Homework Assignment 05

Machiry Aravind Kumar

UCSB

1 Problem 1

Let the elliptic curve equation $y^2 = x^3 - 3x + 4$ defined over the finite field GF(29) be given.

1.1 Apply Hasses theorem and find the range of the order of the elliptic curve group

According to Hasse Theorem, we have $p + 1 - 2\sqrt{p} \leq order \leq p + 1 + 2\sqrt{p}$.
Given P = 29, $\lceil 29 \rceil = 6$. $p + 1 - 2\sqrt{p} = 18$ and $p + 1 + 2\sqrt{p} = 42$.
Range of the elliptic curve group is: $18 \leq order \leq 42$.

1.2 Compute all elements of the elliptic curve group by enumeration.

x	$x^3 - 3x + 4$	y	Points
0	4	±2	(0,2), (0,27)
1	2	-	-
2	6	±8	(2,8), (2,21)
3	22	±14	(3,14), (3,15)
4	27	-	-
5	27	-	-
6	28	±12	(6,12), (6,17)
7	7	±6	(7,6), (7,23)
8	28	±12	(8,12), (8,17)
9	10	-	-
10	17	-	-
11	26	-	-
12	14	-	-
13	16	±4	(13,4), (13,25)
14	9	±3	(14,3), (14,26)
15	28	±12	(15,12), (15,17)
16	21	-	-
17	23	±9	(17,9), (17,20)
18	11	-	-
19	20	±7	(19,7), (19,22)
20	27	-	-
21	9	±3	(21,3), (21,26)
22	1	±1	(22,1), (22,28)
23	9	±3	(23,3), (23,26)
24	10	-	-
25	10	-	-
26	15	-	-
27	2	-	-
28	6	±8	(28,8), (28,21)

1.3 Find the exact order of the group.

Order of the EC group is the number of points on the curve plus one to include point at infinity. From the table above, number of points is equal to 30, thus order of group is **31**.

1.4 Find a primitive element of the group. Call that P.

Since the order of the group is prime, all points except for point at infinity is primitive element. Taking one point: (7, 6). Lets assign: $P = (7, 6)$.

1.5 Compute [15]P using the binary method

We have $P = (7, 6)$.
e = 15 = (1111)

i	e_i	Step 2a	Step 2b
2	1	(7, 6) + (7, 6) = (14,26)	(14,26) + (7,6) = (28,21)
1	1	(28, 21) + (28, 21) = (2,8)	(2,8) + (7,6) = (19,22)
0	1	(19,22) + (19,22) = (13,4)	(13,4) + (7,6) = **(22,28)**

1.6 Compute [15]P using the canonical recoding binary method

We have $P = (7, 6)$. $-P = (7, -6) = (7, 23)$
Canonical recording for $15 = \mathrm{f} = (1000\overline{1})$

i	f_i	Step 2a	Step 2b
3	0	(7, 6) + (7, 6) = (14,26)	(14,26)
2	0	(14, 26) + (14, 26) = (17,20)	(17,20)
1	0	(17, 20) + (17, 20) = (8,12)	(8,12)
0	$\overline{1}$	(8,12) + (8,12) = (22,1)	(22,1) + (7,23) = **(22,28)**