Tutorial 2 Networks securities.

Date
DELTA Pg No.

Q1

Find the particular and general soln to the following Diophantine eqn

$39x + 15y = 270$

We have $d = \gcd(39, 15) = 3$

Since $3 \mid 270$, the eqn has infinite no of solutions

We can divide both sides by 3 to find eq $13x + 5y = 90$.

Using extended Euclidean algo, we find s and t as $13s + 5t = 1$

Sol^n

$39x + 15y = 270$

$a \quad b \quad c$

$s \times a + t \times b = \gcd(a, b)$

$s_1 = 1, \; 0 = s_2$

$t_1 = 0, \; 1 = t_2$

$r_1 = 39, \; r_2 = 15, \; r_1/r_2 = 2$

$r = r_1 - q \times r_2 \qquad s = s_1 - q \times s_2 \qquad t = t_1 - q \times t_2$

	q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
initialize →	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 → (d)			s			t		

$r_1 \leftarrow r_2$
$r_2 \leftarrow r$
$s_1 \leftarrow s_2$
$s_2 \leftarrow s$
$t_1 \leftarrow t_2$
$t_2 \leftarrow t$

Let's check :- $s \times a + t \times b = \gcd(a, b)$

$2 \times 39 + -5 \times 15 = 3$

$78 - 75 = 3$

$3 = 3$ ✓

~~Since, 3 divides 270~~

Particular sol^n :- $x_0 = \left(\frac{c}{d}\right) s \qquad y_0 = \left(\frac{c}{d}\right) t$

$= \left(\frac{270}{3}\right) \times 2 \qquad = \left(\frac{270}{3}\right) \times (-5)$

$x_0 = 180 \qquad y_0 = -450$

$b/d = \frac{15}{3} = 5, \quad a/d = \frac{39}{3} = 13$

General sol^n :-

$x = x_0 + k(b/d) \Rightarrow \boxed{x = 180 + 5k}$

$y = y_0 - k(a/d) \Rightarrow \boxed{y = -450 - 13k}$

Date
DELTA Pg No.

2 (i) Find the soln for the following ~~Diophantine~~ linear eqn

(i) $256x \equiv 442 \pmod{60}$

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

$q = r_1/r_2$	q	r_1	r_2	r	t_1	t_2	t
$60/256 = 0$	0	60	256	60	0	1	0
$r = r_1 - qr_2$	4	256	60	16	1	0	1
$t = t_1 - qt_2$	3	60	16	12	0	1	-3
$r_1 \leftarrow r_2$	1	16	12	4	1	-3	4
$r_2 \leftarrow r$	3	12	4	0	-3	4	-15
$t_1 \leftarrow t_2$		4	0		4	-15	
$t_2 \leftarrow t$		↓ gcd					

t_1 t_2
0 1 ← initialized

∵ Since 4 does not divide 442, $4 \nmid 442$
Hence, no soln exist.

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

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

$232x \equiv 206 \pmod{50}$ $t_1 = 0$, $t_2 = 1$

$q = r_1/r_2 = 50/232 = 0$
$r = r_1 - qr_2$
$t = t_1 - qt_2$
$r_1 \leftarrow r_2$, $r_2 \leftarrow r$
$t_1 \leftarrow t_2$, $t_2 \leftarrow t$

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			?	↑ inverse	

$n_0 = -33 \bmod 50 = 50 - 33 = 17$

Since $2 \mid 206$, Hence there exists 2 soln

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

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

$x_0 = (103 \times 116^{-1}) \bmod 25$

$x_0 = (103 \times 11) \bmod 25$

$x_0 = 8 \bmod 25 = 8$

~~$x_0 = (103 \times 8) \bmod 25 = 824 \bmod 25 = 24$~~

~~$x_1 = x_0 + k(n/d) = 24 + k\left(\frac{200}{2}\right) = 24 + k\left(\frac{50}{2}\right) = 24 + 25k$~~

~~$= 24 + 25 \times 1$~~

~~$x_1 = 49$~~

$x_1 = x_0 + k(n/d) = 8 + k\left(\frac{50}{2}\right) = 8 + 25k = 8 + 25 \times 1$

$x_1 = 33$

$x_1 = 17 + 1 \times 25 = 42$?

