Prof. C. P. Schnorr Sommersemester 2009

Gitter und Kryptographie

Blatt 10, 24.06.2009, Abgabe Mittwoch, 01.07.2009

Aufgabe 1. Konstruiere ein Beispiel NTRU–Schema mit $p = 3, q = 64, N = 7, \mathrm{d_g} = \mathrm{d_f} = 2$. Wähle f, g und berechne

$$f^{-1} \bmod p,\ f^{-1} \bmod q,\ h = f^{-1}g \bmod N.$$

Hinweis: Berechne $\mathrm{ggT}(f, X^N - 1)$ mit dem erweiterten ggT- Algorithmus.

Aufgabe 2. Sei $B = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathbb{R}^{(n+1)\times n}$.

Zeige: $\det(B^t B) = 1 + \sum_{i=1}^{n} a_i^2$.

Aufgabe 3. Sei $B = \mathrm{QR} \in \mathbb{R}^{m\times n}, n = hk$, primal–duale Basis zur Blockweite k. Zeige, dass unter **GSA** gilt

1. $1/q \le \gamma_k^{\frac{2}{k-1}}$

2. $\|b_1\|^2 \le \gamma_k^{\frac{n-1}{k-1}} (\det \mathcal{L})^{\frac{2}{n}}$.