TECHNISCHE UNIVERSITÄT BERLIN Wintersemester 2004/ 2005
Fakultät II – Institut für Mathematik
Dozent: Prof. Dr. F. HESS
WM: M. WAGNER
www.math.tu-berlin.de/~hess/krypto2

2. Übung Kryptographie II

1. Aufgabe Lineare Unabhängigkeit (6 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 (6 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 Kürzeste Vektoren (4 Punkte)

Finde die kürzesten Vektoren des von den folgenden Spalten erzeugten $\mathbb{Z}$-Moduls:

$$\begin{pmatrix} 2 & -2 & 6 \\ -1 & 2 & -3 \\ 3 & 0 & 12 \end{pmatrix}.$$

Gesamt: 16 Punkte