Dr. Michael Reyer

Tutorial 11
- Proposed Solution -

Friday, January 25, 2019

Solution of Problem 1

a) $E_{a,b} : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_7$, $P_1 = (1,1)$, $P_2 = (6,2)$

$$P_1 \Rightarrow 1 \equiv 1 + a + b \Leftrightarrow a + b \equiv 0 \Leftrightarrow a \equiv -b \mod 7$$
$$P_2 \Rightarrow 4 \equiv 6 - 6b + b \Leftrightarrow 5b \equiv 2 \Leftrightarrow b \equiv 6 \Rightarrow a \equiv 1 \mod 7$$
$$\Rightarrow y^2 = x^3 + x + 6$$

Calculate $\Delta = -16(4a^3 + 27b^2) \equiv 5(4 + (-1) \cdot 1) \equiv 15 \equiv 1 \neq 0 \mod 7$. It follows $E_{1,6}$ is an eliptic curve over $\mathbb{F}_7$.

b) $E_{6,1} : y^2 = x^3 + 6x + 1$. With

$$\Delta = -16(4a^3 + 27b^2) \equiv 5(4 \cdot (-1)^3 - 1 \cdot 1) \equiv 3 \neq 0 \mod 7$$

is $E_{6,1}$ an elliptic curve over $\mathbb{F}_7$.

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

$$\Rightarrow y^2 \in \{0, 1, 2, 4\}$$
$$x^3 + 6x + 1 \in \{0, 1, 2, 4, 5\}$$
$$\Rightarrow E_{6,1}(\mathbb{F}_7) = \{(0,1), (0,6), (1,1), (1,6), (2,0), (3,2), (3,5), (5,3), (5,4), (6,1), (6,6), \mathcal{O}\}$$
$$\#E_{6,1}(\mathbb{F}_7) = 12$$

The solutions for the inverses are

$$\begin{aligned}(0,1) &= -(0,6)\\ (1,1) &= -(1,6)\\ (6,1) &= -(6,6)\\ (2,0) &= -(2,0)\\ (3,2) &= -(3,5)\\ (5,3) &= -(5,4)\\ \mathcal{O} &= -\mathcal{O}\end{aligned}$$

Note: $\#E_{6.1}(\mathbb{F}_7) = q + 1 - t \Leftrightarrow t = 7 + 1 - \#E_{6,1}(\mathbb{F}_7) = 8 - 12 = -4$

c) It holds $\mathrm{ord}(P) | \#E_{6,1}(\mathbb{F}_7) = 12 \Rightarrow \mathrm{ord}(P) \in \{1, 2, 3, 4, 6, 12\}$ (cf. Lagrange's theorem).

d) As just observed, the order of the subgroup generated by $Q = (1, 1)$ may be $\mathrm{ord}(Q) \in \{1, 2, 3, 4, 6, 12\}$. We will eliminate one element after another from the set until we reach $\mathrm{ord}(Q) = 12$. The conclusion will be that Q is a generator.

$$\begin{aligned}Q \neq \mathcal{O} &\Rightarrow \mathrm{ord}(Q) \in \{2, 3, 4, 6, 12\}\\ 4Q \neq \mathcal{O} \text{ (known from exercise) } &\Rightarrow \mathrm{ord}(Q) \in \{2, 3, 6, 12\}\end{aligned}$$

Calculate $2Q$.

$$\begin{aligned}2Q &= (1,1) + (1,1) = (x, y), \text{ with}\\ x &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 = \left(\frac{3 \cdot 1 + 6}{2}\right)^2 - 2\\ &= \left(\frac{9}{2}\right)^2 - 2 = (9 \cdot 4)^2 - 2 = 1^2 - 2 = 6\\ y &= \left(\frac{3x_1 + a}{2y_1}\right)(x_1 - x) - y_1 = \frac{9}{2}(1 - 6) - 1\\ &= 1 \cdot 2 - 1 = 1\\ \Rightarrow 2Q &= (6, 1) \neq \mathcal{O} \Rightarrow \mathrm{ord}(Q) \in \{3, 6, 12\}\end{aligned}$$

$$\begin{aligned}Q + 2Q \neq \mathcal{O} \text{ (see inverses above) } &\Rightarrow \mathrm{ord}(Q) \in \{6, 12\}\\ 2Q + 4Q \neq \mathcal{O} \text{ (see inverses above) } &\Rightarrow \mathrm{ord}(Q) = 12\end{aligned}$$

We conclude that Q is a generator.

