Exercise 36.
Consider a polynomial in $x \in \mathbb{R}$ of degree $n$ and its first derivative:

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

The discriminant $\Delta$ is an invariant to evaluate the number and multiplicity of roots in a polynomial $f(x)$. It is computed as following:

$$\Delta = (-1)^{(\frac{n}{2})} \text{Res}(f,f') \frac{1}{f_n}.$$

The resultant $\text{Res}(f,g)$ 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:

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

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

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

Exercise 37.
Describe how the DSA signature scheme can be carried out in a group of $\mathbb{F}_p$-rational points on an elliptic curve $E/\mathbb{F}_p$. 