13.1 Foundations and Definitions

Let $K$ be a field (e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p, \mathbb{F}_{p^2}$)

If $K = \mathbb{F}_p$ (then $p > 3$), in the following $p$ is prime.

Def 13.1 An elliptic curve $E/K$ over the field $K$ is described by an equation:

$$E : y^2 = x^3 + ax + b \quad a, b \in K$$

or $f(x, y) = y^2 - x^3 - ax - b = 0$

provided the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$

For an algebraic extension field $L \supseteq K$ we call

$$E(L) = \{ (x, y) \in L \times L | f(x, y) = 0 \} \cup \{ 0 \}$$

the set of $L$-rational points on $E$.

$0$ denotes the point at infinity, i.e. neutral element.

Remark: a) $E/K$ means $a, b \in K$

b) Since $L \supseteq K$, also $a, b \in L$. Hence, $E/K$ is also $E/L$

c) For $p = 2, 3$ the curve equation is more complicated

d) Condition $\Delta \neq 0$ avoids singularities and ensures that there is a unique tangent at all points on the curve.

Examples: a) $E_1 : y^2 = x^3 - x$ over $\mathbb{R}$, $a = -1, b = 0$

$\Delta = -16(4a^3 + 27b^2) = 64 \neq 0$ : $E_1$ is an EC

b) $E_2 : y^2 = x^3 + 2 + 2$ over $\mathbb{F}_5$, hence $a = 2, b = 2$

$\Delta = -16(4a^3 + 27b^2) = -16(2 + 3) = 0$

Hence, $E_2$ is no EC.

- 1 -
13.2 The group law

On the set of L-valued points, $E(L)$ an algebraic operation "+" is defined. The geometric interpretation is given on the slides. The corresponding formulae are carried over to $E(C)$ over finite fields.

**Addition in $E(L)$:**

Let $P = (x_1, y_1), P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(L)$

i) $P + \mathcal{O} = \mathcal{O} + P = P$ ( $\mathcal{O}$ is the neutral element)

ii) $P + (-P) = (x_1, -y_1) + P = -P + P = P + (-P) = \mathcal{O}$

iii) If $P_1 \neq \pm P_2$, then $P_3 = (x_3, y_3) = P_1 + P_2$ is defined as

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

iv) If $P = -P$, then $2P = P + P = (x_3, y_3)$ is defined as

$$x_3 = \left(\frac{3x_1^2 + a}{2y}\right)^2 - 2x_1, \quad y_3 = \frac{3x_1^2 + a}{2y} (x - x_3) - y$$

**Theorem 13.2** $E(L, +)$ is an abelian group with neutral element $\mathcal{O}$.

**Proof:** Simply check

- $P_1 + P_2 \in E(L)$, $\mathcal{O}$-neutral element, $-P$ is inverse
- Associative law
- Commutative law
Example: $a = 0$, $b = 1$. ($y^2 = x^3 + ax + b$) over $\mathbb{F}_5$

$4 = -1C(4a^3 + 27b^2) \equiv 4(2,1) = 8 \equiv 3 \neq 0 \pmod{5}$

$E : y^2 = x^3 + 1$ is an EC over $\mathbb{F}_5$

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^2$</th>
<th>$x^3$</th>
<th>$x^3 + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: $x^2 \equiv (x^2)^2 \pmod{p}$

Now, look where $x^4 = x^3 + 1 \Rightarrow (2,1) \in E(\mathbb{F}_5)$

$E(\mathbb{F}_5) = \{(0,1), (0,4), (2,2), (2,3), (4,0), \infty\}$

$|E(\mathbb{F}_5)| = 6$

$G = (2,2)$ is a generator of $E(\mathbb{F}_5)$

$G + G = 2 \cdot G = (2,2) + (2,2) = (0,4) \neq \infty$

$G + G + G = 3 \cdot G = 2 \cdot G + G = (0,4) + (2,2) = (4,0) = -3G$

$4 \cdot G = -2G = (0,1)$

$5 \cdot G = -G = (2,3)$

$6 \cdot G = \infty = 2 \cdot 3 \cdot G$

Hence $E(\mathbb{F}_5)$ is a cyclic group of order 6

Example: $a = 1$, $b = 0$, $\mathbb{F}_{23}$ $\Delta \neq 0 \pmod{23}$

$|E(\mathbb{F}_{23})| = 24$

See slides
Group Order: \( \# E(k) \)

If \( k = \mathbb{F}_q = \mathbb{F}_p^m \), there are finitely many points in \( E(k) \).

\( \sigma \in E(k) \) always, hence \( \# E(k) \geq 1 \)

For any fixed \( \tau \in \mathbb{F}_q \), the equation \( Y^2 = x^3 + ax + b \) has at most 2 solutions, as \( \mathbb{F}_q \) is a field. Hence,

\[ \# E(k) \leq 2 \cdot q + 1 \]

Define \( \# E(k) = q + 1 - \tau, \tau \in \mathbb{F}_q \). \( \tau \) is called the trace of \( E \).

**Theorem 13.3 (Hasse, 1933)**

\[ |\tau| \leq 2 \sqrt{q} \]

**Remark:**

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

Hence, \( \# E(\mathbb{F}_q) \) is in the magnitude of \( q \).

b) Knowledge of \( \# E(\mathbb{F}_q) \) is important for cryptographic applications.

c) \( \# E(\mathbb{F}_q) \) may be determined by counting alg. (Schoof alg.)

or construct \( E(\mathbb{F}_q) \) with predetermined order (rank - multiplication) method.

In the previous examples:

a) \( \# E(\mathbb{F}_5) = 6 = 5 + 1 \Rightarrow \tau = 0 \)

b) \( \# E(\mathbb{F}_{23}) = 24 = 23 + 1 \Rightarrow \tau = 0 \)
13.3 The DLP on Elliptic Curves

For the construction of cryptosystems on $E(\mathbb{F}_q)$ we first have to rephrase the DLP for elliptic curves.

**Def.** Given an elliptic curve (EC) over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$, let $a = (P, Q) = n$ and let $Q = a \cdot P = (b P | b \in \mathbb{Z}_n)$. If $Q = a \cdot P$ then $a$ is called the discrete logarithm at $Q$ to the base $P$.

To determine $a \in \mathbb{Z}_n$ with $Q = a \cdot P$, if $Q$ and $P$ are given, is called the elliptic curve discrete logarithm problem (EC DLP).

It is easy to compute $a \cdot P = 2$ see $E_1$.

It can be done by the Double-and-Add algorithm.

The number of doublings is $\lceil \log_2(a) \rceil$ and $\sum a_i$ additions.

If $a = (a_0, a_1, a_2, \ldots, a_i)$.

Is it hard to solve the DLP (EC DLP)?

Consider algorithms and methods for the computation of DL.