Prof. C. P. Schnorr Sommersemester 2017

Kryptographie

Blatt 4, 17.05.2017, Abgabe 24.05.2017

Aufgabe 1. Sei $E_{a,b}(\mathbb{K})$ elliptische Kurve. Zeige:

1. für alle $(\bar{x}, \bar{y}) \in E_{a,b}(\mathbb{K})$: $\mathrm{ord}(\bar{x}, \bar{y}) = 2$ gdw $\bar{x}^3 + a\bar{x} + b = 0$.
2. $E_{a,b}(\mathbb{K})$ zyklisch $\implies$ #Nullstellen von $x^3 + ax + b = 0$ ist ≤ 1.
3. $|E_{a,b}(\mathbb{K})|$ ist ungerade gdw $x^3 + ax + b$ keine Nullstelle in $\mathbb{K}$ hat.

Aufgabe 2. Sei q prim. Zeige:

1. $|E_{0,b}(\mathbb{Z}_q)| = q + 1$ für $q = 2 \bmod 3$, $b \in \mathbb{Z}_q^*$.
2. $|E_{a,0}(\mathbb{Z}_q)| = q + 1$ für $q = 3 \bmod 4$, $a \in \mathbb{Z}_q^*$.

Hinweis: **1.** $x \mapsto x^3$ ist Bijektion von $\mathbb{Z}_q$ für $q = 2 \bmod 3$.

2. Für $q = 3 \bmod 4$ gilt $-1 \notin (\mathbb{Z}_q^*)^2$ weil $\frac{q-1}{2}$ ungerade ist.

Aufgabe 3. Zeige : Alg. 3.34 (Handbook of Applied Kryptography) liefert $QR_p \ni x \mapsto \pm\sqrt{x} \in \mathbb{Z}_p^*$ für $p = 1 \bmod 4$, p prim, $x \in_R QR_p$ im Mittel in $O(\lg p)^4$ Bitoperationen. Begründe die Schritte 5-7 von Algorithm 3.34 für $s = 2$.

Punktzahl pro Aufgabe 5