Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 4, 16.12.2015, Abgabe 20.01.2016

Aufgabe 1.

Sei $N = \prod_{i=1}^{k} \bar{p}_i^{e_i}$ mit k verschiedenen Primzahlen $\bar{p}_i$, $e_i \in \mathbb{N}$, $\bar{p}_i^{e_i} \neq 2$.

Zeige, dass $X^2 = 1 \mod N$ genau 2^k viele Lösungen hat. Benutze dass $\mathbb{Z}_N^* \cong \mathbb{Z}_{\bar{p}_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{\bar{p}_k^{e_k}}^*$, $QR_N \cong QR_{\bar{p}_1^{e_1}} \times \cdots \times QR_{\bar{p}_k^{e_k}}$. $\mathbb{Z}_{\bar{p}_i^e}^*$ ist zyklisch für $\bar{p}_i \neq 2$.

Aufgabe 2. Beweise Theorem 14 (Howgrave-Graham) des Kapitels 3 der Dissertation von Alexander May. Übertrage und vervollständige den Beweis von Theorem 5.

Aufgabe 3. Sei $\mathbf{B} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \vdots \\ 0 & \cdots & 1 \\ a_1 & \cdots & a_n \end{bmatrix} \in \mathbb{R}^{(n+1)\times n}$. Zeige $\det \mathbf{B}^t\mathbf{B} = 1 + \sum_{i=1}^{n} a_i^2$.

Hinweis: $\mathbf{B}^t\mathbf{B} = \begin{bmatrix} 1+a_1^2 & a_1a_2 & \cdots & a_1a_n \\ a_1a_2 & 1+a_2^2 & \cdots & a_2a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1a_n & a_2a_n & \cdots & 1+a_n^2 \end{bmatrix}$ hat die Eigenvektoren

$\mathbf{x}_1 = (a_1, a_2, ..., a_n)^t$ zum Eigenwert $\lambda_1 = 1 + a_1^2 + \cdots + a_n^2$ und

$\mathbf{x}_k = (-a_k, 0, .., 0, a_1, 0, ..., 0)^t$ (mit a_1 an der k-ten Stelle) zum Eigenwert $\lambda_k = 1$ für $k = 2, 3, ..., n$. Es gilt $\mathbf{B}^t\mathbf{B}[\mathbf{x}_1, ..., \mathbf{x}_n] = [\lambda_1\mathbf{x}_1, .., \lambda_n\mathbf{x}_n]$,

$\det(\mathbf{B}^t\mathbf{B}) = \prod_{i=1}^{n} \lambda_i$ (bitte alles prüfen)

5 Punkte pro Aufgabe