Homework 9, Solutions

(5.5) Find all the points on the elliptic curve.
(b) \( E : y^2 = x^3 + 2x + 7 \) over \( \mathbb{Z}_{11} \).

Solution: (b) We first generate the square table (computing \( y^2 \)).

\[
\text{for } y = [0:10], \ [y; \text{powermod}(y, 2, 11)]', \text{end}
\]

\[
\begin{array}{cc}
0 & 0 \\
1 & 1 \\
2 & 4 \\
3 & 9 \\
4 & 5 \\
5 & 3 \\
6 & 3 \\
7 & 5 \\
8 & 9 \\
9 & 4 \\
10 & 1 \\
\end{array}
\]

Then we compute the corresponding \( x^3 + 2x + 7 \) values.

\[
\text{for } x = [0:10], \ [x; \text{mod}(x^3+2x+7, 11)]', \text{end}
\]

\[
\begin{array}{cc}
0 & 7 \\
1 & 10 \\
2 & 8 \\
\end{array}
\]
Therefore,
\[ E = \{ O, (6, 2), (6, 9), (7, 1), (7, 10), (10, 2), (10, 9) \}. \]

(5.6) Make an addition table for the elliptic curve.
(e) \( E : y^2 = x^3 + 2x + 7 \) over \( \mathbb{Z}_{11} \).

Solutions:
(e) From Exercise (5.5)(b), we computed all the points of \( E \).
\[ E = \{ O \} \cup \{ (6, 2), (6, 9), (7, 1), (7, 10), (10, 2), (10, 9) \}. \]

Then we compute the sums of all possible pairs. Note that \(- (6, 2) = (6, 9), -(7, 1) = (7, 10), -(10, 2) = (10, 9)\). Using the property that \( O + P = P, P + (-P) = O, \) and \( P + Q = Q + P \), we can skip some of the computations.

We can have the following systematic approach.
(Step 1) Compute all additions involving \((6, 2)\). Then from the properties, we already know \((6, 2) + O = (6, 2), \) and \((6, 2) + (6, 9) = O\). Hence we only need to compute \((6, 2) + (6, 2), (6, 2) \pm (7, 1)\) and \((6, 2) \pm (10, 2)\).

\[
\text{>> multell([6,2], 2, 2, 7, 11)}
\]
\[
\begin{array}{c}
\text{ans} \\
\hline
10 \\
9
\end{array}
\]
```matlab
>> addell([6,2], [7,1], 2, 7, 11)
an =
   10   2
>> addell([6,2], [7,10], 2, 7, 11)
an =
    7   1
>> addell([6,2], [10,2], 2, 7, 11)
an =
    6   9
>> addell([6,2], [10,9], 2, 7, 11)
an =
    7   10
>> multell([6,9],2,2,7,11)
an =
   10   2
>> addell([6,9], [7,1], 2, 7, 11)
an =
    7   10
>> addell([6,9], [7,10], 2, 7, 11)
an =
   10   9
>> addell([6,9], [10,2], 2, 7, 11)
an =
    7   1
>> addell([6,9], [10,9], 2, 7, 11)
an =
    6   2
>> multell([7,1],2,2,7,11)
an =
    6   2
>> addell([7,1], [10,2], 2, 7, 11)
an =
   10   9
>> addell([7,1], [10,9], 2, 7, 11)
an =
    6   9
>> multell([7,10],2,2,7,11)
```
ans =
 6   9
>> addell([7,10], [10,2], 2, 7, 11)
an
c =
 6   2
>> addell([7,10], [10,9], 2, 7, 11)
an
c =
 10   2
>> multell([10,2], 2, 2, 7, 11)
an
c =
 7   10
>> multell([10,9], 2, 2, 7, 11)
an
c =
 7   1

<table>
<thead>
<tr>
<th></th>
<th>O</th>
<th>(6,2)</th>
<th>(6,9)</th>
<th>(7,1)</th>
<th>(7,10)</th>
<th>(10,2)</th>
<th>(10,9)</th>
</tr>
</thead>
<tbody>
<tr>
<td>O</td>
<td>O</td>
<td>(6,2)</td>
<td>(6,9)</td>
<td>(7,1)</td>
<td>(7,10)</td>
<td>(10,2)</td>
<td>(10,9)</td>
</tr>
<tr>
<td>(6,2)</td>
<td>(6,2)</td>
<td>(10,9)</td>
<td>O</td>
<td>(10,2)</td>
<td>(7,1)</td>
<td>(6,9)</td>
<td>(7,10)</td>
</tr>
<tr>
<td>(6,9)</td>
<td>(6,9)</td>
<td>O</td>
<td>(10,2)</td>
<td>(7,10)</td>
<td>(10,9)</td>
<td>(7,1)</td>
<td>(6,2)</td>
</tr>
<tr>
<td>(7,1)</td>
<td>(7,1)</td>
<td>(10,2)</td>
<td>(7,10)</td>
<td>(6,2)</td>
<td>O</td>
<td>(10,9)</td>
<td>(6,9)</td>
</tr>
<tr>
<td>(7,10)</td>
<td>(7,10)</td>
<td>(7,1)</td>
<td>(10,9)</td>
<td>O</td>
<td>(6,9)</td>
<td>(6,2)</td>
<td>(10,2)</td>
</tr>
<tr>
<td>(10,2)</td>
<td>(10,2)</td>
<td>(6,9)</td>
<td>(7,1)</td>
<td>(10,9)</td>
<td>(6,2)</td>
<td>(7,10)</td>
<td>O</td>
</tr>
<tr>
<td>(10,9)</td>
<td>(10,9)</td>
<td>(7,10)</td>
<td>(6,2)</td>
<td>(6,9)</td>
<td>(10,2)</td>
<td>O</td>
<td>(7,1)</td>
</tr>
</tbody>
</table>