RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 4 / 06. November 2012

AUFGABE 1:
Übung 39 im Skript: Sei $n \geq m$ und $A \in \mathbb{Z}^{m \times n}$ eine ganzzahlige $m \times n$-Matrix mit linear unabhängigen Zeilenvektoren. Zeigen Sie, dass die Menge

$$L = \{\mathbf{x} \in \mathbb{Z}^{n \times 1} \mid A\mathbf{x} = \mathbf{0}\}$$

ein Gitter L mit Gitterdimension $\dim(L) = n - m$ ist.

AUFGABE 2:
Gegeben sei ein Gitter L mit Basis

$$B = \begin{pmatrix} 24 & 14 \\ 9 & 5 \end{pmatrix}.$$

Berechnen Sie mit Hilfe des Gauß-Algorithmus eine reduzierte Basis. Was sind die sukzessiven Minima von L? Was ist die Determinante von L? Durch welche unimodulare Transformation kann B in die vom Gauß-Algorithmus berechnete Basis umgewandelt werden?

AUFGABE 3:
Die Menge

$$L = \{(x_1, x_2) \in \mathbb{Z}^2 \mid 2x_1 - 3x_2 \equiv 0 \bmod 5\}$$

ist ein Gitter. Geben Sie eine Basis B für das Gitter L an und beweisen Sie, dass B eine Basis für L ist.