Homework 12 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
24.01.2012

Solution to Exercise 35.

Given is an elliptic curve $E : Y^2 = X^3 + aX + b$ over a field K with $\operatorname{char} K \neq 2, 3$ (The field is $K = \mathbb{F}_{p^m}$, p is a prime number with $p > 3$ and $m \in \mathbb{N}$). The elliptic curve can be rewritten as a function of X and Y as

$$f(X, Y) = Y^2 - X^3 - aX - b$$

with the discriminant $\Delta = -16(4a^3 + 27b^2)$. For the derivatives of f in X and Y it holds

$$\frac{\delta f}{\delta X} = -3X^2 - a = 0 \Leftrightarrow a = -3X^2 \text{ and} \tag{1}$$

$$\frac{\delta f}{\delta Y} = 2Y = 0 \overset{\operatorname{char} K \neq 2}{\Leftrightarrow} Y = 0. \tag{2}$$

Note that (1) is equivalent to $a \equiv 0$ indepedent of X, if $\operatorname{char} K = 3$.

The definiton for a *singular point* of f is given as

$$P = (x, y) \in E(K) \text{ singular } \Leftrightarrow \left.\frac{\delta f}{\delta X}\right|_P = 0 \wedge \left.\frac{\delta f}{\delta Y}\right|_P = 0. \tag{3}$$

Claim: $\Delta \neq 0 \Leftrightarrow E(K)$ has no singular points.

Proof:
„$\Rightarrow$“ Let $\Delta \neq 0$
Assumption: There exists a singular point $(x, y) \in E(K)$. Then we get

$$\begin{aligned}
& y^2 &&= x^3 + ax + b \\
\overset{(1),(2)}{\Leftrightarrow}\quad & b &&= 2x^3, \qquad\qquad (4)\\
\Rightarrow\quad & \Delta &&= -16(4a^3 + 27b^2) \\
\overset{(1),(4)}{\Leftrightarrow}\quad & &&= -16(4(-3x^2)^3 + 27(2x^3)^2) \\
& &&= -16(4(-27)x^6 + 27(4x^6)) \\
& &&= 0.
\end{aligned}$$

This is a contradiction to the assumption. Hence $E(K)$ has no singular points.

„$\Leftarrow$“ $E(K)$ has no singular points

Assumption: With $\Delta = 0$ it follows $4a^3 + 27b^2 = 0$, as $\operatorname{char} K \neq 2$.

With Cardano's method of solving cubic functions of the form $X^3 + aX + b = 0$ there is a multiple zero x (of degree 2 or 3).

Hence it follows

$$f(x,0) = 0,$$
$$\left.\frac{\delta f}{\delta Y}\right|_{(x,0)} = 2 \cdot 0 = 0 \text{ and}$$
$$\frac{\delta f}{\delta X} = 0 \text{ as x is a multiple zero.}$$

From (3), $(x, 0)$ is a singularity. This is a contradiction to the assumption. Thus $\Delta \neq 0$. $\square$

Remarks: The special cases for char $K = 2, 3$ are

char $K = 2$: The discriminant is $\Delta = 0$ for any elliptic curve.

Find an elliptic curve, where no singular points exist, then the claim does not hold: From (1) it follows $a \equiv x^2$. Inserting this into (2) implies:

$$0 = y^2 = x^3 + ax + b \equiv x^3 + x^3 + b \equiv b \Rightarrow b = 0.$$

Choose $b = 1$ then no singular points exist, but $\Delta = 0$.

char $K = 3$: Then the discriminant is $\Delta = 2a^3$. If $a = 0$ is chosen, then $\Delta = 0$.

Find an elliptic curve, where no singular points exist, then the claim does not hold: From (1) and (2) it follows that $a = 0$ and $y = 0$ hold for a singular point. Choose the elliptic curve $E : Y^2 = X^3 + 1$, $y = 0 \Rightarrow y^2 = 0 \Rightarrow \exists x$ with $0 = x^3 + 1 \Rightarrow x^3 = 2$ which is not possible. Consequently, no singular points exist, but $\Delta = 0$.