Name : SHAHABUDDIN

Roll no. : 19BCS031

Semester : VIII

Assignment Network Security

Tutorial Sheet - 2

19BCS032
Shahabuddin

(1) Diophantine Equation

$ax + by = c$

$d = gcd(a, b)$

$d \mid c \longrightarrow$ infinite solution

$d \nmid c \longrightarrow$ No solution

$39x + 15y = 270$

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

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(a, b)			↓ s			↓ t		

$\because 3 \mid 270$, Thus Infinite Solution.

particular Solution :

$x_0 = (c/d)s = (270/3) \times 2 = 180$

$y_0 = (c/d)t = (270/3) \times -5 = -450$

General Solution :

$x = x_0 + (b/d)k = 180 + (15/3)k = \underline{180 + 5k}$

$y = y_0 - (a/d)k = -450 - (39/3)k = \underline{-450 - 13k}$

19BCS031 Shahabuddin

(2) Linear Congruence (single variable)

$$ax \equiv b \pmod{n}$$

$$d = \gcd(a, n)$$

if $d \mid b \rightarrow$ d solutions

if $d \nmid b \rightarrow$ No solution

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

$$d = \gcd(256, 60) = \gcd(60, 16) = \gcd(16, 12)$$
$$= \gcd(12, 4) = \gcd(4, 0) = 4$$

Here, $4 \nmid 442$, Thus no solution

19BCS031 Shahabuddin

(2)

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

Add -42 both sides

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

$d = \gcd(232, 50) = \gcd(50, 32), = \gcd(32, 18)$

$= \gcd(18, 14) = \gcd(14, 4) = \gcd(4, 2) = \gcd(2, 0)$

$= 2$

$\because 2 \mid 206$ Thus, two solutions exist

Now, divide both sides by $d (=2)$ including modulus

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

Multiply both sides by 116^{-1}

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

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

$= 33 \bmod 25$

$= 8$

$\therefore \boxed{x_0 = 8}$

$x = x_0 + K(n/d) = 8 + K(50/2)$

$= 8 + K \times 25$

$= 8 + 1 \times 25 = 33$

Thus, the two solutions are 8 & 33.

(3) Given,

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

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

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

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

$= x^8 + x^5 + x^4 + x^3 + x^2$

$= x^4 + x + 1 + x^5 + x^4 + x^3 + x^2$

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

$x^2 \otimes P_2 = x \otimes (x^5 + x^3 + x^2 + x + 1)$

$= x^6 + x^4 + x^3 + x^2 + x$

$x^3 \otimes P_2 = x \otimes (x^6 + x^4 + x^3 + x^2 + x)$

$= x^7 + x^5 + x^4 + x^3 + x^2$

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

$= x^8 + x^6 + x^5 + x^4 + x^3$

$= x^4 + x + 1 + x^6 + x^5 + x^4 + x^3$

$= x^6 + x^5 + x^3 + x + 1$

$x^5 \otimes P_2 = x \otimes (x^6 + x^5 + x^3 + x + 1)$

$= x^7 + x^6 + x^4 + x^2 + x$

Now,

$P_1 \otimes P_2 = (x^1 \otimes P_2) + (x^2 \otimes P_2) + (x^5 \otimes P_2)$

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

19BCS031 Shahabuddin

(4) Chinese Remainder Theorem (CRT) :

$x \equiv 2 \pmod 3 \longrightarrow x \equiv a_1 \pmod{m_1}$

$x \equiv 3 \pmod 5 \longrightarrow x \equiv a_2 \pmod{m_2}$

$x \equiv 2 \pmod 7 \longrightarrow x \equiv a_3 \pmod{m_3}$

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

$M_1 = M/m_1 = \frac{105}{3} = 35$

$M_2 = M/m_2 = \frac{105}{5} = 21$

$M_3 = M/m_3 = \frac{105}{7} = 15$

$M_1^{-1} \bmod m_1 = 35^{-1} \bmod 3 = \underline{2}$

$M_2^{-1} \bmod m_2 = 21^{-1} \bmod 5 = \underline{1}$

$M_3^{-1} \bmod m_3 = 15^{-1} \bmod 7 = \underline{1}$

$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + a_3 \times M_3 \times M_3^{-1}) \bmod M$

