Shweta Prasad April 11, 2021

CS 2362 Problem Set 3

Collaborators: *None*

Problem 4-1

The main difference between the two groups is that they are defined for very different operations: the elliptic curve group is defined for the 'addition' operation. $\mathbb{Z}^*_p$ is called a multiplicative group, and as the name suggests, the group operation is modular multiplication (modulo the number p), which for our purposes are usually prime. Another difference is the size of the groups: the elliptic curve group is smaller than the multiplicative group. Also, the elements themselves are different.

The similarities between the two groups is that they are groups over finite fields and that the are both Abelian groups (commutative w.r.t respective operation).

Problem 4-2

Given: two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Assumption, P and Q are both points on the elliptic curve.

- To add P and Q, we do the following: Graphically, we first draw a line through the two points and find the third point at which the line intersects the elliptic curve (a line intersects the EC at at-most 3 points). We then take its reflection on the $x-$axis and the obtained point on the EC is the required point $R = (x_3, y_3)$. Let the EC be given by the equation

$$y^2 = x^3 + ax + b$$

Analytically, we find R using the following equations.

$$x_3 = s^2 - x_1 - x_2 \mod p$$

$$y_3 = s(x_1 - x_3) - y_1 \mod p$$

where the slope

$$s = \begin{cases} \frac{3x_1^2+a}{2y_1} \mod p, & \text{if } P = Q \text{ (point doubling)} \\ \frac{y_2-y_1}{x_2-x_1} \mod p, & \text{if } P \neq Q \text{ (point addition)} \end{cases}$$

- The above sets of equations also covers point doubling.
- Let $\mathcal{O}$ be the point at infinity. We need a point M such that

$$P + M = \mathcal{O}$$

Since the points on the elliptic curve form a group, we know that a unique identity and an inverse for every point in the group, exist. Let the point at infinity $\mathcal{O}$ be the unique identity for this EC. Thus, $M = -P$ (the inverse element w.r.t this group operation) $\forall$ P belonging to the EC.

Therefore, when a point and its inverse are added, it results in the point at infinity.

Problem 4-3

Given parameters: $p = 11, a = 3, b = 3$. Thus the given elliptic curve is

$$y^2 = x^3 + 3x + 3 \mod 11$$

A point on the EC was obtained using the program `ecpoints.py`, such that its $y-$coordinate is not 0 (else s as shown above in Problem $4-2$ cannot be found as 0 has no modular inverse). If there are points such that the $y-$coordinate is non-zero, program outputs two lists of points on the EC, so that once the sum of points is obtained, the existence of that point on the EC can also be cross checked.
From the list, I pick $P = (7, 2)$ to double. Using the formulae given in the previous question, we get

$$\begin{aligned}
s &= 3 \times 49 + 3 \mod 11 \cdot (2 \times 2)^{-1} \mod 11 \\
&= 7 \mod 11 \cdot 3 \mod 11 \\
&= 21 \mod 11 \\
&\equiv 10 \\
x_3 &= 10^2 - 2 \times 7 \mod 11 \\
&\equiv 9 \\
y_3 &= (10 \times (7 - 9) - 2) \mod 11 \\
&= (-22) \mod 11 \\
&\equiv 0
\end{aligned}$$

Thus, $(x_3, y_3) = (9, 0)$, which is a point on the EC. This is the required doubled point.

Problem 4-4

Have submitted code just for fun. It's not what you want. Submitted it just cause I did as much.