TECHNISCHE UNIVERSITÄT BERLIN WS06/07
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr.F. Heß
WM: Dipl.-Math. M. Wagner
`www.math.tu-berlin.de/~hess/krypto-ws2006`

13. Übung Kryptographie

1. Aufgabe Lineare Unabhängigkeit (4 Punkte)

Sei Λ ein Gitter im $\mathbb{R}^n$ und $b_1, \ldots, b_m \in \Lambda$ linear unabhängig über $\mathbb{Z}$. Zeige, daß $b_1, \ldots, b_m$ dann auch linear unabhängig über $\mathbb{R}$ sind. Beweise oder widerlege diese Aussage für den Fall, daß Λ nur ein $\mathbb{Z}$-Modul in $\mathbb{R}^n$ ist.

2. Aufgabe Fortsetzung von Basen (4 Punkte)

Beweise die folgende Aussage: Sei Λ ein Gitter im $\mathbb{R}^n$ und $b_1, \ldots, b_m \in \Lambda$ linear unabhängig. Gilt $(\sum_i \mathbb{Q}b_i) \cap \Lambda = \sum_i \mathbb{Z}b_i$, so läßt sich $b_1, \ldots, b_m$ zu einer Basis von Λ vervollständigen.

3. Aufgabe Einheiten im NTRU-Ring (4 Punkte)

Seien $n, q \in \mathbb{Z}^{>0}$ und $R := (\mathbb{Z}/q\mathbb{Z})[X]/(X^n - 1)$. Ein Element $f \in R$ schreiben wir als $f = [f_0, ..., f_{n-1}]$ mit $f_i \in \mathbb{Z}\ q\mathbb{Z}$. Betrachte die Vorschrift

$$\Phi : R \longrightarrow (Z/q\mathbb{Z}), \quad [f_0, ..., f_{n-1}] \longmapsto \sum_{i=0}^{n} f_i.$$

Zeige, dass Φ ein wohldefinierter surjektiver Ringhomomorphismus ist und beweise oder widerlege durch ein Gegenbeispiel folgende Aussage: $f \in R^\times \Leftrightarrow \Phi(f) \in (\mathbb{Z}/q\mathbb{Z})^\times$

4. Aufgabe Praktische Aufgabe (8 Punkte)

Implementieren Sie in KASH3 einen Algorithmus der für eine Matrix $M \in \mathbb{Z}^{n\times m}$ die Hermite-Normalform berechnet.