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