13.2 The Group Law

On the set of L-rational points $E(L)$ an algebraic operation "+" is defined
Geometric interpretation: → slides
The corresponding formulae are carried over to E 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

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

<u>Theorem 13.2</u> $(E(L),+)$ is an Abelian group with unit element $\mathcal{O}$

<u>Proof</u>: "Simply" check

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

Example: $a = 0,\ b = 1 \quad (Y^2 = X^3 + aX + b)$ over $\mathbb{F}_5$

$\Delta = -16(4a^3 + 27b) \equiv 4(2 \cdot 1) = 8 \equiv 3 \pmod 5$

$E = x^3 + 1$ is an elliptic curve 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

Look, where "$z_1^2 = z_2^3 + 1$" $\Rightarrow (z_2, z_1) \in E(\mathbb{F}$

$E(\mathbb{F}_5) = \{(0,1), (0,4), (2,2), (2,3), (4,0), \mathcal{O}\} \quad |E(\mathbb{F}_5)| = 6$

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

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

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

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

$5 \cdot (2,2) = (0,1) + (1,2) = (2,3) = -G$

$6 \cdot (2,2) = \mathcal{O}$

Hence, $E(\mathbb{F}_5) \cong \mathbb{Z}_6$ cyclic group of order 6

Example: $a = 1,\ b = 0,\ \mathbb{F}_{23} \quad \Delta \not\equiv 0 \pmod{23} \quad |E(\mathbb{F}_{23})| = 24$

Group order : $\# E(K)$

If $K = \mathbb{F}_q$, $q = p^k$, there are only 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,

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

Write $\# E(K) = q + 1 - t$, $t \in \mathbb{Z}$, $|t| \leq q$.
t is called the trace of E.

Theorem 13.3 (Hasse, 1933)

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

Remarks :

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 point counting alg. (Schoof alg.), or construct EC with prescribed order (complex-multiplication) method.

In the previous example : $\# E(\mathbb{F}_5) = 6 = 5 + 1$, hence $t = 0$
$\# E(\mathbb{F}_{23}) = 24 = 23 + 1$, hence $t = 0$

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

<u>Def.</u>: Given an elliptic curve $E/\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$.
Let $\mathrm{ord}(P) = n$ and let $Q \in \langle P \rangle = \{bP \mid b \in \mathbb{Z}_n\}$
If $Q = a \cdot P$ then a is called the <u>discrete logarithm</u> 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 <u>elliptic curve discrete logarithm problem</u> (ECDL

It is easy to compute $a \cdot P$:

<u>Algorithm Double and Add</u>

Input: Point on elliptic curve P, $a = (a_t, \ldots, a_0)_2 \in \mathbb{N}$
Output: $a \cdot P \in E$

```
Q ← P
for (i = t-1 ; i ≥ 0 ; i--)
    Q ← 2Q
    if (a_i = 1)
        Q ← Q + P
    endif
end for
return Q
```

The number of doublings is $\lceil \log_2(a) \rceil$ and $\sum_{i=0}^{t-1} a_i$ addings.

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

Algorithms for solving DLP / ECDLP

- Generic alg. - applicable to arbitrary groups

a) Exhaustive search: Check for all $a = 0, \ldots, n-1$ whether $Q = a \cdot P$

Complexity $O(n)$: worst case: n computations

b) Babystep - Giantstep - Alg. (Shanks)

Let $m = \lceil \sqrt{n} \rceil$

There exist $q \in \mathbb{N}$ and $r \in \{0, \ldots, m-1\}$ s.t. $a = q \cdot m + r$

$\Rightarrow Q = a \cdot P = q \cdot m \cdot P + r \cdot P \iff Q - rP = q \cdot m \cdot P$

Compute all values $Q - r \cdot P$, $0 \leq r \leq m-1$ and store them

If $Q - r \cdot P = 0$, for some r, we've done (Babysteps)

Otherwise compute $m \cdot P$ and then successively $q \cdot m \cdot P$ and compare (Giantsteps)

Complexity: m Babysteps, m Giantsteps, m values to be stored

$\sim O(\sqrt{n})$ (memory & computing complexity)