UNIVERSITY OF NORTH CAROLINA
CHARLOTTE
COLLEGE OF COMPUTING
AND INFORMATICS
COMPUTER SCIENCE

Some Elliptic Curve Point Exercises

Exercise 1

Recall the that we denote the set of points (x, y) located on the elliptic curve $y^2 = x^3 + ax + b$ as $S_{a,b}$, i.e., $S_{a,b} = \{(x, y) : y^2 = x^3 + ax + b\}$. For the purpose of this exercise, we consider the elliptic curves over the real numbers, i.e., $S_{a,b} \subset \mathbb{R} \times \mathbb{R}$, where $\mathbb{R}$ denotes the set of real numbers.

Which of the following points are on the curve $S_{5,7}$?

a) $(2, 4)$

b) $(1, 1)$

c) $(18, 77)$

d) $(4, 6)$

Exercise 2

Consider now the elliptic curve $S_{5,7} \subset F_{11} \times F_{11}$ from Exercise 1 taken considered over the finite field $F_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

For the points a)-d) of Exercise 1, which points are on the curve $S_{5,7} \subset F_{11} \times F_{11}$?
(E.g., $(x, y) = (18, 77)$ coincides with $(18 \ \% \ 11, 77 \ \% \ 11)$ in this case)

Can you answer the question for some of these points without any additional calculations?

Exercise 3

Consider the elliptic curve $S_{5,7}$ over the real numbers ($S_{a,b} \subset \mathbb{R} \times \mathbb{R}$).

a) If $B = (0, y_2) \in S_{5,7}$, what is y_2? Is y_2 unique?

b) If $A = (-1, 1) \in S_{5,7}$, compute $A + B$ with B from part (a).