Prof. C. P. Schnorr Wintersemester 2008/09

Kryptographie

Blatt 5, 14.11.2008, Abgabe 21.11.2008

Aufgabe 1 Seien G_1, G_2 zyklische Gruppen der Ordnung q_1, q_2, $s := \mathrm{ggT}(q_1, q_2)$. Zeige $G_1^s \times G_2^s \subset G_1 \times G_2$ ist zyklische Gruppe der Ordnung $q_1 q_2 / s^2$.

Aufgabe 2 $x^3+ax+b \in \mathbb{K}[x]$ habe eine doppelte Nullstelle in $\mathbb{K}$, $\mathrm{char}(\mathbb{K}) > 3$. Zeige:

1. $4a^3 + 27b^2 = 0$, und die doppelte Nullstelle ist $\sqrt{-\frac{a}{3}}$.
2. Die übliche Punkte-Addition ist für $P_a = (\sqrt{-\frac{a}{3}}, 0)$ nicht erklärt.
3. $E_{a,b}(\mathbb{K}) - \{P_a\}$ ist abgeschlossen gegen die übliche Punkte-Addition.

Aufgabe 3 Seien $X_1, \ldots, X_i, \ldots \in_D \{0,1\}$ unabh. Zufallsvariable mit $\Pr_D[X_i = 1] = \varepsilon$. Zeige für $u := \min\{i \mid X_i = 1\}$ und $k\varepsilon^{-1} \in \mathbb{N}$:

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

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