

Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 1, 24.10.2012, Abgabe 31.10.2012

Entnehme γ_n der Tabelle 2.2.2, Seite 20 des Skripts ([http://mi.informatik.uni-frankfurt.de/ Lecture Notes](http://mi.informatik.uni-frankfurt.de/Lecture%20Notes))

Entnehme \mathbb{D}_n $n = 3, 4, 5$ und \mathbb{E}_8 der Seite 7 des Skripts.

Entnehme R_8 der Seite 21 des Skripts.

Aufgabe 1. Sei $\mathcal{L}_n = \mathcal{L}(\mathbb{D}_n)$ für $n = 3, 4, 5$ $\mathcal{L}_8 = \mathcal{L}(\mathbb{E}_8)$. Gib Vektoren $\mathbf{b} \in \mathcal{L}_n$ so an, dass

$$\|\mathbf{b}\|^2 = \gamma_n(\det \mathcal{L}_n)^{\frac{2}{n}} \quad \text{für } n = 3, 4, 5, 8 .$$

Prüfe diese Gleichungen. Wegen $\|\mathbf{b}\| = \lambda_1(\mathcal{L}_n)$ sind die \mathcal{L}_n Gitter maximaler Dichte Δ , also **kritische** Gitter.

Aufgabe 2. Sei $R_n \in \mathbb{R}^{n \times n}$ die Untermatrix der ersten n Zeilen und Spalten von R_8 . Zeige für $n = 4, 5, 6, 7, 8$:

$$\|\mathbf{b}_1\|^2 = 2 = \gamma_n(\det R_n)^{\frac{2}{n}} .$$

Aufgabe 3. Zeige $\lambda_1(\mathcal{L}(R_n))^2 = 2$ für $n = 1, \dots, 8$. Beweise Lemma 2.2.3. Damit haben die Gitter $\mathcal{L}(R_n)$ maximale Dichte Δ .