Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 4, 06.05.2016, Abgabe Freitag, 13.05.2016

Aufgabe 1. Sei $\mathbf{B}_{24} = \mathbf{R}_{24} = [\mathbf{r}_1, \ldots, \mathbf{r}_{24}]$ die GNF des Leech-Gitters.
Zeige $\lambda_1^2(\mathcal{L}(\mathbf{R}_{24})) = 4$ mit der Beweismethode zu Lemma 2.2.3, Teil 2.
Hinweis: Für $\mathbf{r} := \sum_{i=1}^{23} t_i \mathbf{r}_i \in \mathcal{L}(\mathbf{R}_{23})$, $t_{24} \in \mathbb{Z}$, $\widetilde{\mathbf{r}} := \mathbf{r}_{24} - \pi_{24}(\mathbf{r}_{24}) \in \mathrm{span}(\mathbf{R}_{23})$ gilt $\mathbf{R}_{23}^t \widetilde{\mathbf{r}}_{24} \in \mathbb{Z}^{23}$, $||\widetilde{\mathbf{r}}||^2 = 4 - \frac{1}{8}$. Es folgt
$||\mathbf{r} + t_{24}\mathbf{r}_{24}||^2 = ||\mathbf{r} + t_{24}\widetilde{\mathbf{r}}||^2 + ||t_{24}\pi_{24}(\mathbf{r}_{24})||^2 \in (4 + t_{24}^2(-1/8 + 1/8))\mathbb{N}$.
$\lambda_1^2(\mathcal{L}(\mathbf{R}_{23})) = 4$, $\mathbf{R}_{23}^t \mathbf{R}_{23} \in 4\,\mathbb{Z}^{23\times 23}$, $||\mathbf{r}_i||^2 \in 4\,\mathbb{N}$ sind schon gezeigt.

Aufgabe 2 Die geschichteten Gitter Λ_n der Dimension n mit $\lambda_1^2(\Lambda_n) = 4$ haben nach Conway, Sloane Table 6.1 für $n = 4, 8, 12, 16, 20, 24$ Determinante $\det(\Lambda_n) = 8, 16, 32, 16, 8, 1$ und nach Table 1.2 die zentrierte Dichte $\delta = 1/\det(\Lambda_n) = 1/8, 1/16, 1/32, 1/16, 1/8, 1$. (In Table 6.1 ist $\lambda_n = \det(\Lambda_n)^2$)
Zeige: dies sind auch die δ der $\mathcal{L}(\mathbf{R}_n)$ der Untermatrizen $\mathbf{R}_n$ der ersten n Zeilen und Spalten der GNF des Leech–Gitter für $n = 4, 8, \ldots, 24$.

Aufgabe 3. Sei p Primzahl mit $p = 1 \bmod 4$, $i \in \mathbb{Z}$ und $i^2 = -1 \mod p$ und $\mathcal{L}_p$ das Gitter $\mathcal{L}_p = \{(a, b)^t \in \mathbb{Z}^2 : a - ib = 0 \mod p\}$. Zeige:

1. $\det \mathcal{L}_p = p$, und $\lambda_1^2(\mathcal{L}_p) = p$
2. Löse $269 = a_0^2 + a_1^2$ mit $a_0, a_1 \in \mathbb{N}$ mittels Gauss-Reduktion.

Hinweis: Für $(a, b)^t \in \mathcal{L}_p$ gilt $a^2 + b^2 = 0 \mod p$, ferner $\lambda_1^2 \le \sqrt{\frac{4}{3}} \det \mathcal{L}_p$.

Punktzahl 5 pro Aufgabe