Dr. Michael Reyer

Tutorial 10
- Proposed Solution -

Friday, January 18, 2019

Solution of Problem 1

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 $(x,y) \in E(K)$.

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

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 $\mathrm{char}(K) = 2, 3$).

Solution of Problem 2

By definition: $E : Y^2 = X^3 + aX + b$ with $a, b \in K$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$ describes an elliptic curve.

a) Here: $E : Y^2 = X^3 + X + 1$, i.e., $a = b = 1$, $K = \mathbb{F}_7$. Then,

$$\Delta = -16(4a^3 + 27b^2) = -16(4 + 27) \equiv 5 \cdot 3 \equiv 1 \not\equiv 0 \pmod 7 .$$

It follows that E is an elliptic curve in $\mathbb{F}_7$.

b) We use the following table to determine the points.

z	z^{-1}	z^2	z^3	$1+z+z^3$
0	-	0	0	1
1	1	1	1	3
2	4	4	1	4
3	5	2	6	3
4	2	2	1	6
5	3	4	6	5
6	6	1	6	6

It follows from the third column that,

$$Y^2 \in \{0, 1, 2, 4\} = A ,$$

and from the last column that

$$1 + X + X^3 \in \{1, 3, 4, 5, 6\} = B .$$

Furthermore,

$$C = A \cap B = \{1, 4\} .$$

With $Y^2 = 1 \Leftrightarrow Y \in \{1, 6\}$ and $1 + X + X^3 = 1 \Leftrightarrow X = 0$

$$\Rightarrow (0, 1), (0, 6) \in E(\mathbb{F}_7) .$$

With $Y^2 = 4 \Leftrightarrow Y \in \{2, 5\}$ and $1 + X + X^3 = 4 \Leftrightarrow X = 2$

$$\Rightarrow (2, 2), (2, 5) \in E(\mathbb{F}_7) .$$

We can determine the set of all points on E,

$$E(\mathbb{F}_7) = \{\mathcal{O}, (0, 1), (0, 6), (2, 2), (2, 5)\} .$$

For the trace t it holds

$$\#E(\mathbb{F}_q) = q + 1 - t .$$

Here, $q = 7$, and $\#E(\mathbb{F}_7) = 5$, so

$$5 = 7 + 1 - t \Leftrightarrow t = 3 .$$

Note (Hasse): $t < 2\sqrt{q} = 2\sqrt{7} \approx 5.3$

c) With the group law addition, $E(\mathbb{F}_7)$ is a finite Abelian group. It holds $\operatorname{ord}(P) \mid \#E(\mathbb{F}_7)$ (Lagrange's theorem). It follows for $P \neq \mathcal{O} : 1 < \operatorname{ord}(P) = 5$, i.e., every $P \neq \mathcal{O}$ is a generator. The addition for $P = (x, y)$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ is defined by

(i) $P + \mathcal{O} = P$

(ii) $P + (x, -y) = \mathcal{O} \Rightarrow -P = (x, -y)$

(iii) If $P_1 \neq \pm P_2 \Rightarrow P_3 = (x_3, y_3) = P_1 + P_2$ with $z = \frac{y_2 - y_1}{x_2 - x_1}$, $x_3 = z^2 - x_1 - x_2$, $y_3 = z(x_1 - x_3) - y_1$.

(iv) If $P_1 \neq -P_1 \Rightarrow 2P_1 = P_1 + P_1 = (x_3, y_3)$ with $c = \frac{3x_1^2 + a}{2y_1}$, $x_3 = c^2 - 2x_1$, $y_3 = c(x_1 - x_3) - y_1$.

Start with $P = (0, 1)$.

$$
\begin{aligned}
2P &= 2 \cdot (0,1) \overset{\text{(iv)}}{=} (2,5) \\
&\quad \text{using } c = \frac{1}{2} = 2^{-1} \overset{\text{Table}}{=} 4 \Rightarrow x_3 = 4^2 \equiv 2 \Rightarrow y_3 = 4(-2) - 1 \equiv 5 \mod 7 \\
3P &= (2,5) + (0,1) \overset{\text{(iii)}}{=} (2,2) \\
&\quad \text{using } z = \frac{-4}{-2} = 4 \cdot 2^{-1} = 2 \Rightarrow x_3 = 4 - 0 - 2 = 2 \\
&\qquad\qquad \Rightarrow y_3 = 2(2-2) - 5 \equiv 2 \mod 7 \\
4P &= (2,2) + (0,1) = (0,6) \\
5P &= (0,6) + (0,1) \overset{\text{(ii)}}{=} \mathcal{O} \\
6P &= \mathcal{O} + (0,1) \overset{\text{(i)}}{=} (0,1)
\end{aligned}
$$