Solution of Problem 2

a) $E_\alpha : Y^2 = X^3 + \alpha X + 1$ in $\mathbb{F}_{13}$.

$$\begin{aligned}&\alpha = 2\\ &\Delta = -16(4a^3 + 27b^2) = 10(4 \cdot 2^3 + 27) = 10 \cdot 59 \equiv 5 \not\equiv 0 \mod 13\end{aligned}$$

$\Rightarrow E_2$ is an elliptic curve.

b)

$$
\begin{aligned}
0P &= \mathcal{O} \\
1P &= (0,1) \\
2P &= (0,1) + (0,1) = (1,11) \\
\text{using } x_3 &= \left(\frac{3\cdot 0^2 + 2}{2\cdot 1}\right)^2 - 2\cdot 0 = (2\cdot 2^{-1})^2 = 1 \\
y_3 &= 1\cdot(0-1) - 1 = -2 = 11 \\
3P &= (1,11) + (0,1) = (8,10) \\
\text{using } x_3 &= \left(\frac{1-11}{0-1}\right)^2 - 1 - 0 = (3\cdot 12)^2 - 1 = 36^2 - 1 = 8 \\
y_3 &= 36(1-8) - 11 = 10 \\
4P &= (8,10) + (0,1) = (2,0) \\
\text{using } x_3 &= \left(\frac{1-10}{0-8}\right)^2 - 8 - 0 = (4\cdot 5^{-1})^2 - 8 = (4\cdot 8)^2 - 8 = 2 \\
y_3 &= 20(8-0) - 3 = 1
\end{aligned}
$$

c) $\langle P\rangle \subseteq \{\mathcal{O},(0,1),(1,11),(8,10),(2,0),(0,12),(1,2),(8,3)\}$, where $(0,1) = -(0,12)$, $(1,11) = -(1,2)$, $(8,10) = -(8,3)$ and $(2,0) = -(2,0)$. We start with the five points calculated earlier. Then we add the inverse elements, as they must be elements of the subgroup. With $\#\langle P\rangle = \#E(\mathbb{F}_{13})$ is P a cyclic generator of order $\#\langle P\rangle = 8$.

Note: equivalent solutions are possible.

d) With $b_i = iP$, $a = jm + i$, $g_j = Q - jmP$

$$b_i = g_j \Leftrightarrow iP = Q - jmP \Leftrightarrow Q = (i + jm)P \Leftrightarrow Q = aP$$

$i + mj$ covers all numbers between $0,\ldots,q-1$.

e) The *babysteps* have already been computed. Compute *giantsteps*: $Q - jmP$ until $Q - jmP = iP$ for some i with $j = 0,\ldots,m-1$.

$$
\begin{aligned}
j = 0 &: (8,3) - 0(2,0) = (8,3) \\
j = 1 &: (8,3) - (2,0) = (8,3) + (2,0) = (0,1) = P \\
\text{with } x_3 &= \left(\frac{0-3}{2-8}\right)^2 - 8 - 2 = (10\cdot 2)^2 - 10 = 0 \\
y_3 &= 20(8-0) - 3 = 1
\end{aligned}
$$

$$
\begin{aligned}
&\Rightarrow j = 1, i = 1 \\
&\Rightarrow k = i + jm = 1 + 1\cdot 4 = 5 \\
&\quad Q = 5P \Rightarrow 5(0,1) = (8,3)
\end{aligned}
$$

Check:

$$
\begin{aligned}
5P &= 4P + P = (2,0) + (0,1) = (8,3) \\
\text{using } x_3 &= \left(\frac{1-0}{0-2}\right)^2 - 1 - 0 = 16^2 - 2 = 8 \\
y_3 &= (1\cdot 6)(2-8) - 0 = 6\cdot 7 - 0 = 42 = 3
\end{aligned}
$$