Discrete Structures

IIIT Hyderabad

Monsoon 2020

Tutorial 6

October 5, 2020

Introduction

This Tutorial

- Solving till 1:30PM. After that 2 separate meets.
- After that, doubts till now, about any topic covered.
- Please join the meets as per roll number -
  1. Roll Number 2020909122-37 : Vikrant
  2. Roll Number 2020909138-54 : Jai

Question 1

Consider elliptic curve $E_5(2,1)$ or in equation form as -

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

1.1:: Find all points in the curve.

Sol: Use the following algorithm -

Elliptic curves over modulo a prime $GF(p)$

Finding all points on an elliptic curve
Algorithm: EllipticCurvePoints (p, a, b)

1: $x \leftarrow 0$
2: **while** $x < p$ **do**
3: $w \leftarrow (x^3 + ax + b) \pmod p$
4: **if** w is a perfect square in Z_p) **then**
5: Output $(x, \sqrt{w}), (x, -\sqrt{w})$
6: **end if**
7: $x \leftarrow x + 1$
8: **end while**

1. x = 0, w = 1, output (0,1) and (0,-1)or (0,4).
2. x = 1, w = 4, output (1,2) and (1,-2) or (1,3).
3. x = 2, w = 13 = 3, not perfect square.
4. x = 3, w = 34 = 4, output (3,3) and (3,-3) or (3,2).
5. x = 4, w = 3, not perfect square.

Thus we get (0,1),(0,4),(1,2),(1,3),(3,3) and (3,1).

1.2: If $P = (1, 3)$ and $Q = (3, 2)$ lie on the above curve, find -

1. -P

   Sol: It would be (1,-3) or (1,2). As $3 + 2 = 5$.

2. P + Q

Sol: We need to compute $R = P + Q$.

$$\lambda = \frac{2-3}{3-1} = \frac{-1}{2}$$
$$= \frac{4}{2} = 2$$
$$x_R = 4 - x_P - x_Q$$
$$= 0$$
$$y_R = 2(x_P - x_R) - y_P$$
$$= -1 = 4$$

Thus we get (0,4).

3. 2Q

$$\lambda = \frac{3 \cdot 9 + 2}{4}$$
$$= 1$$
$$x_R = 1 - x_Q - x_Q$$
$$= -5 = 0$$
$$y_R = 1(x_Q - x_R) - y_Q$$
$$= 1$$

Thus we get (0,1).