Prof. C. P. Schnorr Wintersemester 2014/15

Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 1, 22.10.2014, Abgabe 5.11.2014

Entnehme γ_n der Tabelle 2.2.2, Seite 21 des Skripts zur Vorlesung Gitter und Kryptographie. Entnehme $\mathbf{R}_8$ der Seite 21 des Skripts.

Aufgabe 1. Sei $\mathbf{R}_n \in \mathbb{R}^{n\times n}$ die Untermatrix der ersten n Zeilen und Spalten von $\mathbf{R}_8$. Zeige für $n = 4, 5, 6, 7, 8$: $\|\mathbf{b}_1\|^2 = 2 = \gamma_n(\det \mathbf{R}_n)^{\frac{2}{n}}$.

Aufgabe 2. Zeige $\lambda_1(\mathcal{L}(\mathbf{R}_n))^2 = 2$ für $n = 1, \ldots, 8$. Beweise Lemma 2.2.3 des Skripts. Damit haben die Gitter $\mathcal{L}(\mathbf{R}_n)$ maximale Dichte $\triangle$.

Aufgabe 3. Behandle den Fall, dass $p(x)$ nicht monisch ist, $p_d \neq 1$, nach Remark 1, Seite 21 (Copp.). Zeige, dass das Gitter zu $C_1' = C_1 \cup \{x^d\}$ die Dim. $d+1$ und die Determinante $\leq N^{-1}B^{d(d+1)/2}$ hat. Beachte, dass $\mathrm{ggT}(p_0, \cdots, p_d, N) = 1$.

Aufgabe 4. 1.) Beweise Kor. 4.1.5 des Skripts aus Satz 4.1.4 und Lemma 4.1.2. 2.) Zeige, dass für jede LLL–Basis gilt $\|\mathbf{b}_1\|/\lambda_1 \leq \alpha^{\frac{n-1}{4}}/(\mathrm{rd}(\mathcal{L})\sqrt{\gamma_n})$. Dabei sei $\mathrm{rd}(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det \mathcal{L})^{1/n})$ die relative Dichte des Gitters $\mathcal{L}$.

Aufgabe 5. Beweise Remark 2, Seite 22. Zeige, dass man in der enabling condition $c_1(d)(\det L_1)^{\frac{1}{d+1}} < \frac{1}{d+1}$ die rechte Seite $\frac{1}{d+1}$ durch $\frac{1}{\sqrt{d+1}}$ ersetzen kann. Die Schranke für B erhöht sich um den Faktor $(d+1)^{\frac{1}{d}}$.

5 Punkte pro Aufgabe