Chapter-4 pg-113

Q3 Find the result of multiplying $P_1 = (X^5 + X^2 + X)$ by $P_2 = (X^7 + X^4 + X^3 + X^2 + X)$ in $GF(2^8)$ with irreducible polynomial $(X^8 + X^4 + X + 1)$.

Sol $IP = X^8 + X^4 + X + 1$ $\quad P1 = X^5 + X^2 + X$

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

powers	operation	New Result	Reduction
$x^0 \otimes P_2$		$x^7+x^4+x^3+x^2+x$	No
→ $x^1 \otimes P_2$	$x \otimes (x^7+x^4+x^3+x^2+x)$		
	$= x^8+x^5+x^4+x^3+x^2$		
	$= x^4+x+1+x^5+x^4+x^3+x^2$	$= x^5+x^3+x^2+x+1$	Yes
→ $x^2 \otimes P_2$	$x^2 \otimes (x^7+x^4+x^3+x^2+x)$		
	$= x^9+x^6+x^5+x^4+x^3$		
	$= x(x^8)+x^6+x^5+x^4+x^3$		
	$= x(x^4+x+1)+x^6+x^5+x^4+x^3$		
	$= x^5+x^2+x+x^6+x^5+x^4+x^3$	$= x^6+x^4+x^3+x^2+x$	No
	$x \otimes x^5+x^3+x^2+x+1$	$x^7+x^5+x^4+x^3+x^2$	No
$x^3 \otimes P_2$	$x \otimes (x^6+x^4+x^3+x^2+x)$		
$x^4 \otimes P_2$	$x \otimes (x^7+x^5+x^4+x^3+x^2)$		
	$= x^8+x^6+x^5+x^4+x^3$		
	$= x^4+x+1+x^6+x^5+x^4+x^3$	$= x^6+x^5+x^3+x+1$	Yes
→ $x^5 \otimes P_2$	$x(x^6+x^5+x^3+x+1)$	$= x^7+x^6+x^4+x^2+x$	No

$P_1 \times P_2$ $\quad x^5+x^3+x^2+x+1 + x^6+x^4+x^3+x^2+x + x^7+x^5+x^4+x^2+x$

$= x^7+x^5+x^2+x+1$

Q5) (i) $44^{-1} \bmod 667$

q	r_1	r_2	r	t_1	t_2	t
15	667	44	7	0	1	$0-15$
6	44	7	2	1	-15	91
3	7	2	1	-15	91	-288
2	2	1	0	91	-288	667
	1	0		-288	667	

↓ inverse

$44^{-1} \bmod 667$

$= -288 \bmod 667$

$= 667 - 288 = 379$

$= 379 \bmod 667$

$= 379$

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

Date
DELTA Pg No.

Q5 If the value of the following (i) $44^{-1} \bmod 667$ (ii) ~~17364^{41}~~ ^{41} ~~mod~~

(ii) $17364^{41} \bmod 2134$ (Using square and multiply method)

(i) $44^{-1} \bmod 667 = 44^{667-2} \bmod 667 = 44^{665} \bmod 667$

$a \uparrow \quad n \uparrow$

$665 = (1\,0\,1\,0\,0\,1\,1\,0\,0\,1)_2 \leftarrow x$

i	x_i	$y=1$ (initialize)	$a = 44$
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	94

if $x_i = 1 \Rightarrow y = ay \bmod n$

everytime $a = a^2 \bmod n$

$44^2 \bmod 667 = 602$

$y = 44 * 371 \bmod 667 = 316$

$\Rightarrow 44^{-1} \bmod 667 = 244$

(ii) $17364^{41} \bmod 2134$ $\quad a = a^2 \bmod n$

$41 = 1\,0\,1\,0\,0\,1$

i	x_i	$y=1$, $y = ay \bmod n$	$a = 17364$
0	1	292	2038
1	0	"	680
2	0	486	1456
3	1		874
4	0	"	2038
5	1	292	

