

Gitter und Kryptographie

Blatt 10, 21.12.2007, Abgabe 11.01.2008

Aufgabe 1.

Sei $B = \begin{bmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ Na_1 & \cdots & Na_n & Ns \end{bmatrix}, B' = \begin{bmatrix} 1 & \cdots & 0 & \frac{1}{2} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & \frac{1}{2} \\ Na_1 & \cdots & Na_n & Ns \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{(n+1) \times (n+1)},$

$B'' = \begin{bmatrix} 1 & & & \frac{1}{2} \\ & \ddots & & \vdots \\ & & 1 & \frac{1}{2} \\ Na_1 & & Na_n & Ns \\ 0 & & 0 & 1 \end{bmatrix} \in \frac{1}{2}\mathbb{Z}^{(n+2) \times (n+2)}, 0 < s < \sum_{i=1}^n a_i.$

Zeige: $\det B = Ns, \det B' = N |s - \frac{1}{2} \sum_{i=1}^n a_i|, \det \mathcal{L}(B') < \det \mathcal{L}(B'') \leq \det B' \sqrt{1 + \frac{4}{n}}.$

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. Formuliere den LLL-Algorithmus zu gegebener Gram-Matrix $B^t B \in \mathbb{Z}^{n \times n}$

EINGABE $B^t B \in \mathbb{Z}^{n \times n}, 1/4 \leq \delta < 1$

AUSGABE $T \in GL_n(\mathbb{Z}),$ so dass BT LLL-reduziert ist.

Alle arithmetischen Schritte insbesondere die zur Berechnung der $\mu_{k,j}, \|\mathbf{b}_k^*\|^2$ sollen auf \mathbb{Z} operieren.

Aufgabe 4. Zeige: $\gamma_2^2 = \frac{4}{3}.$ $\mathcal{L}(R_2)$ für $R_2 = \sqrt{2} \begin{bmatrix} 1 & \\ 0 & \sqrt{3/4} \end{bmatrix}$ ist kritisch.