Solution of Problem 1

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

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

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

<table>
<thead>
<tr>
<th>( z )</th>
<th>( z^{-1} )</th>
<th>( z^2 )</th>
<th>( z^3 )</th>
<th>( 1 + z + z^3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

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 \( Y^2 = 1 \iff Y \in \{1, 6\} \) and \( 1 + X + X^3 = 1 \iff X = 0 \)
\[
\Rightarrow (0, 1), (0, 6) \in E(\mathbb{F}_7).
\]

With \( Y^2 = 4 \iff Y \in \{2, 5\} \) and \( 1 + X + X^3 = 4 \iff X = 2 \)
\[
\Rightarrow (2, 2), (2, 5) \in E(\mathbb{F}_7).
\]
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
\[
5 = 7 + 1 - t \iff t = 3.
\]

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 \( \text{ord}(P) \mid \#E(\mathbb{F}_7) \) (Lagrange’s theorem). It follows for \( P \neq \mathcal{O} : 1 < \text{ord}(P) = 5 \), 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

\[
\begin{align*}
\text{(i)} & \quad P + \mathcal{O} = P \\
\text{(ii)} & \quad P + (x, -y) = \mathcal{O} \Rightarrow -P = (x, -y) \\
\text{(iii)} & \quad \text{If } P_1 \neq \pm P_2 \Rightarrow P_3 = (x_3, y_3) = P_1 + P_2 \text{ with } z = \frac{y_2 - y_1}{x_2 - x_1}, \quad x_3 = z^2 - x_1 - x_2, \\
& \quad y_3 = z(x_1 - x_3) - y_1. \\
\text{(iv)} & \quad \text{If } P_1 \neq -P_1 \Rightarrow 2P_1 = P_1 + P_1 = (x_3, y_3) \text{ with } c = \frac{3x_1^2 + a}{2y_1}, \quad x_3 = c^2 - 2x_1, \\
& \quad y_3 = c(x_1 - x_3) - y_1.
\end{align*}
\]

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

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

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

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

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 elliptic 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 \( \mathbb{F}_7 \).

\[
\begin{array}{cccccc}
 x & x^2 & x^3 & 6x & x^3 + 6x + 1 \\
 0 & 0 & 0 & 0 & 1 \\
 1 & 1 & 1 & 6 & 1 \\
 2 & 4 & 1 & 5 & 0 \\
 3 & 2 & 6 & 4 & 4 \\
 4 & 2 & 1 & 3 & 5 \\
 5 & 4 & 6 & 2 & 2 \\
 6 & 1 & 6 & 1 & 1 \\
\end{array}
\]

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

The solutions for the inverses are

\[
\begin{align*}
(0, 1) &= -(0, 6) \\
(1, 1) &= -(1, 6) \\
(6, 1) &= -(6, 6) \\
(2, 0) &= -(2, 0) \\
(3, 2) &= -(3, 5) \\
(5, 3) &= -(5, 4) \\
\mathcal{O} &= -\mathcal{O}
\end{align*}
\]

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

c) It holds \( \text{ord}(P) \mid \#E_{6,1}(\mathbb{F}_7) = 12 \Rightarrow \text{ord}(P) \in \{1, 2, 3, 4, 6, 12\} \) \(\text{c.f. Lagrange’s theorem}\).
d) As just observed, the order of the subgroup generated by \( Q = (1, 1) \) may be \( \text{ord}(Q) \in \{1, 2, 3, 4, 6, 12\} \). We will eliminate one element after another from the set until we reach \( \text{ord}(Q) = 12 \). The conclusion will be that \( Q \) is a generator.

\[
Q \neq O \Rightarrow \text{ord}(Q) \in \{2, 3, 4, 6, 12\} \\
4Q \neq O \text{ (known from exercise)} \Rightarrow \text{ord}(Q) \in \{2, 3, 6, 12\}
\]

Calculate \( 2Q \).

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

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

\[
Q + 2Q \neq O \text{ (see inverses above)} \Rightarrow \text{ord}(Q) \in \{6, 12\} \\
2Q + 4Q \neq O \text{ (see inverses above)} \Rightarrow \text{ord}(Q) = 12
\]

We conclude that \( Q \) is a generator.
Solution of Problem 3

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

\[ \alpha = 2 \]
\[ \Delta = -16(4\alpha^3 + 27b^2) = 10(4 \cdot 2^3 + 27) = 10 \cdot 59 \equiv 5 \not\equiv 0 \mod 13 \]
\[ \Rightarrow E_2 \text{ is an elliptic curve.} \]

b)

\[ 0P = \mathcal{O} \]
\[ 1P = (0, 1) \]
\[ 2P = (0, 1) + (0, 1) = (1, 11) \]

using \( x_3 = \left( \frac{3 \cdot 0^2 + 2}{2 \cdot 1} \right)^2 - 2 \cdot 0 = (2 \cdot 2^{-1})^2 = 1 \)

\[ y_3 = 1 \cdot (0 - 1) - 1 = -2 = 11 \]
\[ 3P = (1, 11) + (0, 1) = (8, 10) \]

using \( x_3 = \left( \frac{1 - 11}{0 - 1} \right)^2 - 1 - 0 = (3 \cdot 12)^2 - 1 = 36^2 - 1 = 8 \)

\[ y_3 = 36(1 - 8) - 11 = 10 \]
\[ 4P = (8, 10) + (0, 1) = (2, 0) \]

using \( x_3 = \left( \frac{1 - 10}{0 - 8} \right)^2 - 8 - 0 = (4 \cdot 5^{-1})^2 - 8 = (4 \cdot 8)^2 - 8 = 2 \)

\[ y_3 = 20(8 - 0) - 3 = 1 \]

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 \( b_i = iP, a = jm + i, g_j = Q - jmP \)

\[ b_i = g_j \iff iP = Q - jmP \iff Q = (i + jm)P \iff Q = aP \]

\( i + mj \) 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 \( j = 0, \ldots, m - 1 \).

\[ j = 0 : (8, 3) - 0(2, 0) = (8, 3) \]
\[ j = 1 : (8, 3) - (2, 0) = (8, 3) + (2, 0) = (0, 1) = P \]

with \( x_3 = \left( \frac{0 - 3}{2 - 8} \right)^2 - 8 - 2 = (10 \cdot 2)^2 - 10 = 0 \)

\[ y_3 = 20(8 - 0) - 3 = 1 \]
\[ j = 1, i = 1 \]
\[ k = i + jm = 1 + 1 \cdot 4 = 5 \]
\[ Q = 5P \Rightarrow 5(0, 1) = (8, 3) \]

Check:

\[ 5P = 4P + P = (2, 0) + (0, 1) = (8, 3) \]
using \[ x_3 = \left( \frac{1 \cdot 0 - 0^2}{0 - 2} \right) - 1 - 0 = 16^2 - 2 = 8 \]
\[ y_3 = (1 \cdot 6)(2 - 8) - 0 = 6 \cdot 7 - 0 = 42 = 3 \]