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

$= (140 + 63 + 30) \bmod 105$

$= 233 \bmod 105$

$= \underline{23}$

Thus, $\boxed{x = 23}$

19BCS031 Shahabuddin

(5) ii) $44^{-1} \bmod 667 = ?$

$r = r_1 - q \times r_2$ | $t = t_1 - q \times t_2$

q	r_1	r_2	r	t_1	t_2	t
15	667	44	7	0	1	-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	

$44^{-1} \bmod 667 = -288 \bmod 667$

$= 379$

Thus, $44^{-1} \bmod 667 = 379$

19BCS031 Shahabuddin

(5) ii) $17364^{41} \bmod 2134 = ?$

using Square and multiply method

32	16	8	4	2	1
1	0	1	0	0	1

$(41)_{10} = (101001)_2$

i	x_i	Multiplication ($Y=1$)	Squaring $a = 17364$
0	1	$Y = 1 \times 17364 \bmod 2134 = 292$	$a = 17364^2 \bmod 2134 = 2038$
1	0		$a = 2038^2 \bmod 2134 = 680$
2	0		$a = 680^2 \bmod 2134 = 1456$
3	1	$Y = (292 \times 1456) \bmod 2134 = 486$	$a = 1456^2 \bmod 2134 = 874$
4	0		$a = 874^2 \bmod 2134 = 2038$
5	1	$Y = (486 \times 2038) \bmod 2134 = 292$	

$a = (2038 \times 2038) \bmod 2134$
$= (4076 \times 1019) \bmod 2134$
$= (1942 \times 1019) \bmod 2134$
$= 680$

$a = (1456 \times 1456) \bmod 2134$
$= (728 \times 2912) \bmod 2134$
$= (728 \times 778) \bmod 2134$
$= 874$

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

19BCS031 Shahabuddin

⑥ $(x^3+x+1)^{-1}$ modulo (x^4+x+1) = ?

$r = r_1 - q \times r_2$ | $t = t_1 - q \times t_2$

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	(x^2+1)	0
	1	0		(x^2+1)	0	
	gcd					

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

$$(x^2+1)^2 = x^4+1+2x^2 \quad (2x^2 \to 0)$$
$$= x+1+1$$
$$= x$$

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

Thus,

$$(x^3+x+1)^{-1} \text{ modulo } (x^4+x+1) = x^2+1$$

19BCS031 Shahabuddin

(7) Miller - Rabin test :

$2047 - 1 = 2046$

$\Rightarrow \quad 2047 - 1 = 2^1 \times 1023$

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

Here, $K = 1$

from 0 to $K-1$ $(1-1=0)$, it will never enter in the loop.

Thus, 2047 is composite.

19BCS031 Shahabuddin

GF(2^4)

(8) Given, $Ip = f(x) = x^4+x+1$

$f(g) = g^4+g+1 = 0 \Rightarrow \underline{g^4 = g+1}$

$N = 2^n - 2 = 2^4 - 2 = 14$

$\{0, g^0, g^1, g^2, \dots, g^N\}$

$0 \rightarrow \underline{0000}$

$g^0 \rightarrow \underline{0001}$

$g^1 \rightarrow \underline{0010}$

$g^2 \rightarrow \underline{0100}$

$g^3 \rightarrow \underline{1000}$

$g^4 \rightarrow g+1 \rightarrow \underline{0011}$

$g^5 \rightarrow g(g^4) \rightarrow g(g+1) \rightarrow g^2+g \rightarrow \underline{0110}$

$g^6 \rightarrow g(g^5) \rightarrow g(g^2+g) \rightarrow g^3+g^2 \rightarrow \underline{1100}$

$g^7 \rightarrow g(g^6) \rightarrow g(g^3+g^2) \rightarrow g^4+g^3 \rightarrow g^3+g+1$

$= \underline{1011}$

$g^8 \rightarrow g(g^7) \rightarrow g(g^3+g+1) \rightarrow g^4+g^2+g \rightarrow g+1+g^2+g$

$\rightarrow g^2+1 = \underline{0101}$

$g^9 \rightarrow g(g^8) \rightarrow g(g^2+1) \rightarrow g^3+g = \underline{1010}$

$g^{10} \rightarrow g(g^9) \rightarrow g(g^3+g) \rightarrow g^4+g^2 \rightarrow g^2+g+1 = \underline{0111}$

