Lösungen zu den Aufgaben der VL Kryptographie II

Unsere Lösungen zu den Aufgaben,
möglicherweise „quick and dirty“

19. November 2004

Übungsblatt 1

1. Aufgabe

Um die Smith-Normalform (kurz **SNF**) zu berechnen benötigt man u.a. folgende Aussage:

Lemma 1 *Für gegebene* $a_1, \ldots, a_n \in \mathbb{Z}$ *gibt es ein* $U \in \mathrm{GL}(n, \mathbb{Z})$ *mit* $c := \mathrm{ggT}(a_1, \ldots, a_n)$ *und*

$$(a_1, \ldots, a_n) \cdot U = (c, 0, \ldots, 0)$$

Als Beispiel für eine SNF wollen wir die SNF von

$$A := \begin{pmatrix} 12 & 6 & 21 & 9 \\ 19 & 6 & 0 & 21 \\ 2 & 5 & 1 & 17 \\ 1 & 1 & 0 & 13 \\ 63 & 22 & 11 & 15 \end{pmatrix}$$

berechnen. Dazu bilden wir für das Tupel $(12, 6)$ die Matrix

$$U_1 := \begin{pmatrix} 12 & 6 \\ 1 & 1 \end{pmatrix}$$

mit $\det U_1 = 6 = \mathrm{ggT}(12, 6)$ und erweitern U_1 zu einer Matrix

$$U_2 := \begin{pmatrix} 12 & 6 & 21 \\ 1 & 1 & 0 \\ \frac{-va_1}{\det U_1} & \frac{-va_2}{detU_1} & u \end{pmatrix} = \begin{pmatrix} 12 & 6 & 21 \\ 1 & 1 & 0 \\ -2 & -1 & -3 \end{pmatrix}$$

wobei $a_1 = 12, a_2 = 6, u = -3$ und $v = 1$ mit $u \det(U_1) + v \cdot 21 = 3$ ist. Für U_2 gilt dann $\det U_2 = 3$. Dann bilden wir eine Matrix $U_3 \in \mathbb{Z}^{4\times 4}$ mit

$$U_3 = \begin{pmatrix} 12 & 6 & 21 & 9 \\ 1 & 1 & 0 & 0 \\ -2 & -1 & -3 & 0 \\ \frac{-va_1}{\det U_2} & \frac{-va_2}{\det U_2} & \frac{-va_3}{\det A_2} & u \end{pmatrix} = \begin{pmatrix} 12 & 6 & 21 & 9 \\ 1 & 1 & 0 & 0 \\ -2 & -1 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

mit $u = 1, v = 0$ und $u \det U_2 + v \cdot 9 = \mathrm{ggT}(\det U_2, 9) = 3$. Jetzt teilt man die erste Zeile von U_3 durch 3 und erhält eine Matrix

$$R_1 = \begin{pmatrix} 4 & 2 & 7 & 3 \\ 1 & 1 & 0 & 0 \\ -2 & -1 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

mit $\det U_4 = 1$ und

$$A_1 := AR_1^{-1} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ -39 & -7 & -91 & 138 \\ 10 & 8 & 23 & -13 \\ 0 & 1 & 0 & 13 \\ -112 & -19 & -265 & 351 \end{pmatrix}.$$

Tut man nun das selbe wieder für die 1. Zeile von A_1^t, so erhlt man nacheinander Matrizen

$$U_1 := \begin{pmatrix} 3 & -39 \\ 0 & 1 \end{pmatrix}, U_2 := \begin{pmatrix} 3 & -39 & 10 \\ 0 & 1 & 0 \\ -1 & 13 & -3 \end{pmatrix}, U_3 := \begin{pmatrix} 3 & -39 & 10 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 13 & -3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

und

$$L_1 := \begin{pmatrix} 3 & 0 & -1 & 0 & -3 \\ -39 & 1 & 13 & 0 & 39 \\ 10 & 0 & -3 & 0 & -10 \\ 0 & 0 & 0 & 1 & 0 \\ -112 & 0 & 0 & 0 & 113 \end{pmatrix}.$$

Mit

$$R_2 := \begin{pmatrix} 1 & 885 & 2334 & -1118 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

erhalten wir

$$L_1^{-1}AR_1^{-1}R_2^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -7 & -91 & 138 \\ 0 & 24 & 69 & -39 \\ 0 & 1 & 0 & 13 \\ 0 & 877 & 2311 & -1105 \end{pmatrix}.$$

