Prof. C. P. Schnorr Wintersemester 2013/14

Kryptographie

Blatt 5, 13.12.2013, Abgabe 20.12.2013

Aufgabe 1.

$x^3 + ax + b \in \mathbb{K}[x]$ habe eine doppelte Nullstelle in $\mathbb{K}$, $\text{char}(\mathbb{K}) > 3$. 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 2. Seien $X_1, \ldots, X_i, \ldots$ unabh. Zufallsvariable über $\{0,1\}$ mit $\Pr_D[X_i = 1] = \varepsilon$. Zeige für $u := \min\{i \mid X_i = 1\}$ und $k\varepsilon^{-1} \in \mathbb{N}$:

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

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

Aufgabe 3. Ändere den Extraktionsalgorithmus $\text{AL}(\tilde{P}, h)$ zu $(P,V)_{DL}$ wie folgt ab: In Stufe 2 mache $k \cdot u$ neue Proben zum Auffinden einer zweiten 1 in der durch Stufe 1 fixierten Zeile.

Wie hängt die erwartete Laufzeit $E_{w_{\text{AL}}}|\text{AL}|$ von k ab? Für welches k wird sie minimal?

Punktzahl pro Aufgabe 5