Gitter und Kryptographie

Blatt 5, 25.11.2005, Abgabe 02.12.2005

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

1. $\det \mathcal{L}_p = p$,
2. Für den kürzesten Vektor $(a_0, b_0)^t \in \mathcal{L}_p \backslash \{\mathbf{0}\}$ gilt: $p = a_0^2 + b_0^2$,
3. Löse $269 = a_0^2 + a_1^2$ mit $a_0, a_1 \in \mathbf{N}$ mittels Gauss-Redukton.

Hinweis: Für $(a,b)^t \in \mathcal{L}_p$ gilt $a^2 + b^2 = 0 \mod p$.

Aufgabe 2. Seien $\mathcal{L}' \subset \mathcal{L}$ Gitter. Zeige die Äquivalenz folgender Aussagen:

1. $\mathrm{span}(\mathcal{L}') \cap \mathcal{L} = \mathcal{L}'$.
2. Jede Basis von $\mathcal{L}'$ ist zu einer Basis von $\mathcal{L}$ erweiterbar.

Hinweis : Kap. 1.3 Skript

Aufgabe 3. Zeige, dass D_4 und $\mathcal{L}^{(4)}$ isometrisch sind. Transformiere die gegebenen Basen in isometrische Basen (siehe Skript S.7, S 24).

Aufgabe 4. Berechne die Dichte $\triangle$ der dichtesten bekannten Gitter der Dimension $2 \le n \le 8$ und $180 \le n \le 512$ und vergleiche sie mit der existentiellen Minkowski-Schranke $\triangle \ge \sum_{k=1}^{\infty} k^{-n} 2^{-n+1} \approx 2^{-n+1}$.

Benutze z.B. R_n für $2 \le n \le 8$ und für $180 \le n \le 512$ die Angabe $\log_2 \delta$ in Table 1.3 (Conway Sloane).