13.1 Foundations and Definitions

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

If $K = \mathbb{F}_{p^k}$, then $p \geq 3$ in the following, p is prime.

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

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

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

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

the set of L-rational points on E.

$\mathcal{O}$ denotes the point at infinity, i.e., neutral element.

Remarks: 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 $\mathbb{R}$ $\quad a = -1, b = 0$

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

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

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

Hence, E_2 is no EC.

13.2 The group law

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

Addition in $E(L)$:

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

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

ii) $P + (x, -y) = (x, -y) + P = -P + P = P + (-P) = \mathcal{O}$

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 $P \neq -P$, then $2P = P + P = (x_3, y_3)$ is defined as

$$x_3 = \left(\frac{3x_2^2 + a}{2y}\right)^2 - 2x \,, \quad x_3 = \frac{3x^2 + a}{2y}(x - x_3) - y$$

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

Proof: "Simply" check

- $P_1 + P_2 \in E(L)$, $\mathcal{O}$ unit element, $-P$ is inverse
- associate law,
- commutative law

<u>Example</u> $a = 0, b = 1$ $(y^2 = x^3 + ax + b)$ over $\mathbb{F}_5$

$\Delta = -16(4a^3 + 27b^2) \equiv 4(2 \cdot 1) = 8 \equiv 3 \not\equiv 0 \pmod 5$

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

z	z^2	z^3	z^3+1
0	0	0	1
1	1	1	2
2	4	3	4
3	4	2	3
4	1	4	0

<u>Note</u>: $z^2 \equiv (p-z)^2 \pmod p$

<u>Now</u>: "look" where "$z_1^2 = z_2^3 + 1$" $\Rightarrow (z_2, z_1) \in E(L)$

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

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

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

$G + G = 2 \cdot G = (2,2) + (2,2) = (0,4) \neq \mathcal{O}$

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

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

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

$6 \cdot G = \mathcal{O}$ $(= 2 \cdot 3 \cdot G$

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

<u>Example</u>: $a = 1, b = 0, \mathbb{F}_{23}$ $\Delta \not\equiv 0 \pmod{23}$

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

see slides

Group Order : $\# E(K)$

If $K = \mathbb{F}_q = \mathbb{F}_{p^k}$, there are finitely many points in $E(K)$

$\mathcal{O} \in E(K)$ always, hence $\# E(K) \geq 1$

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

$$\# E(K) \leq 2 \cdot q + 1$$

Write $\# E(K) = q + 1 - t$, $t \in \mathbb{Z}$ $|t| \leq q$

t is called the <u>trace of E</u>.

<u>Theorem 13.3 (Hasse, 1933)</u>

$$|t| \leq 2\sqrt{q}$$

<u>Remarks</u> a) $q + 1 - 2\sqrt{q} \leq \# E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$

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 EC with prescribed order (complex-multiplication) method.

In the previous examples: a) $\# E(\mathbb{F}_5) = 6 = 5 + 1 \Rightarrow t = 0$

b) $\# E(\mathbb{F}_{23}) = 24 = 23 + 1 \Rightarrow t = 0$

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 $\operatorname{ord}(P) = n$ and let $Q \in \langle P \rangle = \{ bP \mid b \in \mathbb{Z}_n \}$
If $Q = a \cdot P$ then a is called the discrete logarithm of 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 (ECDLP)

It is easy to compute $a \cdot P$: $\to$ see Ex.
It can be done by the Double-and-Add algorithm.
The number of doublings is $\lceil \log_2(a) \rceil$ and $\sum_{i=0}^{t-1} a_i$ addings, if $a = (a_{t-1}, a_{t-2}, \dots, a_0)_2$

Is it hard to solve the DLP / ECDLP?
Consider algorithms and methods for the computation of DL.