Elliptic Curve Cryptography

Midterm, 2008 Spring

[1] (a) 14 points

<table>
<thead>
<tr>
<th>x</th>
<th>x^3 + x + 1</th>
<th>y</th>
<th>y^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1,10</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>5,6</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>3,8</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>5,6</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>5,6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>2,9</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>X</td>
<td>10</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>∞</td>
</tr>
</tbody>
</table>

(b) (6,6)

\[ \lambda = \frac{3x^2+1}{2x^8} = \frac{7}{4} = 10, \quad x_3 = 10^2 - 3 - 3 = 6, \quad y_3 = (3 - 6) \times 10 - 8 = 6 \]

(c) (0,1)

\[ \lambda = \frac{6-8}{6-3} = \frac{9}{3} = 3, \quad x_3 = 3^2 - 3 - 6 = 0, \quad y_3 = (3 - 0) \times 3 - 8 = 1 \]

(d) 9

\[ 1728 \times \frac{4+1^3}{4+1^3+27+1^2} = \frac{4}{9} = 9 \]

(e) 14560

\[ s_0 = 2, \ s_1 = a = 11 + 1 - 14 = -2, \ s_n = as_{n-1} - qs_{n-2} \]
\[ s_2 = -18, \ s_3 = 58, \ s_4 = 82 \]
\[ \#E(F_{11^4}) = 11^4 + 1 - 82 = 14560 \]

[2] Using subfield curve as [1](e)

(a) 968

\[ s_0 = 2, \ s_1 = -1, \ s_2 = -3, \ s_3 = 5, \ s_4 = 1, \ s_5 = -11, \ s_6 = 9, \ s_7 = 13, \]
\[ s_8 = -31, \ s_9 = 5, \ s_{10} = 57, \ \#E_0(F_{2^{10}}) = 2^{10} + 1 - 57 = 968 \]

(b) 968

\[ s_0 = 2, \ s_1 = 1, \ s_2 = -3, \ s_3 = -5, \ s_4 = 1, \ s_5 = 11, \ s_6 = 9, \ s_7 = -13, \]
\[ s_8 = -31, \ s_9 = -5, \ s_{10} = 57, \ \#E_0(F_{2^{10}}) = 2^{10} + 1 - 57 = 968 \]
[3] For an odd \( n \), the x-coordinates of points in \( E[n] \) satisfy the \( n \)-th division polynomial \( \Psi_n(x) \). Also, the roots of \( x^q - x \) represent all elements in \( F_q \).

We can find the x-coordinates of \( E[n] \cap E(F_\ell) \) by use of \( \gcd(\Psi_n(x), x^q - x) \). Again, \( n \) is odd, so the y-coordinate of points in \( E[n] \) must be nonzero. Hence, \( \#E[n] \cap E(F_\ell) = \deg(\gcd(\Psi_n(x), x^q - x)) + 1 \), where 1 is \( \infty \).

[4] (a) Use the fact \( q^\ell - 1 \equiv 1 \pmod{\ell} \)

\[
\begin{align*}
x &\leftarrow \ell - 1 \\
\text{for } i = 1 \text{ to } r \\
&\quad \text{for } j = e_i \text{ to } 0 \\
&\quad \quad y \leftarrow x/p_i \\
&\quad \quad \text{if } q^j \equiv 1 \pmod{\ell} \\
&\quad \quad \quad x \leftarrow y \\
&\quad \quad \text{else} \\
&\quad \quad \quad \text{next } i \\
&\text{return } x
\end{align*}
\]

(b) See MOV Attack in Text p.145

Now \( N = \ell \), a prime. And we need \( d = \gcd(M, \ell) \neq 1 \) in step 3.

So, we have to search a random point \( T \in E(F_{\ell^m}) \), and \( \text{ord}(T) = h\ell \).

After that, we don’t need to repeat the algorithm as the step 6. When we found a proper \( T \), this is done.

[5] 100

Use the group isomorphism \( \phi \) between \( E(F_{119}) \) and \( Z_{119} \).

\[
\phi(P) = \frac{1}{1} = 1, \quad \phi(Q) = \frac{4}{8} = 100, \quad \text{so } Q = 100P
\]

[6] (a) See Lemma 4.5 in Text p.93

(b) 174

\( \phi_{199}(P) = 5P \). Consider the endomorphism \( (\phi_{199} - 5) \).

The number of points satisfying \( \phi_{199}(P) = 5P \) is the degree of \( (\phi_{199} - 5) \)

\[
a = 199 + 1 - 190 = 10 \\
\deg(\phi_{199} - 5) = 1^2 * 199 + 5^2 - 1 * 5 * 10 = 174
\]

[7] (a) Let \((x, y)\) be \((dx_1, d^2y_1)\). \( E^{(d)} \) can be transformed to \( dy_1^2 = x_1^3 + ax_1 + b \)

(b) 3974

\[
a = 4003 + 1 - 4034 = -30. \quad \#E_2 = 4003 + 1 - \left(\frac{-1}{4003}\right)a = 3974
\]


[9] \(-10 \pm 93i \) or \(-10 \pm 106i \)

\[
x^2 + 20x - 7 = 0, \quad x = \frac{-20 \pm \sqrt{400 + 28}}{2} = -10 \pm \frac{\sqrt{-169}}{2} = -10 \pm 93i
\]