Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 5, 20.01.2016, Abgabe 03.02.2016

Aufgabe 1. Sei $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$, $\mathbf{b} \sim (u, v)$. Zeige für $v' \in \mathbb{Z}$, dass $||\mathbf{b} - v'\mathbf{N}||^2 \geq \ln uv + \hat{z}^2_{\mathbf{b}-v'\mathbf{N}}$ (mit Gleichheit für quadratfreies uv) für $\hat{z}_{\mathbf{b}-v'N} := N^c(\ln \frac{u}{vN^{v'}}) = N^c(\ln \frac{u}{v} - v' \ln N)$, die letzte Koordinate von $\mathbf{b} - v'\mathbf{N}$.
Hinweis : Modifiziere den Nachweis von Fact 1.

Aufgabe 2. Sei $\mathbf{b} \in \mathcal{L}(\mathbf{B}_{n,c})$, $\mathbf{b} \sim (u, v)$. Ferner habe $\mathbf{b} - v'\mathbf{N}$ mit $v' \in \mathbb{Z} \setminus \{0\}$ minimale Länge in $\mathcal{L}(\mathbf{N}, \mathbf{B}_{n,c})$.
Zeige: $\lambda_1^2(\mathcal{L}(\mathbf{N}, \mathbf{B}_{n,c})) > (2c-1)\ln N + \hat{z}^2_{\mathbf{b}-v'\mathbf{N}}$ mit "$\approx$ " für quadratfreies uv.
Hinweis : Folge dem Beweis von Lemma 2, aber benutze die Behauptung von Aufgabe 1 statt Fact 1.

D.h. in der unteren Schranke zu λ_1^2 von $\mathcal{L}(\mathbf{B}_{n,c})$ nach Lemma 2 wird $2c \ln N$ erniedrigt zu $(2c-1)\ln N$, denn wegen $u - vN^{v'} \approx o(u)$ gilt $\ln v = \ln u - v' \ln N + o(1)$, aber $\hat{z}^2_{\mathbf{b}}$ erhöht sich auf $\hat{z}^2_{\mathbf{b}-v'\mathbf{N}}$.

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

$$\mathbf{B}_{n,c} = \begin{bmatrix} \sqrt{\ln p_1} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \sqrt{\ln p_n} \\ N^c \ln p_1 & \cdots & N^c \ln p_n \end{bmatrix} \quad c = (\ln N)^\beta \geq 1,\ p_n = (\ln N)^\alpha$$

Zeige: $rd(\mathcal{L}) = o(n^{-1/4})$ falls $\alpha > 2\beta + 2$ und

$$M_{n,c} = \left\{ (u, v) \in \mathbb{N}^2 \;\middle|\; \begin{array}{l} |u - v| = 1,\ N^c/2 \leq v \leq N^c \\ u, v \text{ are } p_n\text{-smooth} \end{array} \right\} \neq \emptyset.$$

Dabei ist $rd(\mathcal{L})$ definiert durch $\lambda_1^2 = \gamma_n rd(\mathcal{L})^2 (\det(\mathcal{L}))^{2/n}$
Hinweis : Beweis von Theorem 4 in Factoring Integers by CVP Algorithms.

Punktzahlen: 5, 6, 8