3. Übung Elementare Algorithmen in der Algebra

Priv. Doz. Dr. G. Nebe **(SS 00)**

Aufgabe 10. Algorithmus 2.15 führt die Berechnung einer rationalen Approximation einer modulo N bekannten Zahl c auf die Bestimmung eines kleinen "Minimalpolynoms" (nicht normiert, vom Grad 1) von c zurück. Verallgemeinern Sie diese Strategie für beliebige Grade:
Gegeben: eine Zahl $c \in \mathbb{Z}$, $n, N \in \mathbb{N}$.
Gesucht: $a_0, \ldots, a_n \in \mathbb{Z}$ mit $\sum_{i=0}^{n} a_i^2 \neq 0$ minimal, so dass $\sum_{i=0}^{n} a_i c^i \equiv 0 \pmod{N}$.
Bestimmen Sie ein kleines Minimalpolynom vom Grad 2 für $c \equiv 280182 \pmod{5^8}$.
(Hinweis: Mit readlib(lattice); erhält man eine Funktion "lattice" in MAPLE, die den LLL-Algorithmus zum Finden kurzer Vektoren in Gittern durchführt.)

Aufgabe 11. Sei L ein Gitter im Euklidischen Raum (V, Φ). Ein Vektor $v \in L$ heißt *primitiv*, falls $a^{-1}v \notin L$ für alle $1 \neq a \in \mathbb{N}$.
Zeigen Sie, dass $v \in L$ genau dann primitiv ist, wenn man v zu einer Gitterbasis von L ergänzen kann.
Sei $v \in L$ primitiv, $\pi : V \to v^{\perp}$ die Orthogonalprojektion auf $v^{\perp}$ und $L' := \pi(L)$.
Zeigen Sie, dass $det(L') = det(L)/\Phi(v, v)$.
Sind $v_2, \ldots, v_n \in L$, so dass $(\pi(v_2), \ldots, \pi(v_n))$ eine Gitterbasis von L' ist, dann ist $(v, v_2, \ldots, v_n)$ eine Gitterbasis von L.

Aufgabe 12. Geben Sie ein Beispiel eines 2-dimensionalen Gitters an, für welches in der Hermite Ungleichung Gleichheit gilt.

Aufgabe 13. Ersetzt man den Parameter $3/4$ in der Definition einer LLL-reduzierten Basis (3.10 (b)) durch einen Parameter $\alpha \in (1/4, 1)$, so gelten analoge Aussagen wie in Satz 3.11 (i), (ii), (iii), mit $\beta := 4/(4\alpha - 1)$ anstelle von 2.

Abgabe: Donnerstag, den 4.5.00, in der Übung 12:30 Uhr im kl. physik. Hörsaal