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

Exercise 9
- Proposed Solution -

Friday, January 12, 2018

Solution of Problem 1

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

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

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

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

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 $\mathrm{ord}(P) | \#E_{6,1}(\mathbb{F}_7) = 12 \Rightarrow \mathrm{ord}(P) \in \{1, 2, 3, 4, 6, 12\}$ (c.f. 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 $2Q$.

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

Let $\mathrm{ord}(Q) = 2$, then $4Q = \mathcal{O}$, a contradiction $\Rightarrow \mathrm{ord}(Q) \in \{3, 6, 12\}$

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

We conclude that Q is a generator.

Solution of Problem 2

a) $\Delta = -16(4 \cdot 4^3 + 27 \cdot 1) \equiv -4528 \equiv -3 \equiv 2 \not\equiv 0 \mod 5.$

$\Rightarrow E$ is an elliptic curve.

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

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

This provides that $y^2 \in \{0,1,4\}$ and $x^3+4x+1 \in \{0,1,2\}$.

So we only need to consider the cases where both terms are either equal 0:

$$\begin{aligned} x^3+4x+1 = 0 &\Rightarrow x = 3 \\ y^2 = 0 &\Rightarrow y = 0 \end{aligned}$$

or equal 1:

$$\begin{aligned} x^3+4x+1 = 1 &\Rightarrow x \in \{0,1,4\} \\ y^2 = 1 &\Rightarrow y \in \{1,4\} \end{aligned}$$

This enables us to find all the points on the curve:

$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (1,1), (1,4), (4,1), (4,4), (3,0)\}$$

The total number of points on the curve is $\#E(\mathbb{F}_5) = 8$.

c) Is $Q = (1,1)$ a generator of the curve?

$$\begin{aligned} 2Q &\overset{(ii)}{=} Q + Q \\ x &= ((3 \cdot 1^2 + 4)(2 \cdot 1)^{-1})^2 - 2 \cdot 1 = (2 \cdot 2^{-1})^2 - 2 = -1 \equiv 4 \\ y &= 1(1-4) - 1 = -3 - 1 = -4 \equiv 1 \end{aligned}$$

$2Q = (4,1)$ is a point on the curve.

$$\begin{aligned} 4Q &\overset{(ii)}{=} 2Q + 2Q \\ x &= ((3 \cdot 4^2 + 4)(2 \cdot 1)^{-1})^2 - 4 \cdot 2 = (2 \cdot 2^{-1})^2 - 4 \cdot 2 = 3 \\ y &= 0 \end{aligned}$$

$4Q = (3,0)$ is a point on the curve.

$$\begin{aligned} 8Q &\overset{(ii)}{=} 4Q + 4Q \\ &(3,0) + (3,0) = \mathcal{O}, \text{as this point is selfinverse} \end{aligned}$$

Hence $(1,1)$ is a generator of the curve.

d) The binary representation of 45 is 101101.

$$\begin{aligned}45P &= P + 4P + 8P + 32P \\ &= P + 2^2P + 2^3P + 2^5P \\ &= P + 2\cdot 2P + 2\cdot 2\cdot 2P + 2\cdot 2\cdot 2\cdot 2\cdot 2P \\ &= P + 2(2(P + 2P) + 2\cdot 2\cdot 2\cdot 2\cdot 2P \\ &= P + 2(2(P + 2(P + 2\cdot 2P))))\end{aligned}$$

The last line corresponds to the representation of Horner's scheme.

e) The iterative algorithm starts with the point P. Then it iterates through the bits of k from the MSB k_m downto k_0. It doubles if the current k_i is zero or it doubles and adds otherwise. At the end of the loop it returns the computed point $Q = kP$.

Algorithm 1 $f_{\text{it}}(P, k = k_m, \ldots, k_0)$

```
Q ← P;
for i ← m − 2 downto 0 do
    Q ← 2Q;            // Double
    if k_i == 1 then   // if i-th the bit is 1
        Q ← Q + P;     // Add
    end if;
end for;
return Q;
```

When the iterative algorithm is applied to the given example with $k = 45$, we obtain the following sequence from the for-loop:

$$P, 2P, 2(2P) + P, 2(2(2P) + P), 2(2(2(2P) + P)), 2(2(2(2(2P) + P))) + P$$

The last outcome can be reformulated to $2(2(2(2(2P)+P)))+P = 2^5P+2^3P+2^2P+P$ which corresponds to the binary expansion of $45P$.

f) In the recursive algorithm, it calls itself recursively without the last bit.

Algorithm 2 $f_{\text{rec}}(P, k)$

```
if k == 1 then
    return P;
else
    if k mod 2 = 0 then                  // i.e., the LSB is zero
        return 2 · f_rec(P, k >> 1);     // Double, right-shift k by one bit
    else                                 // otherwise the LSB is one
        return P + 2 · f_rec(P, k >> 1); // Double and Add, right-shift k by one bit
    end if;
end if;
```

When the recursive algorithm is applied to the given example with $k = 45$, we obtain $45P = P + 2(2(P + 2(P + 2(2P))))$ which corresponds to the Horner's scheme of $45P$.