$17364^{41} \bmod 2134 = 292$

Q4 ~~If the value of the following: (i)~~

If the value of X is defines as follows : $\quad X \equiv 2 \pmod 3$ $\quad X \equiv 3 \pmod 5$ $\quad X \equiv 2 \pmod 7$

Find suitable X value to satisfy given eq using CRT

Chinese Remainder Theorem

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

$M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$ $\quad M_3 = \frac{105}{7} = 15$

$M_1^{-1} = 35^{-1} \bmod 3$ $\quad b_1 = 2$

$M_2^{-1} = 21^{-1} \bmod 5$ $\quad b_2 = 1$

$M_3^{-1} = 15^{-1} \bmod 7$ $\quad b_3 = 1$

$x = (a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3) \bmod 105$

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

$x = 233 \bmod 105 = 23$

$x = 23$

Q6 Find the multiplicative inverse of (x^3+x+1) in GF(2^4) with the modulus (x^4+x+1) using extended Euclidean algo.

$r_1 = x^4+x+1$ $\quad r_2 = x^3+x+1$

$q = r_1 / r_2 = x$ $\quad t_1 = 0$ $\quad t_2 = 1$

$r = r_1 - q r_2$ $\quad t = t_1 - q t_2$

$r_1 \leftarrow r_2$, $r_2 \leftarrow r$ $\quad t_1 \leftarrow t_2$ $\quad t_2 \leftarrow t$

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	$+x$	$1+x^2$	$x^4+1 = x+x+x = x$
	1	0		$1+x^2$	x	
	↓			↓		
	gcd			multiplicative inverse		$= 1+x^2$

Verify $(1+x^2)(x^3+x+1) \pmod{x^4+x+1}$

$= (x^5+x^3+x^2) \pmod{x^4+x+1} = (x^5+x^2+x+1) \pmod{x^4+x+1}$

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

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

$= x^2+x+x^2+x+1$

$= 1$

Q7 Using Miller–Rabin test, prove that the number 2047 is prime or composite.

$n-1 = m \times 2^k$

$2047-1 = 2046$

$\Rightarrow 2047-1 = 1023 \times 2^1$ (n, m, a, k)

2	2046
3	1023
	341

Initialisation: $T = 2^{1023} \bmod 2047$

for $i = 1$ to $k-1$

$= 1$ (eq 0)

$\therefore$ no loop

$\because k-1 = 1-1 = 0$

& it'll never enter loop

Hence a composite no.

Q8 Generate elements of the field $GF(2^4)$ using the IP $f(x) = x^4+x+1$. Also find value of g^3/g^8

$g^0 = 0 = 0000$
$g^0 = 1 = 0001$
$g^1 = g = 0010$
$g^2 = g^2 = 0100$
$g^3 = g^3 = 1000$
$g^4 = g+1 = 0011$
$g^5 = g^2+g = 0110$
$g^6 = g^3+g^2 = 1100$
$g^7 = g^4+g^3 = g^3+g+1 = 1011$
$g^8 = g^4+g^2+g = g^2+g+1 = 0101$
$g^9 = g^3+g = 1010$
$g^{10} = g^4+g^2 = g^2+g+1 = 0111$
$g^{11} = g^3+g^2+g = 1110$
$g^{12} = g^4+g^3+g^2 = g^3+g^2+g+1 = 1111$
$g^{13} = g^4+g^3+g^2+g$
$= g+1+g^3+g^2+g$
$= g^3+g^2+1 = 1101$
$g^{14} = g^4+g^3+g = g+1+g^3+g$
$= g^3+1 = 1001$
$g^{15} = g^4+g = g+1+g = 1 = 0001$

$g^3/g^8 = g^3 \times g^{-8 \bmod 15} = g^3 \times g^{7 \bmod 15} = g^3 \times g^7 = (g^3 \times (g^3+g+1)) \pmod{IP}$
$= g^6+g^4+g^3 \pmod{IP}$
$= g^3+g^2+g+1+g^3$
$= g^2+g+1 = 0111 = g^{10}$

