

## Kryptographie

Blatt 5, 13.05.2005, Abgabe 20.05.2005

**Aufgabe 1.** Seien  $X_1, \dots, X_i, \dots \in_D \{0, 1\}$  unabh. Zufallsvariable mit  $\Pr_D[X_i = 1] = \varepsilon$ . Zeige für  $u := \min_i X_i = 1$  und  $k\varepsilon^{-1} \in \mathbb{N}$ :

1.  $0 < \text{Ws}[u \leq k\varepsilon^{-1}] = 1 - (1 - \varepsilon)^{k\varepsilon^{-1}} = 1 - e^{-k} + O(ke^{-k}\varepsilon)$ .
2.  $0 < e^{-\frac{1}{k}} - \text{Ws}[u > \varepsilon^{-1}/k] = O(e^{-\frac{1}{k}}\varepsilon)$ .

Benutze dass  $0 < e^{\pm 1} - (1 \pm \frac{1}{n})^n = O(\frac{1}{n})$ .

**Aufgabe 2.** Sei  $E_{a,b}(\mathbb{K})$  elliptische Kurve . Zeige:

1. für alle  $(\bar{x}, \bar{y}) \in E_{a,b}(\mathbb{K})$ :  $\text{ord}(\bar{x}, \bar{y}) = 2$  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  $\leq 1$ .
3.  $|E_{a,b}(\mathbb{K})|$  ist ungerade gdw  $x^3 + ax + b$  keine Nullstelle in  $\mathbb{K}$  hat.

**Aufgabe 3.** Sei  $q$  prim. Zeige:

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

*Hinweis:*  $x \mapsto x^3$  ist Bijektion von  $\mathbb{Z}_q$  für  $q = 2 \pmod{3}$ ,  $-1 \notin (\mathbb{Z}_q^*)^2$  für  $q = 3 \pmod{4}$ . 2. gilt für beliebige  $a \in \mathbb{Z}_q^*$ .

**Aufgabe 4.** Die Schnorr Signaturen  $(c_i, y_i)$  zur Nachricht  $m_i$  seien nach Vorschrift mit  $r_i \in \mathbb{Z}_q^*$  für  $i = 1, \dots, t$  zum Schlüssel  $x, h = g^x$  erzeugt. Zeige:

Kennt man zu  $(c_i, y_i, m_i)$   $i = 1, \dots, t$  die Koeffizienten  $a_0, \dots, a_t$  einer Gleichung  $\sum_{i=1}^t a_i r_i = a_0$  so erhält man  $x = \log_g h$  sofern  $\sum_{i=1}^t a_i c_i \neq 0$ .

*Hinweis:*  $g^{r_i} = g^{y_i} h^{-c_i}$ .