Exercise 11 in Advanced Methods of Cryptography - Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-01-23

Solution of Problem 35

a) In this case we consider a quadratic function ($n = 2$) and its derivative ($m = 1$):

$$f(x) = ax^2 + bx + c, \quad f'(x) = 2ax + b$$

Inserting this into the resultant yields:

$$\begin{aligned}\operatorname{Res}(f, f') &= \det \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} = a \cdot \det \begin{pmatrix} b & 0 \\ 2a & b \end{pmatrix} - 2a \cdot \det \begin{pmatrix} b & c \\ 2a & b \end{pmatrix} \\ &= ab^2 - 2a(b^2 - 2ac) = ab^2 - 2ab^2 + 4a^2c = -ab^2 + 4a^2c\end{aligned}$$

The discriminant of $f(x)$ yields:

$$\Delta = (-1)^{\binom{2}{2}} \cdot (-ab^2 + 4a^2c)a^{-1} = b^2 - 4ac$$

Remark: The *abc*-formula for solving quadratic equations is known as:

$$x_{1,2} = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}$$

The corresponding *pq*-formula is obtained for $a = 1$, $b = p$, $c = q$:

$$x_{1,2} = -\frac{p}{2} \pm \frac{\sqrt{p^2 - 4q}}{2} = -\frac{p}{2} \pm \sqrt{\frac{p^2 - 4q}{4}} = -\frac{p}{2} \pm \sqrt{(\tfrac{p}{2})^2 - q}$$

b) In this second case we consider a cubic function ($n = 3$) and its derivative ($m = 2$):

$$f(x) = x^3 + ax + b, \quad f'(x) = 3x^2 + a$$

Inserting this into the resultant yields:

$$\underbrace{\det \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix}}_{(III)} = \underbrace{1 \cdot \det \begin{pmatrix} 1 & 0 & a & b \\ 0 & a & 0 & 0 \\ 3 & 0 & a & 0 \\ 0 & 3 & 0 & a \end{pmatrix}}_{(I)} \underbrace{+3 \cdot \det \begin{pmatrix} 0 & a & b & 0 \\ 1 & 0 & a & b \\ 3 & 0 & a & 0 \\ 0 & 3 & 0 & a \end{pmatrix}}_{(II)}$$

The evaluation of the determinant (I) yields:

$$\begin{aligned}
&1 \cdot \det \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 3 & 0 & a \end{pmatrix} + 3 \cdot \det \begin{pmatrix} 0 & a & b \\ a & 0 & 0 \\ 3 & 0 & a \end{pmatrix} \\
&= a \cdot \det \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - 3a \cdot \det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \\
&= a^3 - 3a^3 = -2a^3
\end{aligned}$$

The evaluation of the determinant (II) yields:

$$\begin{aligned}
&(-3) \cdot \det \begin{pmatrix} a & b & 0 \\ 0 & a & 0 \\ 3 & 0 & a \end{pmatrix} + 3 \cdot 3 \cdot \det \begin{pmatrix} a & b & 0 \\ 0 & a & b \\ 3 & 0 & a \end{pmatrix} \\
&= (-3)a \cdot \det \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + 9a \cdot \det \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + 9 \cdot 3 \cdot \det \begin{pmatrix} b & 0 \\ a & b \end{pmatrix} \\
&= (-3)a^3 + 9a^3 + 27b^2 = 6a^3 + 27b^2
\end{aligned}$$

Combining (I) and (II) provides the determinant (III):

$$-2a^3 + 6a^3 + 27b^2 = 4a^3 + 27b^2$$

Altogether, the discriminant of $f(x)$ results in:

$$\Delta = (-1)^{\binom{3}{2}} \cdot (4a^3 + 27b^2) = -(4a^3 + 27b^2)$$

Solution of Problem 36

Given an elliptic curve (EC), $E : Y^2 = X^3 + aX + b$, over a field K with $\mathrm{char}(K) \neq 2, 3$ ($K = \mathbb{F}_{p^m}, p$ 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

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

$$\frac{\partial f}{\partial Y} = 2Y = 0 \overset{\mathrm{char}(K)\neq 2}{\Leftrightarrow} Y = 0. \tag{2}$$

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

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

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

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

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

$$\begin{aligned}
&y^2 = x^3 + ax + b \\
&\overset{(1),(2)}{\Leftrightarrow} 0 = x^3 + (-3x^2)x + b = -2x^3 + b \\
&\Leftrightarrow b = 2x^3 \qquad (4)
\end{aligned}$$

Inserting these values for y, a and b into the discriminant yields:

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

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

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

Assume $\Delta = 0$ it follows $4a^3 + 27b^2 = 0$, as $\mathrm{char}(K) \neq 2$.
It follows with Cardano's method of solving cubic functions of the form $X^3 + aX + b = 0$ that it has a multiple root x (of degree 2 or 3):

$$\begin{aligned}f(x,0) &= -x^3 - (-3x^2)x - 2x^3 = 0, \\ \frac{\partial f}{\partial Y} \,|_{(x,0)} &= 2 \cdot 0 = 0, \text{ and} \\ \frac{\partial f}{\partial X} \,|_{(x,0)} &= -3x^2 - (-3x^2) = 0, \text{ as } x \text{ is a multiple root.}\end{aligned}$$

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

As a result, $\Delta \neq 0$ is necessary (excluding $\mathrm{char}(K) = 2, 3$).