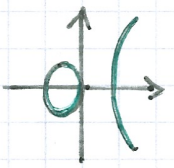
# Eigenes „Gesamtbild" CRYPTO1 – Ell. Kurven (EC) (O+I)

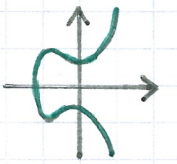
18/20/21/22.5.22

$E_{a,b} = \{(x,y) \in F^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ ist EC über Körper F, wobei $2^2 \cdot a^3 + 3^3 \cdot b^2 \neq 0$ und für die Vorlesung $F = \mathbb{Z}_p$, $p \in \mathbb{P}$, $p \geq 5$.

$E_{-1,0}$ bzw. $y^2 = x^3 - x$:



$E_{-1,1}$ bzw. $y^2 = x^3 - x + 1$:

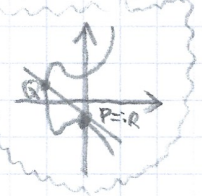


Definition der Gruppenoperation/Addition: $\overbrace{(x_1,y_1)}^{P} + \overbrace{(x_2,y_2)}^{Q} = \overbrace{(x_3,y_3)}^{-R}$:

**Fall 0:**

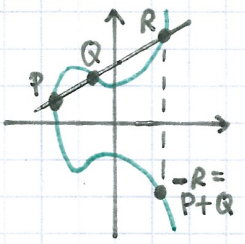
$P + \mathcal{O} = \mathcal{O} + P = P$

Sonderfall: wenn P Wendepkt., dann R=P selbiges, wenn Q Wendepkt.




($x_1 = x_2$, $y_1 \neq y_2$, $y_1 = 0 \vee y_2 = 0$ ist geometr. unmögl.!)

**Fall 1:**

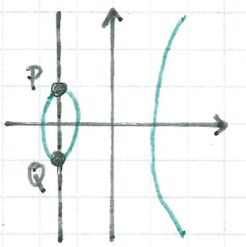



$x_1 \neq x_2$

$P + Q = -R$

$m = (y_2 - y_1)/(x_2 - x_1)$
$x_3 = m^2 - x_1 - x_2$
$y_3 = m(x_1 - x_3) - y_1$

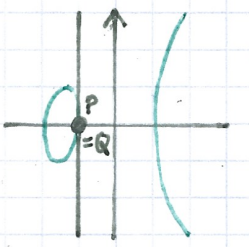
**Fall 2(a):**




$x_1 = x_2$
$0 \neq y_1 \neq y_2 \neq 0$

$P + Q = \mathcal{O}$

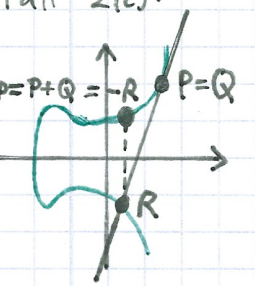
**Fall 2(b):**




$x_1 = x_2$
$y_1 = y_2 = 0$

$P + Q = \mathcal{O}$

**Fall 2(c):**




$x_1 = x_2$
$y_1 = y_2 \neq 0$

$P + Q = -R$

$m = (3x_1^2 + a)/(2y_1)$
$x_3 = m^2 - x_1 - x_2$
$y_3 = m(x_1 - x_3) - y_1$

## Quadratischer Twist:

Sei $E_{a,b}$ eine EC über Körper F (VL: $F = \mathbb{F}_p$) und $d \neq 0$ kein Quadrat in F.
Definiere den „Quadratischen Twist": $E_{a,b}^{(d)} := E_{d^2 a, d^3 b}$
Während $E_{a,b}$ und $E_{a,b}^{(d)}$ nicht isomorph über F sind, sind sie es über einer Körpererweiterung von F, in der es ein u mit $u^2 = d$ gibt, bspw. im algebraischen Abschluss von F (VL: $\overline{\mathbb{F}_p}$).
Wenn F ein endlicher Körper mit q Elementen (VL: $q \in \mathbb{P}$) ist, dann gilt $|E_{a,b}| + |E_{a,b}^{(d)}| = 2q + 2$, da man für jedes $x \in F$ genau 2 Punkte auf $E_{a,b}$ und/oder $E_{a,b}^{(d)}$ erhält (genaueres siehe Extrablatt).

Das Interessante ist, dass $E_{a,b}$ u. $E_{a,b}^{(d)}$ zwar eine unterschiedliche Arithmetik haben, die komplexe Analyse der Kurven aber dieselbe ist!

## Theorem von Hasse-Weyl / Hasse's theorem on elliptic curves:

...gibt eine obere und untere Abschätzung für die Anzahl der Punkte auf einer EC über einem endlichen Körper mit q Elementen (VL: $q \in \mathbb{P}$):
$|\,|E_{a,b}| - (q+1)\,| \leq 2 \cdot \sqrt{q}$ (d.h. EC $E_{a,b}$ hat $\approx q$ Elemente).

## ECDH:

$G \in E_{a,b}$ ist öffentlich

$A \xrightarrow{t_A \cdot G} B$

$A \xleftarrow{t_B \cdot G} B$

Geheimnis: $(t_A \cdot t_B) \cdot G$
DLP: $t_A = d\log_G(t_A \cdot G)$

Achtung!: EC ist additive Gruppe, daher Mal statt Hoch!

## ElGamal-Verschlüsselungsverfahren:

Alice's privater Schlüssel: $t_A \in \mathbb{N}$
Alice's öffentl. Schlüssel: $A = t_A \cdot G$, $A \in E_{a,b}$
Bob's Nachricht an Alice: $N \in E_{a,b}$
Allgemein bekannt: $G \in E_{a,b}$, $\text{ord}(G) = q$
Verschlüsseln: Wähle zufällig $r \in_R [2, q-2]$
$(r \cdot G,\ N + r \cdot A)$
Entschlüsseln: $N = (N + r \cdot A) - t_A \cdot r \cdot G$
klappt da $r \cdot A = r \cdot t_A \cdot G = t_A \cdot r \cdot G$