# Homework 13 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Georg Böcherer, Henning Maier

25.01.2011

**Exercise 41.** Consider the following equation:

$$Y^2 = X^3 + X + 1.$$

(a) Show that this equation describes an elliptic curve $E$ over the field $\mathbb{F}_7$.

(b) Determine all points in $E(\mathbb{F}_7)$ and compute the trace $t$ of $E$.

(c) Draw a plot of the elliptic curve $E$ over $\mathbb{F}_7$.

(d) Show that $E(\mathbb{F}_7)$ is cyclic and give a generator.

**Exercise 42.** Consider the following parameterized equation:

$$E_a : Y^2 = X^3 + aX + (a + 1).$$

(a) For which values of $a$ does $E_a$ describe an elliptic curve over $\mathbb{F}_{11}$?

(b) How many points are in $E_4(\mathbb{F}_{11})$? Determine all points and draw a plot.

(c) Find the inverse to each point $P \in E_4(\mathbb{F}_{11})$.