



Präsenzübungen zur Vorlesung

Kryptanalyse

WS 2009/2010

Blatt 4 / 25. November 2009

AUFGABE 1:

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:

Für $n > 2$ sei $\gcd(a_1, \dots, a_n) = \gcd(\gcd(a_1, \dots, a_{n-1}), a_n)$. 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 4:

Sei $N \in \mathbb{N}$ und $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. Lösen Sie die Polynomgleichung $f(x) = 0 \pmod N$ mittels Linearisierung und Lösen eines SVPs. Welche Schranke erhalten Sie für die Größe der Lösung?