Exercise 11 in Advanced Methods of Cryptography

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

2015-01-23

Problem 35. (*elliptic curve discriminant*) Consider a polynomial in $x \in \mathbb{R}$ of degree n and its first derivative:

$$f(x) = f_n x^n + \cdots + f_1 x + f_0, \quad f'(x) = n f_n x^{n-1} + \cdots + f_2 x + f_1$$

The *discriminant* Δ is an invariant to evaluate the multiplicity of roots in a polynomial $f(x)$. It is computed by:

$$\Delta = (-1)^{\binom{n}{2}} \cdot \operatorname{Res}(f, f') \frac{1}{f_n}$$

The exponent $\binom{n}{2}$ denotes the binomial coefficient of n over 2. The *resultant* $\operatorname{Res}(f, g)$ is used to compute shared roots in the polynomial $f(x)$ of degree n and polynomial $g(x)$ of degree m. The resultant is defined as the determinant of the $(m+n) \times (m+n)$ *Sylvester matrix*:

$$\operatorname{Res}(f, g) = \det \begin{pmatrix} f_n & & \cdots & & f_0 & 0 & & 0 \\ 0 & f_n & & \cdots & & f_0 & & \\ & & \ddots & & & & \ddots & 0 \\ 0 & & 0 & f_n & & \cdots & & f_0 \\ g_m & & \cdots & & g_0 & 0 & & 0 \\ 0 & g_m & & \cdots & & g_0 & & \\ & & \ddots & & & & \ddots & 0 \\ 0 & & 0 & g_m & & \cdots & & g_0 \end{pmatrix}$$

a) Compute the discriminant Δ of the quadratic polynomial $f(x) = ax^2 + bx + c$.

b) Compute the discriminant Δ of the cubic polynomial $f(x) = x^3 + ax + b$.

Problem 36. (*singular points on elliptic curves*) Let $E : Y^2 = X^3 + aX + b$ be a curve over the field K with $\operatorname{char}(K) \neq 2, 3$ 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 for the discriminant Δ of the curve E that the following holds:

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