Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 10
- Proposed Solution -

Friday, January 19, 2018

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:

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

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:

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

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 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:

$$\Delta = -16(4a^3 + 27b^2) \equiv -16064 \equiv 1 \not\equiv 0 \pmod 7. \tag{1}$$

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

z	z^2	z^3	$z^3 + 2z + 6$
0	0	0	6
1	1	1	2
2	4	1	4
3	2	6	4
4	2	1	1
5	4	6	1
6	1	6	3

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:

$$\begin{aligned}
-(1,3) &= (1,4), \\
-(2,2) &= (2,5), \\
-(3,2) &= (3,5), \\
-(4,1) &= (4,6), \\
-(5,1) &= (5,6), \\
-\mathcal{O} &= \mathcal{O}
\end{aligned}$$

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

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

$$\begin{aligned}
cP + dQ &= c'P + d'Q \\
\Rightarrow (c - c')P &= (d' - d)Q = (d' - d)aP \\
\Rightarrow a &\equiv (c - c')(d' - d)^{-1} \pmod{(\operatorname{ord}(P))}.
\end{aligned}$$

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:

$$\begin{aligned}
2P &= (4,1) + (4,1) = (x_3, y_3) \\
x_3 &= ((3 \cdot 4^2 + 2)(2 \cdot 1)^{-1})^2 - 2 \cdot 4 \\
&\equiv ((3 \cdot 2 + 2)2^{-1})^2 + 6 \equiv (8 \cdot 4)^2 + 6 \equiv 1 \pmod 7 \\
y_3 &= (8 \cdot 4)(4 - 1) - 1 \equiv 4 \pmod 7 \\
\Rightarrow 2P &= (1,4)
\end{aligned}$$

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

$$\begin{aligned}
2P + 4Q &= (1,4) + (3,5) = (x_3, y_3) \\
x_3 &= ((5 - 4)(3 - 1)^{-1})^2 - 1 - 3 \equiv (1 \cdot 2^{-1})^2 - 4 \\
&\equiv 5 \pmod 7 \\
y_3 &= (1 \cdot 4)(1 - 5) - 4 \equiv 4(-4) - 4 \equiv 1 \pmod 7 \\
\Rightarrow 2P + 4Q &= (5,1) \\
-P - 3Q &= -(4,1) + (5,6) = (4,6) + (5,6) = (x_3, y_3) \\
x_3 &= 0 - 4 - 5 \equiv 5 \pmod 7 \\
y_3 &= 0 - 6 \equiv 1 \pmod 7 \\
\Rightarrow -P - 3Q &= (5,1)
\end{aligned}$$

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 $\mathrm{char}(K) \neq 2, 3$ ($K = \mathbb{F}_{p^m}, p$ 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

$$\frac{\partial f}{\partial X} = -3X^2 - a = 0 \Leftrightarrow a = -3X^2 \text{ and} \tag{2}$$
$$\frac{\partial f}{\partial Y} = 2Y = 0 \overset{\mathrm{char}(K)\neq 2}{\Leftrightarrow} Y = 0. \tag{3}$$

Note that (2) 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

$$P = (x, y) \in E(K) \text{ singular } \Leftrightarrow \frac{\partial f}{\partial X}|_P = 0 \wedge \frac{\partial f}{\partial Y}|_P = 0. \tag{4}$$

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

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

$$\begin{aligned} y^2 &= x^3 + ax + b \\ \overset{(2),(3)}{\Leftrightarrow} 0 &= x^3 + (-3x^2)x + b = -2x^3 + b \\ \Leftrightarrow b &= 2x^3 \end{aligned} \tag{5}$$

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

$$\begin{aligned} \Rightarrow \Delta &= -16(4a^3 + 27b^2) \overset{(2),(5)}{=} -16(4(-3x^2)^3 + 27(2x^3)^2) \\ &= -16(4 \cdot (-27) \cdot x^6 + 27 \cdot 4 \cdot x^6)) = 0 \end{aligned}$$

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 (4) that $(x, 0)$ is a singularity, which is a contradiction to the assumption.

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