Lineare Gleichungssysteme modulo T

Bachelorarbeit

May 14, 2018

Fatima Akil

4855378

fatima-akil@web.de

Universität Freie Universität Berlin
Fakultät Mathematik
Erstgutachter Prof. Dr. Borndörfer

.

Inhaltsverzeichnis

1 Einleitung **2**

2 Lineare Algebra - Grundlagen **4**
2.1 Gruppen, Körper und Ringe 4
2.2 Lineare Gleichungssysteme über Körpern 8

3 Lineare diophantische Gleichungssysteme **13**
3.1 Hermite-Normalform 14
3.2 Smith-Normalform 19

4 Lineare Gleichungssysteme modulo T **23**
4.1 Gauß-Algorithmus 24
4.2 Hermite-Normalform 26
4.3 Smith Normalform 29
4.4 Chinesischer Restsatz 34

5 Periodische Taktfahrpläne **38**
5.1 Periodic Event Scheduling Problem 38

6 Fazit **49**

Literaturverzeichnis **50**

Selbstständigkeitserklärung **51**

1 Einleitung

Mit dem Voranschreiten der Technologie erhalten die öffentlichen Verkehrsmittel eine größere Bedeutung. Die Beförderung mehrerer Personen eröffnet der Gesellschaft viele Möglichkeiten, unter Anderem den Vorteil der Zeitersparnis. Die Dauer des Verkehrswegs mit öffentlichen Verkehrsmitteln ist häufig geringer, als die mit individuellen Verkehrsmitteln. Jedes öffentliche Transportmittel ist mit einem Fahrplan versehen. Dieser bietet Passagieren, die öffentliche Verkehrsmittel öfter nutzen, eine Strukturierung und Planung ihrer Zeit. Dabei lassen sich Taktfahrpläne aufgrund ihres periodischen Verhaltens leicht einprägen. Dieses periodische Verhalten ist durch mathematische Modellierungen darstellbar.
Das persönliche Nutzverhalten vieler Bürger im Personenverkehr ist auf die öffentlichen Verkehrsmittel beschränkt. Diese beinhalten im Gegensatz zum individuellen Verkehrsmittel eine Wartezeit. Dabei stellt sich die Frage, ob man anhand mathematischer Modelle diese Wartezeit minimieren kann. Eine bekannte mathematische Modellierung dieses Problems ist das *Periodic Event Scheduling Problem (PESP)*. Die optimale Planung eines periodischen Taktfahrplanes steht im Vordergrund.

Während ich dieses Problem betrachtet habe, wurde ich auf das Rechnen mit linearen Gleichungssystemen modulo T aufmerksam. Bei periodischen Taktfahrplänen wird ein einheitliches zeitliches Muster, welches sich nach T Minuten wiederholt, betrachtet. Das dabei zu betrachtende Lösungsproblem eröffnet ein Teilgebiet der Mathematik, welches bislang nicht im Vordergrund stand: Das Lösen linearer Gleichungen modulo T, wobei T für die Zeit in Minuten steht und somit 60 ist. Da 60 keine Primzahl ist, kann – wie im Laufe der Arbeit präsentiert – das lineare Gleichungssystem nicht mehr über einen Körper gelöst werden. Lineare Gleichungssysteme werden nun über Nicht-Körpern betrachtet.

Die Literatur weist sowohl im deutschsprachigem als auch im englischsprachigen Raum wenig Umfang bezüglich linearer Gleichungssysteme über Nicht-Körper auf. Der Bestand an Fachliteratur bezüglich den Themen lineare diophantische Gleichungssysteme, Hermite-Normalform und Smith-Normalform ist zurzeit gering, dennoch erreichbar, beispielsweise in [1], welches in dieser Bachelorarbeit genutzt wurde.
Insbesondere wurde ich bei der Suche nach geeigneter Literatur zu linearen Gleichungssystemen über Restklassenringe, die keinen Körper bilden, nicht fündig. Dabei recherchierte ich sowohl in den Universitätsbibliotheken als auch in webbasierenden Suchmaschinen.

Aufgrund dem geringen Bestand an Fachliteratur in diesem Kontext, war ich gezwungen, an vielen Stellen eigene logische Verknüpfungen zu konzipieren und zu beweisen. Dies brachte viele Schwierigkeiten mit sich, die mit bestmöglichem Verständnis bearbeitet wurden.
Abseits der Zugänglichkeit der Literatur, finde ich es sehr überraschend, dass sich viele Professoren der Mathematik mit diesem Themenbereich nicht beschäftigten. Insbesondere gingen von den Dozenten, die ich um Literaturempfehlung bat, kein Werk aus. Damit wurde das Thema "Lineare Gleichungssysteme Modulo T" einerseits eine große Herausforderung, andererseits eine große Motivation, da ich mit dieser Bachelorarbeit vielen Interessenten der Mathematik als Sekundärliteratur dienen kann.
Die Arbeit gliedert sich wie folgt:

