Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 4, 05.12.2012, Abgabe 12.12.2012

Aufgabe 1. Sei $N = pq, p > q > p/2$.

Gegeben seiq_0 und M, so dass $q_0 = q \bmod M$, $M \geq N^{\frac{1}{4}}$.

Zeige, dass man N in Pol–Zeit $(\log N)^{O(1)}$ zerlegen kann.

Hinweis: Beweis von Theorem 12 (Diss. May).

Berechne $x_0 = \frac{q-q_0}{M}$ in Pol. Zeit nach Theorem 7. Für welche f'_q, δ, β, c_N ?

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

Zeige $\det \mathbf{B}^t\mathbf{B} = 1 + \sum_{i=1}^{n} a_i^2$ für $n = 2, 3$.

Aufgabe 3. Sei $\mathbf{B}_{\alpha,c} \in \mathbb{R}^{(n+1)\times n}, c \geq 1$ die Primzahlbasismaitrix.

Zeige $rd(\mathcal{L}) = o(n^{-1/4})$ falls $M_{\alpha,c} \neq \phi,\ \alpha > 2\beta + 2$.

Hinweis: Folge dem Beweis von Theorem 6: Average Time Fast SVP and...