4.1 Elliptic Curves over Finite Fields

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008
Outline

1. Examples
   - Example 4.1
   - Example 4.2
   - Example 4.3

2. Theorem 4.1

3. Theorem 4.2

4. Theorem 4.3

5. Theorem 4.4
Example 4.1 - (1)

- $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^3 + x + 1$</th>
<th>$y$</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>$\pm 1$</td>
<td>(0, 1), (0, 4)</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>$\pm 1$</td>
<td>(2, 1), (2, 4)</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>$\pm 1$</td>
<td>(3, 1), (3, 4)</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>$\pm 2$</td>
<td>(4, 2), (4, 3)</td>
</tr>
<tr>
<td>$\infty$</td>
<td></td>
<td>$\infty$</td>
<td>$\infty$</td>
</tr>
</tbody>
</table>

$\rightarrow |E(\mathbb{F}_5)| = 9$
Example 4.1 - (2)

Compute \((3, 1) + (2, 4)\):

\[
\text{for } \frac{4 - 1}{2 - 3} \equiv 2 \text{ (mod 5)}
\]

\[
\to y = 2(x - 3) + 1 = 2x
\]

Substituting this into \(y^2 = x^3 + x + 1\)

\[
\to 0 = x^3 - 4x^2 + x + 1
\]

Sum of 3 roots = 4, we have known two roots 2, 3, so the remaining is 4

\[
\to y = 2x \quad \therefore y = 3
\]

Reflecting across x-axis \(\to y = -3 = 2\)

\[
\therefore (3, 1) + (2, 4) = (4, 2)
\]

Actually \(E(F_5)\) is cyclic, generated by \((0, 1)\). (Ex. 4.1)

i.e. \(E(F_5) \cong \mathbb{Z}_9\)
Example 4.2

\[ y^2 = x^3 + 2 \text{ over } \mathbb{F}_7 \]

\[ E(\mathbb{F}_7) = \{ \infty, (0, 3), (0, 4), (3, 1), (3, 6), (5, 1), (5, 6), (6, 1), (6, 6) \} \]

all points satisfy \( 3P = \infty \)

\[ E(\mathbb{F}_7) \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3 \]
Example 4.3 - (1)

1. \( y^2 + xy = x^3 + 1 \) over \( \mathbb{F}_2 \)
   
   \[ E(\mathbb{F}_2) = \{ \infty, (0, 1), (1, 0), (1, 1) \} \]

   (1, 0), (1, 1) have order 4 , (0, 1) has order 2 \( \therefore E(\mathbb{F}_2) \simeq \mathbb{Z}_4 \)

2. \( y^2 + xy = x^3 + 1 \) over \( \mathbb{F}_4 = \{ 0, 1, \omega, \omega^2 \} \) with the relation
   
   \[ \omega + \omega^2 + 1 = 0 \]

   \[
   \begin{align*}
   x = 0 & \quad \rightarrow \quad y^2 = 1 \quad \rightarrow \quad y = 1 \\
   x = 1 & \quad \rightarrow \quad y^2 + y = 0 \quad \rightarrow \quad y = 0, 1 \\
   x = \omega & \quad \rightarrow \quad y^2 + \omega y = 0 \quad \rightarrow \quad y = 0, \omega \\
   x = \omega^2 & \quad \rightarrow \quad y^2 + \omega^2 y = 0 \quad \rightarrow \quad y = 0, \omega^2 \\
   x = \infty & \quad \rightarrow \quad y = \infty
   \end{align*}
   \]

   \[ E(\mathbb{F}_4) = \{ \infty, (0, 1), (1, 0), (1, 1), (\omega, 0), (\omega, \omega), (\omega^2, 0), (\omega^2, \omega^2) \} \]

   \( \therefore \text{char.}(\mathbb{F}_4) = 2 \quad \therefore \text{at most one point of order 2 (Proposition 3.1)} \)

   In fact, (0, 1) has order 2

   \( \therefore E(\mathbb{F}_4) \) is cyclic of order 8 . i.e. \( E(\mathbb{F}_4) \simeq \mathbb{Z}_8 \)

   Any one of 4 points containing \( \omega \) or \( \omega^2 \) is a generator.
Example 4.3 - (2)

Let \( \phi_2(x, y) = (x^2, y^2) \)

\[
E(\mathbb{F}_2) = \{(x, y) \in E(\mathbb{F}_4) \mid \phi_2(x, y) = (x, y)\}
\]

(see Lemma 4.5)
Theorem 4.1

Theorem 4.1

\[ E/F_q \ . \ Then \]

\[ E(\mathbb{F}_q) \simeq \mathbb{Z}_n \ or \ \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \]

for \( n \geq 1 \) or for \( n_1, n_2 \geq 1 \) with \( n_1 \mid n_2 \)

Proof:

- Any finite abelian group is isomorphic to (Appendix B)

\[ \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r} \ with \ n_i \mid n_{i+1} \ for \ i \geq 1 \]

Since for each \( i \), \( \mathbb{Z}_{n_i} \) has \( n_1 \) elements of order dividing \( n_1 \)

We find \( E(\mathbb{F}_q) \) has \( n_1^r \) elements of order dividing \( n_1 \).

By Theorem 3.2, there are at most \( n_1^2 \)

\[ \therefore r \leq 2 \]
Theorem 4.2

Theorem 4.2 (Hasse)

Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

(Proof will be given in Section 4.2)
Theorem 4.3

Let $q = p^n$, $N = q + 1 - a$

$\exists$ an elliptic curve $E$ over $\mathbb{F}_q$ such that $\# E(\mathbb{F}_q) = N$

if and only if $|a| \leq 2\sqrt{q}$ and $a$ satisfies one of the following

1. $\gcd(a, p) = 1$
2. $n$ is even and $a = \pm 2\sqrt{q}$
3. $n$ is even, $p \not\equiv 1 \pmod{3}$, and $a = \pm \sqrt{q}$
4. $n$ is odd, $p = 2$ or $3$, and $a = \pm p^{(n+1)/2}$
5. $n$ is even, $p \not\equiv 1 \pmod{4}$, and $a = 0$
6. $n$ is odd, and $a = 0$
Theorem 4.4

Let $N$ be as in Theorem 4.3.

Write $N = p^e n_1 n_2$ with $p$ divides $n_1 n_2$, $n_1$ divides $n_2$ (possibly $n_1 = 1$)

$\rightarrow \exists$ an elliptic curve $E$ over $\mathbb{F}_q$ such that

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{p^e} \oplus \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

if and only if

1. $n_1$ divides $q - 1$ in cases (1), (3), (4), (5), (6) in Theorem 4.3.
2. $n_1 = n_2$ in case (2) in Theorem 4.3

These are the only groups.