Homework 6

Number Theory and Cryptography (201912400327)

Due Date: June 20, 2024

Question 1.

Draw the elliptic curve $y^2 = x^3 + 1$ and illustrate the addition and doubling of points on the graph, by adding $P = (0, 1)$ and $Q = (2, 3)$, and also $Q + Q = 2Q$.

Question 2.

Let E be the elliptic curve $y^2 = x^3 + 1$ defined over $\mathbb{F}_{11}$.

- Find all points on $E(\mathbb{F}_{11})$.
- Let $P = (5, 4)$. Show that P is on E, and compute $2P$ using the doubling formulas on E.
- Let $P = (5, 4)$ and $Q = (7, 5)$. Compute $P + Q$ using the addition formulas on E.

Question 3.

Check if $y^2 = x^3 + 3x + 8$ is an elliptic curve over the following fields. If so, find all the points on the curve.

- $\mathbb{Q}$
- $\mathbb{F}_3$
- $\mathbb{F}_{13}$

Question 4.

Let $E: \ y^2 = x^3 + 3x + 8$ be an elliptic curve over $\mathbb{F}_{13}$ and $P = (2, 3)$ be a point on the curve. Please calculate $9P$.