Q9 Find the order of elements and primitive roots of $a^i \equiv x \pmod{19}$ defined for the group $G = \langle Z_{19}^*, \times \rangle$

$\phi(19) = 18$ elements = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19.

i =	1	2	3	4	... 18
a_1 = 1	1	1	1	1	1 ...
a_2 = 2	2	4	8	16	
3	3	9	8	5	
} 18					

Pg = 276

Tutorial 2

quad non residue = QNR

Q11 Using quadratic residue (QR), solve following congruences:-

(i) $x^2 \equiv 3 \bmod 23$ (ii) $x^2 \equiv 7 \bmod 19$

in eq $x^2 \equiv a \pmod p$, p is prime and a is QR if eq has 2 solns and a is QNR if no soln

in Z_p^* with $(p-1)$ elements $\frac{(p-1)}{2}$ elements are QR and $\frac{p-1}{2}$ are QNR

if $a^{(p-1)/2} \equiv 1 \bmod p \Rightarrow$ a is QR

if $a^{(p-1)/2} \equiv -1 \bmod p \Rightarrow$ a is QNR

(i) $x^2 \equiv 3 \bmod 23 \Rightarrow a = 3$

$\Rightarrow 3^{(23-1)/2} \bmod 23 = 3^{22/2} \bmod 23$

$= 3^{11} \bmod 23 = 1$

$23 = 4k+3 \Rightarrow x = \pm a^{(p+1)/4} \bmod 23$

$x = \pm 3^6 \bmod 23 \Rightarrow x = \pm 16 \bmod 23$

(ii) $x^2 \equiv 7 \pmod{19} \Rightarrow a = 7$

$7^{(19-1)/2} \bmod 19 = 7^9 \bmod 19 = 1 \Rightarrow$ QR

$19 = 4k+3 \Rightarrow x = \pm a^{\frac{p+1}{4}} \bmod 19$

$x = \pm 7^{20/4} \bmod 19 \quad x = \pm 7^5 \bmod 19$

$x = \pm 11 \bmod 19$

(Tut) same as Q6, Q14 same as Q7

Q15 Find g^{20} value for $GF(2^4)$ using IR $f(x) = x^4 + x + 1$

$g^{20} = (g^4)^5 = (g+1)^5 = (g+1)(g^4+1) = (g+1)(g+1+1)$

$= x^5 + x + x^4 + 1 \quad = g^4 + g$

$= 0110$

$= g^5$

Q16 Assuming the quadratic congruence modulo a composite is defined as $x^2 \equiv 36 \bmod 77$. Find all value of x for this congruence

$77 = 7 \times 11$

$x^2 \equiv 36 \bmod 7 = 1 \bmod 7 \longrightarrow x = \pm 1^{\frac{7+1}{4}} \bmod 7 = \pm 1^2 \bmod 7 = \pm 1 \bmod 7$

and $x^2 \equiv 36 \bmod 11 = 3 \bmod 11 \longrightarrow x = \pm 3^{\frac{11+1}{4}} \bmod 11 = \pm 3^3 \bmod 11 = \pm 27 \bmod 11$

$x = \pm 5 \bmod 11$

Set 1 :-

b) $x = \pm 1 \bmod 7$, $x = \pm 5 \bmod 11$

$M = 7 \times 11 = 77$

$M_1 = 77/7 = 11$, $M_2 = 77/11 = 7$

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

$= 2$ $\qquad$ $= 8$

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

$x = (22 + 280) \bmod 77$

$x = 71 \bmod 77$

Set 2 : $x = 1 \bmod 7$, $x = -5 \bmod 11 = 6 \bmod 11$

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

$x = 50 \bmod 77$

Set 3 $x = -1 \bmod 7 = 6 \bmod 7$, $x = 5 \bmod 11$

$x = (6 \times 11 \times 2 + 5 \times 7 \times 8) \bmod 77$

$= 27 \bmod 77$

Set 4 $x = 6 \bmod 7 = 6 \bmod 7$, $x = -5 \bmod 11 = 6 \bmod 11$

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

$x = 6 \bmod 77$