Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 2, 07.11.2012, Abgabe 14.11.2012

Aufgabe 1. 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 $\mathcal{L}$.

Zu D. Coppersmith: Finding small solutions of small degree polynomials.

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

Aufgabe 3. 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 $(d+1)^{\frac{1}{d}}$.