Topics in Algebra: Cryptography - Blatt 3

http://www.mat.univie.ac.at/~gagt/crypto2019

Goulnara Arzhantseva
goulnara.arzhantseva@univie.ac.at

Martin Finn-Sell
martin.finn-sell@univie.ac.at

1 Test questions from the lecture to refresh:

Question 1. Give a proof of Theorem 2 from the Annex notes for Chapter 2.

2 Exercises

Throughout these exercises, let $\mathbb{F}_p$ be the field with p elements, where p is prime and $E := E(\mathbb{F}_p)$ be the set of $\mathbb{F}_p$-points of an elliptic curve defined over $\mathbb{F}_p$.

Question 2. Suppose that $p > 3$ is an odd prime, and $a, b \in \mathbb{F}_p$. Further, suppose that the equation $x^3+ax+b = 0 \mod p$ has three distinct solutions in $\mathbb{F}_p$. Prove that the corresponding elliptic curve group $(E, +)$ is not a cyclic group. (Hint: Consider the subgroup of elements of order 2.)

Question 3. Using Hasse's bound, show that the only finite fields $\mathbf{k}$ over which there is an elliptic curve without $\mathbf{k}$-rational points are $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_4$.

Question 4. Let $p > 3$ is prime. Suppose also that $|E|$ is a prime, $P \in E$ and $P \neq \mathcal{O}$, where $\mathcal{O}$ is the point at infinity.

i) Prove that the discrete logarithm $\log_P(-P) = |E| - 1$;

ii) Describe how to compute $|E|$ in $O(p^{\frac{1}{4}})$ time using Hasse's bound on $|E|$ together with a modification of Shank's algorithm.

Question 5. (Finite Fields and their extensions)

1. Show that for an irreducible polynomial f over $\mathbb{F}_p$ that the finite field extension $\mathbf{k}$ generated by $\mathbb{F}_p$ and the roots of f is isomorphic to $\mathbb{F}_p^n$ for some $n > 0$.

2. Compute the algebraic closure of $\mathbb{F}_p$.

Question 6. We consider the following two models for the projective plane $\mathbb{R}P^2$. Here $\mathbb{R}^3$ is given by (x, y, z)-coordinates.
Model 1: the sphere S^2 in $\mathbb{R}^3$ with antipodal points identified.
Model 2: the plane $P = \{(x, y, z) \mid z = 1\}$ in $\mathbb{R}^3$.

1. Describe why (or prove how) these models are equivalent (Perhaps a sketch would help).
2. What are lines in the second model of $\mathbb{R}P^2$?
3. What do these lines look like as lines on the sphere?