**TECHNISCHE UNIVERSITÄT BERLIN** WS 2008-2009
**Fakultät II – Institut für Mathematik**
Dozent: Prof. Dr. Michael Pohst
Assistent: Osmanbey Uzunkol Abgabe: 04.02.2009
`www.math.tu-berlin.de/~kant/algebra2-ws2008` in der Übung

# 12. Übung Algebra II

(Gitter und LLL-Algorithmus)

---

## 1. Aufgabe

Finden Sie die kürzesten Vektoren des von den Zeilen der folgenden Matrix erzeugten $\mathbb{Z}$-Moduls:

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

**(6 Punkte)**

## 2. Aufgabe

Berechnen Sie in der Vorlesung definierte Hermitische Konstante $\gamma_k^k$ für $k = 2$.

**(3 Punkte)**

## 3. Aufgabe

(a) Es seien $F = \mathbb{Q}(\rho)$ ein Körper. Zeigen Sie, dass für $x \in \mathbb{Z}[\rho] \subseteq \mathcal{O}_F$ genau dann $||x||^2 = M_1$ gilt, falls $x$ eine Einheitswurzel ist, wobei $M_1$ und $\mathcal{O}_F$ wie in der Übung definert sind.

(b) Bestimmen Sie für $m \in \mathbb{Z}$ alle $x \in \mathbb{Z}[\sqrt{m}]$, $m$ kein Quadrat, mit $||x||^2 \leq \max(2, |m|)$. (Dabei ist $||x||^2 = |x^{(1)}|^2 + |x^{(2)}|^2$ für die Bilder $x^{(1)}, x^{(2)}$ (Konjugierte) von $x$ unter $\mathrm{Gal}(\mathbb{Q}(\sqrt{m})/\mathbb{Q})$. )

**(8 Punkte)**

## 4. Aufgabe

Wir nennen eine Folge $(b_1, b_2, \cdots, b_n)$ von positiven ganzen Zahlen **superincreasing**, falls für alle $i$, $2 \leq i \leq n$, die Ungleichung $b_i > \sum_{j=1}^{i-1} b_j$ gilt.

**Superincreasing subset sum Problem** ist zu gegebenem $s \in \mathbb{Z}$ ein Vektor $(x_1, x_2, \cdots, x_n)$ mit $\sum_{i=1}^{i=n} x_i b_i = s$ zu finden, wobei $x_i \in \{0, 1\}, 1 \leq i \leq n$ ist.

(a) Erklären Sie, wie man **superincreasing subset sum Problem** effizient lösen kann (**Hinweis**: mittels der Gittertheorie).

(b) Lösen Sie folgendes superincreasing subset sum Problem:

$$2x_1 + 5x_2 + 9x_3 + 21x_4 + 45x_5 + 103x_6 + 215x_7 + 450x_8 + 946x_9 = 1236.$$

Das **Merkle-Hellman Knapsack** Public-Key Kryptosystem basiert auf superincresing subset sum Problem.

**Schlüsselerzeugung für Verschlüsselungsfunktion:**

- Fixiere eine positive Zahl $n$.
- Wähle eine superincreasing Folge $(b_1, b_2, \cdots, b_n)$ und $M$ mit $M > b_1 + b_2 + \cdots + b_n$.
- Wähle eine zufällige Zahl $W$, $1 \leq W \leq M - 1$ mit $\text{ggT}(W, M) = 1$.
- Wähle eine zufällige Permutation $\pi$ von Zahlen $\{1, 2, \cdots, n\}$.
- Berechne $a_i \equiv W b_{\pi(i)} (\text{mod } M)$ für $i = 1, 2, \cdots, n$.
- Public-Key ist $(a_1, a_2, \cdots, a_n)$ und Private-Key ist $(\pi, M, W, (b_1, b_w, \cdots, b_n))$.

**Verschlüsselungsfunktion:**

Zusammenfassung: $B$ verschlüsselt eine Nachricht $m$, welche von $A$ entschlüsselt wird.

- Erhalte den Public-Key $(a_1, a_2, \cdots, a_n)$ von $A$.
- Representiere die Nachricht $m$ als binäre Folge von Länge $n$, $m = m_1 m_2 \cdots m_n$.
- Berechne $c = m_1 a_1 + m_2 a_2 + \cdots + m_n a_n$.
- Sende die verschlüsselte Nachricht $c$ an $A$ zu.

**Entschlüsselungsfunktion:**

- Berechne $d \equiv W^{-1} c (\text{mod } M)$.
- Löse das superincreasing subset sum Problem um die Zahlen $r_1, r_2, \cdots, r_n, r_i \in \{0, 1\}$ zu finden, so dass $d = r_1 b_1 + r_2 b_2 + \cdots + r_n b_n$ gilt.
- Die Nachrichtenbits sind $m_i = r_{\pi(i)}$, $i = 1, 2, \cdots, n$.

(c) Zeigen Sie, dass die Entschlüsselungsfunktion die ursprüngliche Nachricht $m$ wiederfindet.

(d) Es sei $(12, 17, 33, 74, 157, 316)$ von $A$ gewählter superincreasing Folge mit $M = 737$, $W = 635$ und die Permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 2 & 5 & 4 \end{pmatrix}$. Finden Sie die Public- und Private-Key von $A$.

(e) Verschlüsseln Sie die Nachricht $m = 101101$ mit von $(d)$ gefundenem Public-Key.

(f) Entschlüsseln Sie die Chiffretext $1605$ mit $(d)$ gefundenem Private-Key.

**(3+10 Punkte)**