Homework 8 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

28.06.2007

Exercise 22.
Consider the equation

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

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

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

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

Exercise 23.
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.
Prove that for the discriminant Δ of E it holds that

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

Exercise 24.
Given a prime p and an elliptic curve $E : Y^2 = X^3 + aX + b$ over the finite field $\mathbb{F}_p$, consider the map

$$\phi : E \to \overline{\mathbb{F}_p} \times \overline{\mathbb{F}_p}, \quad (x, y) \mapsto (x^p, y^p).$$

Show that $\phi(x, y) \in E$ for all $(x, y) \in E$. Furthermore prove that ϕ is a group homomorphism, i.e., that $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$. The map $\phi : E \to E$ is called *Frobenius endomorphism on* E.