Solution to **Exercise 33** of Homework 11

Given $E : Y^2 = X^3 + aX + b$ over a field K with $\operatorname{char} K \neq 2, 3$ ($K = \mathbb{F}_{p^m}, p$ prime, $p > 3$, $m \in \mathbb{N}$), $f(X, Y) = Y^2 - X^3 - aX - b$ and $\Delta = -16(4a^3 + 27b^2)$ it holds

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

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

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

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

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

Proof:
„⇒“ indirect proof
Assumption: There exists a singular point $(x, y) \in E(K)$.

$$y^2 = x^3 + ax + b \overset{(1),(2)}{\Leftrightarrow} 0 = -2x^3 + b \Leftrightarrow b = 2x^3 \tag{4}$$

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

Which is a contradiction to the assumption. It follows $E(K)$ has no singular points.

„⇐“ Indirect proof with assumption $\Delta = 0 \Rightarrow 4a^3 + 27b^2 = 0$.
It follows with Cardano's method of solving cubic functions of the form $X^3 + aX + b = 0$ that $X^3 + aX + b = 0$ has a multiple null x (of degree 2 or 3). Hence

$$\begin{aligned} f(x, 0) &= 0, \\ \frac{\delta f}{\delta Y}\ |_{(x,0)} &= 2 \cdot 0 = 0 \text{ and} \\ \frac{\delta f}{\delta X} &= 0 \text{ as x is a multiple null.}\end{aligned}$$

It follows by (3) that $(x, 0)$ is a singularity, which is a contradiction to the assumption. It follows $\Delta \neq 0$.

□