RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann, Enrico Thomae

**Präsenzübungen zur Vorlesung**

# Kryptanalyse

**WS 2010/2011**

Blatt 4 / 03. November 2010

**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:**
Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Lösen Sie die Polynomgleichung $f(x) = 0 \bmod N$ mittels Linearisierung und Lösen eines SVPs. Welche Schranke erhalten Sie für die Größe der Lösung?

**AUFGABE 4:**
Für $n > 2$ sei $\gcd(a_1, \ldots, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$. Zeigen Sie, dass man ganze Zahlen $u_1, u_2, u_3 \in \mathbb{Z}$ berechnen kann mit

$$u_1 a_1 + u_2 a_2 + u_3 a_3 = \gcd(a_1, a_2, a_3).$$

**AUFGABE 5:**
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.