Solution of Problem 1

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:

\[
\text{Res}(f, f') = \det \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} = a \cdot \det \begin{pmatrix} b & 0 \\ 2a & b \end{pmatrix} - 2a \cdot \det \begin{pmatrix} b & c \\ 2a & b \end{pmatrix}
\]

\[ = ab^2 - 2a(b^2 - 2ac) = ab^2 - 2ab^2 + 4a^2c = -ab^2 + 4a^2c \]

The discriminant of \(f(x)\) yields:

\[
\Delta = (-1)^{\frac{1}{2}} \cdot (-ab^2 + 4a^2c)a^{-1} = b^2 - 4ac
\]

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 \(a = 1, b = p, c = q\):

\[ x_{1,2} = -\frac{p}{2} \pm \frac{\sqrt{p^2 - 4q}}{2} = -\frac{p}{2} \pm \sqrt{\frac{p^2 - 4q}{4}} = -\frac{p}{2} \pm \sqrt{\frac{(p/2)^2 - q}{4}} \]

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:

\[
\det \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix} = 1 \cdot \det \begin{pmatrix} 1 & 0 & a & b \\ 0 & a & 0 & 0 \\ 3 & 0 & a & 0 \\ 0 & 3 & 0 & a \end{pmatrix} + 3 \cdot \det \begin{pmatrix} 0 & a & b & 0 \\ 1 & 0 & a & b \\ 3 & 0 & a & 0 \\ 0 & 3 & 0 & a \end{pmatrix}
\]
The evaluation of the determinant (I) yields:

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

The evaluation of the determinant (II) yields:

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

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:

\[
\Delta = (-1)^{\frac{3}{2}} \cdot (4a^3 + 27b^2) = -(4a^3 + 27b^2)
\]

**Solution of Problem 2**

a) In general, the formula \(E : Y^2 = X^3 + aX + b\) with \(a, b \in K\) describes an elliptic curve. Here, we have \(a = 2, b = 6\) with \(a, b \in \mathbb{F}_7\).

\(E\) is an elliptic curve over \(\mathbb{F}_7\), since the discriminant is:

\[
\Delta = -16(4a^3 + 27b^2) \equiv -16064 \equiv 1 \neq 0 \pmod{7}. \tag{1}
\]

b) The point-counting algorithm is solved in a table:

<table>
<thead>
<tr>
<th>(z)</th>
<th>(z^2)</th>
<th>(z^3)</th>
<th>(z^3 + 2z + 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>3</td>
</tr>
</tbody>
</table>
From this table we obtain:

\[ Y^2 \in \{0, 1, 2, 4\}, \]
\[ X^3 + 2X + 6 \in \{0, 1, 2, 3, 4, 6\}, \]

and hence it follows:

\[ E(\mathbb{F}_7) = \{(1, 3), (1, 4), (2, 2), (2, 5), (3, 2), (3, 5), (4, 1), (4, 6), (5, 1), (5, 6), \mathcal{O}\} \]

The inverses of each point are:

\[-(1, 3) = (1, 4),\]
\[-(2, 2) = (2, 5),\]
\[-(3, 2) = (3, 5),\]
\[-(4, 1) = (4, 6),\]
\[-(5, 1) = (5, 6),\]
\[-\mathcal{O} = \mathcal{O}\]

c) The order of the group is \( \text{ord}(E(\mathbb{F}_q)) = \#E(\mathbb{F}_q) = 11 \).

d) To obtain the discrete logarithm for \( Q = aP \), we rearrange the equation:

\[ cP + dQ = c'P + d'Q \]
\[ \Rightarrow (c - c')P = (d' - d)Q = (d' - d)aP \]
\[ \Rightarrow a \equiv (c - c')(d' - d)^{-1} \pmod{\text{ord}(P)}. \]

As \( \gcd(d' - d, n) = 1 \) holds, the discrete logarithm \( a \) exists.

e) The left-hand side and the right-hand side of (2) are evaluated and compared:

\[ 2P = (4, 1) + (4, 1) = (x_3, y_3) \]
\[ x_3 = ((3 \cdot 4^2 + 2)(2 \cdot 1)^{-1})^2 - 2 \cdot 4 \]
\[ \equiv ((3 \cdot 2 + 2)2^{-1})^2 + 6 \equiv (8 \cdot 4)^2 + 6 \equiv 1 \pmod{7} \]
\[ y_3 = (8 \cdot 4)(4 - 1) - 1 \equiv 4 \pmod{7} \]
\[ \Rightarrow 2P = (1, 4) \]

For the inverse of 2 we have: \( 1 = 7 + 2(-3) \Rightarrow 2^{-1} \equiv 4 \pmod{7} \).

\[ 2P + 4Q = (1, 4) + (3, 5) = (x_3, y_3) \]
\[ x_3 = ((5 - 4)(3 - 1)^{-1})^2 - 1 - 3 \equiv 1 \cdot 2^{-1})^2 - 4 \]
\[ \equiv 5 \pmod{7} \]
\[ y_3 = (1 \cdot 4)(1 - 5) - 4 \equiv 4(-4) - 4 \equiv 1 \pmod{7} \]
\[ \Rightarrow 2P + 4Q = (5, 1) \]
\[ -P - 3Q = -(4, 1) + (5, 6) = (4, 6) + (5, 6) = (x_3, y_3) \]
\[ x_3 = 0 - 4 - 5 \equiv 5 \pmod{7} \]
\[ y_3 = 0 - 6 \equiv 1 \pmod{7} \]
\[ \Rightarrow -P - 3Q = (5, 1) \]

Equation (2) is fulfilled. The discrete logarithm is:

\[ a = (2 - (-1))((-3) - 4)^{-1} \equiv 3(-7)^{-1} \equiv 3 \cdot 3 \equiv 9 \pmod{11} \]
Solution of Problem 3

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

$$\frac{\partial f}{\partial X} = -3X^2 - a = 0 \iff a = -3X^2 \quad (2)$$

$$\frac{\partial f}{\partial Y} = 2Y = 0 \quad \text{char}(K) \neq 2 \iff Y = 0. \quad (3)$$

Note that $(2)$ is equivalent to $a \equiv 0$ independent of $X$, if $\text{char}(K) = 3$.

The definition for a singular point of $f$ is given as $P = (x, y) \in E(K)$ singular $\iff \frac{\partial f}{\partial X}|_P = 0 \land \frac{\partial f}{\partial Y}|_P = 0. \quad (4)$

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

Proof:

$\Rightarrow$ Let $\Delta \neq 0$

Assumption: There exists a singular point $(x, y) \in E(K)$.

$$y^2 = x^3 + ax + b \quad (2), (3)$$

$$0 = x^3 + (-3x^2)x + b = -2x^3 + b \iff b = 2x^3 \quad (5)$$

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

$$\Rightarrow \Delta = -16(4a^3 + 27b^2) \quad (2), (5)$$

$$= -16(4 \cdot (-27) \cdot x^6 + 27 \cdot 4 \cdot x^6)) = 0$$

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 $\text{char}(K) \neq 2$.

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):

$$f(x, 0) = -x^3 - (-3x^2)x - 2x^3 = 0,$$

$$\frac{\partial f}{\partial Y}|_{(x,0)} = 2 \cdot 0 = 0, \text{ and}$$

$$\frac{\partial f}{\partial X}|_{(x,0)} = -3x^2 - (-3x^2) = 0, \text{ as } x \text{ is a multiple root}.$$