Nicole Robles

CYEN 489 – 001

Homework - Elliptic Curve Addition

6.5

(c) E: $y^2 = x^3 + 4x + 5$ over F(11)

Discriminant: $4A^3 + 27B^2 = 4(4)^3 + 27 * (5)^2 \equiv 7(mod\ 11)$

x	y^2	y
0	5	4,7
1	10	N/A
2	10	N/A
3	0	0
4	8	N/A
5	7	N/A
6	3	5,6
7	2	N/A
8	10	N/A
9	0	0
10	0	0

The y's:

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 9$

$4^2 \equiv 5$

$5^2 \equiv 3$

$6^2 \equiv 3$

$7^2 \equiv 5$

$8^2 \equiv 9$

$9^2 \equiv 4$

Points: {O, (0,4), (0,7), (3,0), (6,5), (6,6), (9,0), (10,0)}

(d) E: $y^2 = x^3 + 9x + 5$ over F(11)

Discriminant: $4A^3 + 27B^2 = 4(9)^3 + 27 * (5)^2 \equiv 5(mod\ 11)$

x	y^2	y
0	5	4,7
1	4	2,9
2	9	3,8
3	4	2,9
4	6	N/A
5	10	N/A
6	0	0
7	4	2,9
8	6	N/A
9	1	1,10
10	6	N/A

The y's:

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 9$

$4^2 \equiv 5$

$5^2 \equiv 3$

$6^2 \equiv 3$

$7^2 \equiv 5$

$8^2 \equiv 9$

$9^2 \equiv 4$

Points: {O, (0,4), (0,7), (1,2), (1,9), (2,3), (2,8), (3,2), (3,9), (6,0), (7,2), (7,9), (9,1), (9,10)}

(e) E: $y^2 = x^3 + 9x + 5$ over F(13)

Discriminant: $4A^3 + 27B^2 = 4(9)^3 + 27 * (5)^2 \equiv 3(mod\ 13)$

x	y^2	y
0	5	N/A
1	2	N/A
2	5	N/A
3	7	N/A
4	1	1,12
5	6	N/A
6	2	N/A
7	8	N/A
8	4	2,11
9	9	3,10
10	3	4,9
11	5	N/A
12	8	N/A

The y's:

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 9$

$4^2 \equiv 3$

$5^2 \equiv 12$

$6^2 \equiv 10$

$7^2 \equiv 10$

$8^2 \equiv 12$

$9^2 \equiv 3$

$10^2 \equiv 9$

$11^2 \equiv 4$

$12^2 \equiv 1$

Points: {O, (4,1), (4,12), (8,2), (8,11), (9,3), (9,10), (10,4), (10,9)}

6.6

(a) E: $y^2 = x^3 + 1x + 2$ over F(5)

Discriminant: $4A^3 + 27B^2 = 4(1)^3 + 27 * (2)^2 \equiv 2(mod\ 5)$

x	y^2	y
0	2	N/A
1	4	2,3
2	2	N/A
3	2	N/A
4	0	0

The y's:

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 4$

$4^2 \equiv 1$

Points: {O, (1,2), (1,3), (4,0)}

+	O	(1,2)	(1,3)	(4,0)
O	O	(1,2)	(1,3)	(4,0)
(1,2)	(1,2)	(4,0)	O	(1,3)
(1,3)	(1,3)	O	(4,0)	(1,2)
(4,0)	(4,0)	(1,3)	(1,2)	O

(b) E: $y^2 = x^3 + 2x + 3$ over F(7)

Discriminant: $4A^3 + 27B^2 = 4(2)^3 + 27 * (3)^2 \equiv 2(mod\ 7)$

x	y^2	y
0	3	N/A
1	6	N/A
2	1	1,6
3	1	1,6
4	5	N/A
5	5	N/A
6	0	0

The y's:

$0^2 \equiv 0$

$1^2 \equiv 1$

$2^2 \equiv 4$

$3^2 \equiv 2$

$4^2 \equiv 2$

$5^2 \equiv 4$

$6^2 \equiv 1$

Points: {O, (2,1), (2,6), (3,1), (3,6), (6,0)}

+	O	(2,1)	(2,6)	(3,1)	(3,6)	(6,0)
O	O	(2,1)	(2,6)	(3,1)	(3,6)	(6,0)
(2,1)	(2,1)	(3,6)	O	(2,6)	(6,0)	(3,1)
(2,6)	(2,6)	O	(3,1)	(6,0)	(2,1)	(3,6)
(3,1)	(3,1)	(2,6)	(6,0)	(3,6)	O	(2,1)
(3,6)	(3,6)	(6,0)	(2,1)	O	(3,1)	(2,6)
(6,0)	(6,0)	(3,1)	(3,6)	(2,1)	(2,6)	O