g	1110
g^{12}	$g^4+g^3+g^2 = g^3+g^2+g+1$	1111
g^{13}	$g^4+g^3+g^2+g = g^3+g^2+1$	1101
g^{14}	$g^4+g^3+g = g^3+1$	1001

$g^3 / g^8 = g^3 \times g^{-8\%15} = g^3 \times g^7 = g^{10}$

$= g^2+g+1 = 0111$ Ans

9) $G = \langle 2, 19, \mathbb{N} \rangle$

$\phi(19) = 18$

elements = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18

28 mod 19

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	3	9	8	5	15	17												
4																		
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		
13																		
14																		
15																		
16																		
17																		
18																		

ii) $x^2 \equiv 3 \bmod 23$

$3^{(22)/2} \% 23 = 1 \rightarrow QR.$

$p = 4k+3$

$x = \pm a^{(p+1)/4} \% 23$

$= \pm 3^{(24/4)} \% 23 = \pm 16.$

ii) $x^2 = 7 \bmod 19$

$7^{18/2} \% 19 \equiv 1 \rightarrow QR.$

$p = 4k+3 \Rightarrow x = \pm (7)^{(20/5)} \% 19$

$= \pm 7^5 \% 19 = \pm 11.$

Page No.
Date

15 g^{20} $2^4 + 1 = 15$

$g^{20 \bmod 15} = g^5$

$g^3 = g^3$

$g^4 = g + 1$

$g^5 = g^2 + g$. Ans

16) $x^2 \equiv 36 \pmod{77}$

$77 = 7 \times 11$

$x^2 = 36 \bmod 7 = 1 \bmod 7$, $x^2 = 36 \bmod 11 = 3 \bmod 11$

~~$x \equiv 1 \bmod 7$~~

$x^2 \equiv 1 \bmod 7$

$x = \pm (1)^{8/4} = \pm 1$

$x^2 \equiv 3 \bmod 11$

$x = \pm 3^{12/4} = 27 \bmod 11$

$= \pm 5$

set 1 :- $x \equiv +1 \bmod 7$, $x \equiv +5 \bmod 11$

$M = 7 \times 11 = 77$

$M_1 = 11$, $M_2 = 7$

$M_1^{-1} = 11^{-1} \bmod 7$ $\quad M_2^{-1} = 7^{-1} \bmod 11$

$= 2$ $\quad = 8$

$x = (1 \times 11 \times 2 + 5 \times 7 \times 8) \% 77$

$= (22 + 280) \% 77$

$x \equiv 71 \bmod 77$ Ans

set 2 :- $x \equiv 1 \bmod 7$, $x \equiv 6 \bmod 11$

$x = (1 \times 11 \times 2 + 6 \times 7 \times 8) \% 77$

$= 22 + 336 = 358 \% 77 = 50 \bmod 77$ Ans

set 3 $\Rightarrow$ $x \equiv 6 \bmod 7$, $x \equiv 5 \bmod 11$

$x = (6 \times 22 + 5 \times 56) \bmod 77$

$= 132 + 280 = 27 \bmod 77$ Ans

set 4 $\Rightarrow$ $x \equiv 6 \bmod 7$, $x \equiv 6 \bmod 11$

$x = (6 \times 22 + 6 \times 56) \% 77$

$= 468 \% 77 = 6 \% 77$ Ans