$g^{11} \rightarrow g(g^{10}) \rightarrow g(g^2+g+1) \rightarrow g^3+g^2+g = \underline{1110}$

$g^{12} \rightarrow g(g^{11}) \rightarrow g(g^3+g^2+g) = g^4+g^3+g^2$

$= g^3+g^2+g+1 = \underline{1111}$

$g^{13} \rightarrow g(g^{12}) \rightarrow g(g^3+g^2+g+1) = g^4+g^3+g^2+g$

$= g^3+g^2+1 = \underline{1101}$

$g^{14} \rightarrow g(g^{13}) \rightarrow g(g^3+g^2+1) = g^4+g^3+g$

$= g^3+1 = \underline{1001}$

\# $g^9 \times g^{11} = g^{20} = g^{20 \bmod 15} = g^5 = g(g^4)$ [8. no. 14]

$= g(g+1) = g^2+g = \underline{0110}$

\# $g^3 / g^8 = g^{(3-8)} = g^{-5} = g^{-5 \bmod 15} = g^{10}$

$= g^2+g+1 = \underline{0111}$

Note:- the exponents are calculated modulo 2^n-1, $2^4-1 = 15$ in this case.

19BCS031 Shahabuddin

(9)

The order of the group is ~~$\phi(n)$~~

$$\phi(19) = 18$$

the order of each element

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

The number of primitive roots are

$$\phi(\phi(19)) = \phi(\phi(19)) = \phi(18) = 6$$

The primitive roots are those element with order 18. They are 2, 3, 10, 13, 14 & 15

(10)

$$2x^{11} \equiv 22 \mod 19$$

or

$$2x^{11} \equiv 3 \mod 19$$

Apply the function L_2 to both sides of the congruence. Note that working modulus is $\phi(19) = 18$.

$$L_2(2x^{11}) \equiv L_2(3) \pmod{18}$$

$$L_2(2) + 11 \times L_2(x) \equiv L_2(3) \pmod{18}$$

$$1 + 11 \times L_2(x) \equiv 13 \pmod{18}$$

$$11 \times L_2(x) \equiv 12 \mod 18$$

$$L_2(x) \equiv (11^{-1} \times 12) \mod 18$$

$$L_2(x) = (5 \times 12) \mod 18$$

$$L_2(x) \equiv 6 \mod 18$$

$\therefore$ $\boxed{x = 7}$

19BCS031 Shahabuddin

(11) Quadratic Congruence modulo prime (P):

$$x^2 \equiv a \pmod p$$

If p is in the form of $4k+3$ and a is QR in Z_p^*, then

$$x \equiv a^{(p+1)/4} \pmod p$$

$$x \equiv -a^{(p+1)/4} \pmod p$$

How to check a is QR in Z_p^* ?

→ If $a^{(p-1)/2} \equiv 1 \pmod p$; a is QR (Quadratic Residue)

→ If $a^{(p-1)/2} \equiv -1 \pmod p$; a is ~~NQR~~ QNR (Quadratic non-Residue)

i) $x^2 \equiv 3 \pmod{23}$

Here, $p = 23 = 20 + 3 = 4 \times 5 + 3$ ($4k+3$, form)

$$a^{(p-1)/2} \pmod p = 3^{(23-1)/2} \pmod{23}$$

$$= (3^{11}) \bmod 23$$

$$= (3^3 \times 3^3 \times 3^3 \times 3^2) \bmod 23$$

$$= (4 \times 4 \times 4 \times 9) \bmod 23$$

$$= (4 \times 4 \times 13) \bmod 23$$

$$= 24 \bmod 23$$

$$= 1$$

Thus, 3 is QR in Z_{23}^*.

$x \equiv \pm a^{(p+1)/4} \pmod p \equiv \pm 3^{(23+1)/4} \pmod{23}$

$\equiv \pm 3^6 \pmod{23} \equiv \pm (3^3 \times 3^3) \bmod 23$

$\equiv \pm 16 \bmod 23$

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

Here, $p = 19 = 16 + 3 = 4\times4+3$ [4K+3 form]

$a^{(p-1)/2} \pmod p = 7^{(19-1)/2} \pmod{19}$

$= 7^9 \pmod{19}$

$= (7^2 \times 7^2 \times 7^2 \times 7^2 \times 7) \bmod 19$

$= (11 \times 11 \times 11 \times 11 \times 7) \bmod 19$

$= (7 \times 7 \times 7) \bmod 19$

$= (11 \times 7) \bmod 19$

$= 1$

Thus, 7 is QR in Z^*_{19}.

