Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 2, 11.11.2015, Abgabe 25.11.2015

Aufgabe 1. Vergleiche die Dichte $\triangle$ folgender Untergitter des Leech Gitters $\mathcal{L}(\mathbf{B}_{24})$: $\mathbf{B}_{22} = \{\mathbf{B}_{24}\mathbf{x} \mid x_{23} = x_{24} = 0\}$, $\Lambda_{22} = \mathcal{L}(\mathbf{B}_{22})$,

$\overline{\mathbf{B}}_{22} = \{\mathbf{z} = \mathbf{B}_{24}\mathbf{x} \mid z_{21} = z_{22} = z_{23}\}$, $K_{22} = \mathcal{L}(\overline{\mathbf{B}}_{22})$.

$\hat{\mathbf{B}}_{22} = \{\mathbf{z} = \mathbf{B}_{24}\mathbf{x} \mid z_{22} = z_{23} = 0\}$, $F_{22} = \mathcal{L}(\hat{\mathbf{B}}_{22})$.

Zeige $\triangle(K_{22}), \triangle(F_{22}) > \triangle(\Lambda_{22})$.

`Hinweis:` $\triangle(K_{22})/\triangle(\Lambda_{22}) = rd(K_{22})/rd(\Lambda_{22})$ und $rd(\mathcal{L}) = \lambda_1/(\sqrt{\gamma_n}(\det \mathcal{L})^{1/n})$ sichert dass $\triangle(K_{22})/\triangle(\Lambda_{22}) = (\det \Lambda_{22}/\det K_{22})^{1/22}$. Es folgt $\triangle(\Lambda_{22}) < \triangle(K_{22})$ für das ab Dimension 1 iterativ geschichtete Gitter Λ_{22}.

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

5 Punkte pro Aufgabe