Homework 12 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

24.01.2012

Exercise 34. Consider the 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) Show that $E(\mathbb{F}_7)$ is cyclic and give a generator.

Exercise 35.

Let $E : Y^2 = X^3 + aX + b$ be a curve over the field K with $\mathrm{char}(K) \neq 2, 3$ and let $f := Y^2 - X^3 - aX - b$.
A point $P = (x, y) \in E$ is called *singular*, if both formal partial derivatives $\partial f/\partial X(x, y)$ and $\partial f/\partial Y(x, y)$ vanish at P.

(a) Prove that for the discriminant Δ of E it holds that

$$\Delta \neq 0 \Leftrightarrow E \text{ has no singular points.}$$