Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 9

Friday, January 12, 2018

Problem 1. *(working with elliptic curves II)* Consider the following function in the field $\mathbb{F}_7$

$$E_{a,b} : y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{F}_7$.

a) Determine the parameters a, b for which $P_1 = (1, 1)$ and $P_2 = (6, 2)$ are points on the curve. Do these parameters describe an elliptic curve in the field $\mathbb{F}_7$? Give a reason.

Consider the curve $E_{6,1}$ for the remainder of this exercise.

b) Show that $E_{6,1}$ is an elliptic curve in the field $\mathbb{F}_7$. Determine all points P and their inverses $-P$ in the $\mathbb{F}_7$-rational group.

c) What are possible group orders for any group which is generated by an arbitrary point P of the curve?

d) Show that $Q = (1, 1)$ is a generator of $E_{6,1}(\mathbb{F}_7)$. You know that $4 \cdot (1, 1) = (3, 2)$.

Problem 2. *(elliptic curve double-and-add)* Consider the cubic equation $E : y^2 = x^3 + 4x + 1$.

a) Is E an elliptic curve over $\mathbb{F}_5$? Substantiate your answer.

b) Determine all points on the elliptic curve E and the order of the corresponding group.

c) Is point $Q = (1, 1)$ a generator of the group? Substantiate your answer.

In analogy to the *Square-and-Multiply* algorithm in a ring $\mathbb{Z}_n$, the k-th multiple of P can be algorithmically computed based on doubling and addition on an elliptic curve over a field $\mathbb{F}_q$. You may use the binary representation of factor $k = (k_m, \ldots, k_0)_2 = \sum_{i=0}^{m} k_i \, 2^i$.

d) Describe $45P$ in terms of doubling and addition of P only.

e) Formulate an *iterative Double-and-Add* algorithm $f_{\mathrm{it}}(P, k)$ to calculate $k\,P$.

f) Give a *recursive* version $f_{\mathrm{rec}}(P, k)$ of the above *Double-and-Add* algorithm.