$x \equiv \pm a^{(p+1)/4} \pmod p$

$\equiv \pm 7^{(19+1)/4} \pmod{19}$

$\equiv \pm (7^5) \bmod 19$

$\equiv \pm (7^2 \times 7^2 \times 7) \bmod 19$

$\equiv \pm (11 \times 11 \times 7) \bmod 19$

$\equiv \pm 11 \bmod 19$

19BCS031 Shahabuddin

(12) (i) $(x^2)^{-1}$ modulo (x^3+x^2+1) = ?

$r = r_1 - q \times r_2$ | $t = t_1 - q \times t_2$

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

$$x^2(x+1) = x^3 + x^2$$
$$= x^2+1 + x^2$$
$$= 1$$

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

Thus, $(x^2)^{-1}$ modulo $(x^3+x^2+1) = x+1$

ii) $(x^2+1)^{-1}$ modulo $(x^3+x^2+1) = ?$

$t = t_1 - q \times t_2$

q	r_1	r_2	r	t_1	t_2	t
$(x+1)$	(x^3+x^2+1)	(x^2+1)	$(x+1)$	0	1	$(x+1)$
(x^2+1)	(x^2+1)	$(x+1)$	0	1	$(x+1)$	$(x^2$ [illegible]
	1 ↓ gcd	0		$(x+1)$	$(x^2$ [illegible]	

$$x+1$$
$$x^2+1 \;\overline{)\; x^3+x^2+1}$$
$$x^3+x \quad\quad x^2+1$$
$$x+1$$

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

$(x^2+1)^2 =$ [illegible] x^2+1+2x

$= x^2$ [illegible] $+1$

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

x^2+1+2x^0

Thus, $(x^2+1)^{-1}$ modulo $(x^3+x^2+1) = x$

iii) $(x^2+x)^{-1}$ modulo $(x^3+x^2+1) = ?$

q	r_1	r_2	r	t_1	t_2	t
x	(x^3+x^2+1)	(x^2+x)	1	0	1	x
(x^2+x)	(x^2+x)	1	0	1	x	0
	1	0		x	0	

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

$x(x^2+x) = x^3+x^2$

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

$= 1$

$\therefore (x^2+x)^{-1} \bmod (x^3+x^2+1) = x$

19BCS031 Shahabuddin

(13) Addition table for GF(2^3)

⊕	000 (0)	001 (1)	010 (x)	011 (x+1)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	001 (1)	010 (x)	011 (x+1)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
001 (1)	001 (1)	000 (0)	011 (x+1)	010 (x)	101 (x^2+1)	100 (x^2)	111 (x^2+x+1)	110 (x^2+x)
010 (x)	010 (x)	011 (x+1)	000 (0)	001 (1)	110 (x^2+x)	111 (x^2+x+1)	100 (x^2)	101 (x^2+1)
011 (x+1)	011 (x+1)	010 (x)	001 (1)	000 (0)	111 (x^2+x+1)	110 (x^2+x)	101 (x^2+1)	100 (x^2)
100 (x^2)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)	000 (0)	001 (1)	010 (x)	011 (x+1)
101 (x^2+1)	101 (x^2+1)	100 (x^2)	111 (x^2+x+1)	110 (x^2+x)	001 (1)	000 (0)	011 (x+1)	010 (x)
110 (x^2+x)	110 (x^2+x)	111 (x^2+x+1)	100 (x^2)	101 (x^2+1)	010 (x)	011 (x+1)	000 (0)	001 (1)
111 (x^2+x+1)	111 (x^2+x+1)	110 (x^2+x)	101 (x^2+1)	100 (x^2)	011 (x+1)	010 (x)	001 (1)	000 (0)