Diesen Prozess wiederholt man für die Marix

$$\begin{pmatrix} -7 & -91 & 138 \\ 24 & 69 & -39 \\ 1 & 0 & 13 \\ 877 & 2311 & -1105 \end{pmatrix}$$

und wir erhalten insgesamt

$$L_2 := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1299 & 1 & 0 & 0 \\ 0 & 98 & 0 & 1 & 0 \\ 0 & 48428 & 0 & 0 & 0 \end{pmatrix}, L_3 := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 3 & -1 & -3 \\ 0 & 0 & 133 & -44 & -133 \\ 0 & 0 & 668 & 0 & -669 \end{pmatrix}$$

und

$$L_4 := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 17436 & 79 \\ 0 & 0 & 0 & -3562241 & -16140 \end{pmatrix},$$

für die linke Seite und für die rechte Seite

$$R_3 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -7 & -91 & 138 \\ 0 & 0 & -1 & 0 \\ 0 & 3 & 39 & -59 \end{pmatrix}, R_4 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 81 & 1013 \\ 0 & 0 & -2 & -25 \end{pmatrix}$$

und

$$R_5 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 3567621 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Insgesamt erhalten wir

$$L_4^{-1}L_3^{-1}L_2^{-1}L_1^{-1}AR_1^{-1}R_2^{-1}R_3^{-1}R_4^{-1}R_5^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Übungsblatt 2

Aufgabe 1: Sei Λ ein Gitter im $\mathbb{R}^n$ und $b_1, \ldots, b_m \in \Lambda$ linear unabhngig ber $\mathbb{Z}$. Zeige, da $b_1, \ldots, b_m$ dann auch linear unabhngig ber $\mathbb{R}$ sind. Beweise oder widerlege diese Aussage fr den Fall, da Λ nur ein $\mathbb{Z}$-Modul in $\mathbb{R}^n$ ist.

Lösung: Schreibe $(b_1, \ldots, b_m) = (a_1, \ldots, a_n)U$ für eine Basis a_i von Λ und $U \in \mathbb{Z}^{nm}$. Die a_i sind $\mathbb{R}$-linear unabhängig, da Λ ein Gitter ist und alle Basen durch (über $\mathbb{Z}$) invertierbare Matrizen ineinander überführt werden. Die Spalten von U sind $\mathbb{Z}$-linear unabhängig, da die b_i $\mathbb{Z}$-linear unabhängig sind. Daher sind die Spalten von U auch $\mathbb{R}$-linear unabhängig (man werfe hierzu beispielsweise einen Blick auf die Spalten Hermite Normalform von U, für die dies offensichtlich gilt). Aus $(b_1, \ldots, b_m)\lambda = 0$ mit $\lambda \in \mathbb{R}^m$ folgt nun $(a_1, \ldots, a_n)U\lambda = 0$, und daraus $U\lambda = 0$, und daraus $\lambda = 0$. — Für $\Lambda = \mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$ gilt die Aussage natürlich nicht.

Aufgabe 2: Beweise die folgende Aussage: Sei Λ ein Gitter im $\mathbb{R}^n$ und $b_1, \ldots, b_m \in \Lambda$ linear unabhngig. Gilt $(\sum_i \mathbb{Q}b_i) \cap \Lambda = \sum_i \mathbb{Z}b_i$, so lt sich $b_1, \ldots, b_m$ zu einer Basis von Λ vervollstndigen.

Lösung: Schreibe $(b_1, \ldots, b_m) = (a_1, \ldots, a_t)U$ für eine Basis a_i von Λ, mit $m \leq t$. Wende Zeilen Hermite Normalform auf U an, liefert U als obere Dreiecksmatrix mit unterem Teil Null, wobei die Diagonalelemente ungleich Null sind. Also $\sum_{i=1}^m \mathbb{Q}b_i = \sum_{i=1}^m \mathbb{Q}a_i$. Also $a_i \in \sum_{i=1}^m \mathbb{Q}b_i$ und nach Voraussetzung $a_i \in \sum_{i=1}^m \mathbb{Z}b_i$. Daher sind die Diagonalelemente in U betraglich gleich eins, daher ist $b_1, \ldots, b_m, a_{m+1}, \ldots, a_t$ eine Basis von Λ.

Aufgabe 3: Finde die krzesten Vektoren des von den folgenden Spalten erzeugten $\mathbb{Z}$-Moduls:

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

Lösung: Basis erstmal vereinfachen durch Anwendung einer Spalten Hermite Normalform. Die ergibt die Diagonalmatrix mit $2, 1, 3$ auf der Diagonalen. Die Spalten sind orthogonal, und daher sind also $e_2, -e_2$ die kürzesten Vektoren.

Übungsblatt 3

Aufgabe 1: Seien $a_1, \ldots, a_m \in \mathbb{R}^{n_1}$ und $b_1, \ldots, b_m \in \mathbb{R}^{n_2}$ linear unabhngig. Die a_i und b_i heien isometrisch, wenn $\langle a_i, a_j \rangle = \langle b_i, b_j \rangle$ fr alle $1 \leq i, j \leq m$.

Dies liefert eine quivalenzrelation auf linear unabhngigen Teilmengen mit m Elementen in $\mathbb{R}^n$ fr alle $n \geq m$.