19BCS031 Shahabuddin

Multiplication table for GF (2^3) IP = x^3+x^2+1

⊗	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)	000 (0)
001 (1)	000 (0)	001 (1)	010 (x)	011 ($x+1$)	100 (x^2)	101 (x^2+1)	110 (x^2+x)	111 (x^2+x+1)
010 (x)	000 (0)	010 (x)	100 (x^2)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	011 ($x+1$)	001 (1)
011 ($x+1$)	000 (0)	011 ($x+1$)	110 (x^2+x)	101 (x^2+1)	111 (x^2+x+1)	100 (x^2)	001 (1)	010 (x)
100 (x^2)	000 (0)	100 (x^2)	101 (x^2+1)	111 (x^2+x+1)	110 (x^2+x)	010 (x)	001 (1)	011 ($x+1$)
101 (x^2+1)	000 (0)	101 (x^2+1)	111 (x^2+x+1)	100 (x^2)	010 (x)	011 ($x+1$)	001 (1)	110 (x^2+x)
110 (x^2+x)	000 (0)	110 (x^2+x)	001 (1)	010 (x)	011 ($x+1$)	111 (x^2+x+1)	101 (x^2+1)	100 (x^2)
111 (x^2+x+1)	000 (0)	111 (x^2+x+1)	011 ($x+1$)	001 (1)	110 (x^2+x)	100 (x^2)	010 (x)	101 (x^2+1)

19BCS031 Shahabuddin

(14) IP = $f(x) = x^4 + x + 1$

$f(g) = g^4 + g + 1 = 0$

$\Rightarrow g^4 = g + 1$

$g^{20} = g^{20 \bmod 15} = g^5 = g(g^4)$

$= g(g+1)$

$= g^2 + g$

$= 0110$

19BCS031 Shahabuddin

(15) Quadratic Congruence Modulo a Composite.

$$x^2 \equiv a \pmod{n}$$

$$n = p_1 \times p_2 \times \cdots \times p_k$$

$$x^2 \equiv a \pmod{p_1}$$
$$x^2 \equiv a \pmod{p_2}$$
$$\vdots$$
$$x^2 \equiv a \pmod{p_k}$$

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

Here, $n = 77 = 11 \times 7 = p_1 \times p_2$

$x^2 \equiv 36 \bmod 11$ —— (i)

$x^2 \equiv 36 \bmod 7$ —— (ii)

On solving (i)

$x^2 \equiv 36 \bmod 11 \equiv 3 \bmod 11$

$x = \pm 3^{(p_1+1)/4} \pmod{11}$

$= \pm 3^{(11+1)/4} \pmod{11}$

$= \pm 27 \bmod 11$

$= \pm 5 \bmod 11$

On solving (ii)

$x^2 \equiv 36 \bmod 7 \equiv 1 \bmod 7$

$x = \pm (1)^{(p_2+1)/4} \pmod{7}$

$= \pm 1 \bmod 7$

Set 1: $x \equiv +5 \bmod 11$ | $x \equiv 1 \bmod 7$

$\rightarrow M = m_1 \times m_2 = 11 \times 7 = \underline{77}$

$\rightarrow M_1 = \frac{M}{m_1} = \frac{77}{11} = \underline{7}$

$M_2 = \frac{M}{m_2} = \frac{77}{7} = \underline{11}$

$\rightarrow M_1^{-1} \bmod m_1 = 7^{-1} \bmod 11 = \underline{8}$

$M_2^{-1} \bmod m_2 = 11^{-1} \bmod 7 = \underline{2}$

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

$= 302 \bmod 77 = 71 \bmod 77$

$= -6 \bmod 77 = \underline{-6}$

Set2: $x \equiv +5 \bmod 11$ | $x \equiv -1 \bmod 7 \equiv 6 \bmod 7$

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

$= 27 \bmod 77 = \underline{27}$

Set 3: $x \equiv -5 \bmod 11$ $\equiv 6 \bmod 11$ | $x \equiv 1 \bmod 7$

$x = (6 \times 7 \times 8 + 1 \times 11 \times 2) \bmod 77 = 50 \bmod 77$

$= -27 \bmod 77 = \underline{-27}$

Set4: $x \equiv 6 \bmod 11$ | $x \equiv -1 \bmod 7 \equiv 6 \bmod 7$

$x = (6 \times 7 \times 8 + 6 \times 11 \times 2) \bmod 77 = 468 \bmod 77 = \underline{6}$

Thus, the answer is ± 6 & ± 27.