1. Finde einen eindeutigen Reprsentanten einer solchen quivalenzklasse in $\mathbb{R}^m$.

2. Benutze 1., um jedem Gitter $\Lambda \subseteq \mathbb{R}^n$ ein vollständiges Vertretergitter in der Isometrieklasse von Λ zuzuordnen. Wie ist die Isometrie gegeben? Ist dieses Vetretergitter eindeutig durch Λ bestimmt?

Hinweis: Verwende die Q-R Zerlegung von Matrizen (Q mit orthonormalen Spalten und R obere Dreiecksmatrix, entstehend aus dem Gram-Schmidt Orthonormalisierungverfahren).

Lösung: Zum Teil 1. Schreibe $a_1, \ldots, a_m$ als Matrix M, und berechne die Q-R Zerlegung von M mittels des Gram-Schmidt Verfahrens angewendet auf die Spalten von M. Dann gilt $R \in \mathbb{R}^{mm}$ mit Einsen auf der Diagonalen. Wir nehmen die Spalten von R als eindeutige Vertreterbasis, denn R hängt nur von den Werten $\langle a_i, a_j \rangle$ ab, welche invariant unter Isometrie sind. Außerdem gilt $Q^{tr}Q = I_m$ und $M^{tr}M = R^{tr}Q^{tr}QR = R^{tr}R$. Dies zeigt, daß die a_i und die Spalten von R isometrisch sind.

Zum Teil 2. Wir ordnen einer Basis von Λ die eindeutige bestimmte Basis bestehend aus den Spalten von R aus 1. zu, und bilden das von diesen Vektoren erzeugte Gitter Λ'. Wegen $\det(R) = 1$ ist Λ' vollständig. Die Isometrie wird durch Multiplikation der Vektoren aus Λ' mit Q von links gegeben (ist Isometrie, weil $Q^{tr}Q = I_m$). Das Vertretergitter Λ' wird durch Λ nicht eindeutig bestimmt, da die Konstruktion von der gewählten Basis abhängt und zwei Basen von Λ nicht unbedingt isometrisch sein müssen.

Aufgabe 2: Beweise den Satz von Blichfeldt im Fall S kompakt und $\mathrm{vol}(S) = d(\Lambda)$.

Lösung: Mit den Bezeichnung wie im Beweis im Skript für $\mathrm{vol}(S) > \mathrm{vol}(\Pi)$. Sei $\mathrm{vol}(S) = \mathrm{vol}(\Pi)$ und S kompakt. Für jedes $k \in \mathbb{Z}^{\geq 1}$ erhalten wir $z_{1,k}, z_{2,k} \in (1 + 1/k)S$ mit $z_{1,k} \neq z_{2,k}$ und $z_{1,k} - z_{2,k} \in \Lambda$. Weil $2S$ kompakt ist, gibt es in $z_{1,k}$ und $z_{2,k}$ konvergente Teilfolgen, deren Grenzwerte z_1 und z_2 wegen der Abgeschlossenheit von S in S liegen. Aufgrund der Diskretheit von Λ bildet die Differenz dieser konvergenten Teilfolgen eine in $\Lambda \backslash \{0\}$ konvergente Folge, deren Grenzwert gleich $z_1 - z_2$ ist. Es ergibt sich also $z_1 \neq z_2$ und $z_1 - z_2 \in \Lambda$.

Aufgabe 3: Zeige, da die unteren Abschatzungen fr die sukzessiven Minima durch die Gram-Schmidt orthogonalisierten Vektoren in Abhangigkeit

von der Eingabebasis beliebig schlecht werden kann. Welche grobe Bedingung kann man im Umkehrschlu an die Eingabebasis stellen, damit die Abschätzung möglichst scharf wird, und warum?

Lösung: Es gilt $d(\Lambda) = \mathrm{vol}(\Pi(b_1, \ldots, b_m)) = \mathrm{vol}(\Pi(b_1^*, \ldots, b_m^*)) = \prod_{i=1}^{m} ||b_i^*||$, da die Gram-Schmidt Transformationsmatrix Determinante eins hat. Es gilt weiter $b_1 = b_1^*$. Ist $||b_1||$ betraglich sehr groß, so werden die $||b_i^*||$ für $i > 1$ betraglich sehr klein, und folglich werden die Abschätzungen schlechter. Wir können $||b_1||$ beliebig groß machen, zum Beispiel, indem wir b_1 durch b_1 plus ein großes Vielfaches von b_2 ersetzen. Entsprechend klein ist dann der Winkel zwischen b_1 und b_2.

Für bessere Abschätzungen sollte die Basis b_i möglichst orthogonal sein, so daß sich die Werte $||b_i||$ und $||b_i^*||$ nicht zuviel voneinander unterscheiden.