In Kapitel 2 werden grundlegende Inhalte wiederholt. Darunter fallen sowohl Grundbegriffe, wie Gruppen und Ringe, als auch das Lösen linearer Gleichungssysteme über Körpern. Es wird der Gauß-Algorithmus erklärt und anhand eines Beispiels verdeutlicht.
In Kapitel 3 werden, auf Kapitel 2 aufbauend, Lösungsverfahren der beiden Mathematiker Charles Hermite und Henry John Stephen Smith für lineare diophantische Gleichungssysteme eingeführt.
Anschließend werden in Kapitel 4 sowohl die in Kapitel 3 dargestellten Lösungsverfahren als auch der Gauß-Algorithmus bezüglich linearer Gleichungssysteme modulo T präsentiert und mit Beispielen vorgeführt. Als weitere Lösungsmöglichkeit wird der chinesische Restsatz ebenfalls vorgestellt.
In Kapitel 5 wird auf das Periodic Event Scheduling Problem eingegangen und erläutert, wie die vorgestellten Verfahren auf dieses mathematische Modell angewandt werden können. In diesem Zusammenhang finden der Gauß-Algorithmus, die in Kapitel 3 vorgestellten Lösungsverfahren - die Hermite-Normalform und die Smith-Normalform - und der chinesische Restsatz ihre Verwendung wieder.
Abschließend erfolgt eine Zusammenfassung zu allen Kapiteln.

2 Lineare Algebra - Grundlagen

In diesem Kapitel der Bachelorarbeit werden grundlegende Begriffe zwecks Vollständigkeit und Verständlichkeit in den darauffolgenden Kapiteln repetiert. In diesem Zusammenhang werden Gruppen, Ringe und Körper erfasst und dem folgend die Modulo-Rechnung wiederholt. Anschließend wird das Konstrukt der Matrizen erläutert und abschließend lineare Gleichungen, insbesondere lineare Gleichungssysteme, präsentiert.

Vorerst werden einige Notationen, welche in dieser Arbeit verwendet werden, festgelegt.

- $\mathbb{N}$ – Menge der natürlichen Zahlen *ohne* Null
- $\mathbb{Z}$ – Menge der ganzen Zahlen *mit* Null
- $\exists\, a$ – Es existiert ein a
- $\forall a$ – Für alle a
- $a \equiv_T b$ – a kongruent b modulo T
- $a|b$ – a teilt b
- $a|_T b$ – a teilt b modulo T

2.1 Gruppen, Körper und Ringe

In dieser Arbeit werden überwiegend Körper und Ringe betrachtet. Um diese Begriffe zu definieren, werden zunächst Gruppen eingeführt und darauf aufbauend Körper und Ringe. Die Definitionen dieser Begriffe stammen aus [2].

2.1.1 Definition: Sei G eine nichtleere Menge mit einer inneren Verknüpfung $*$, wobei

$$* : G \times G \to G, (a, b) \mapsto a * b.$$

Dann ist (G,$*$) eine *Gruppe*, wenn folgende Eigenschaften für $a, b, c \in G$ erfüllt sind:

- Assoziativgesetz: $(a * b) * c = a * (b * c)$
- Neutrales Element: $\exists\, e \in G,$ sodass $a * e = a\ \forall a \in G$
- Inverses Element: $\forall a \in G\ \exists\, a^{-1}$ sodass gilt: $a * a^{-1} = e = a^{-1} * a$

Gilt zusätzlich noch das Kommutativgesetz, $a * b = b * a$, so heißt die Gruppe *kommutativ*.

Auf dieser Grundlage werden Ringe und Körper wie folgt definiert.

2.1.2 Definition: Sei K eine nichtleere Menge mit zwei inneren Verknüpfungen $\cdot$ und $+$, wobei

$$\cdot : K \times K \to K, (a, b) \mapsto a \cdot b.$$

$$+ : K \times K \to K, (a, b) \mapsto a + b.$$

Dann ist (K,$\cdot$,$+$) ein *Körper*, wenn folgende Eigenschaften für $a, b, c \in K$ erfüllt sind:

- $(K, +)$ ist eine kommutative Gruppe
- $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe
- Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$

2.1.3 Definition: Sei R eine nichtleere Menge mit zwei inneren Verknüpfungen $\cdot$ und $+$, wobei

$$\cdot : R \times R \to R, (a, b) \mapsto a \cdot b.$$

$$+ : R \times R \to R, (a, b) \mapsto a + b.$$

Dann ist $(R,\cdot,+)$ ein *Ring*, wenn folgende Eigenschaften für $a, b, c \in R$ erfüllt sind:

- $(R,+)$ ist eine kommutative Gruppe
- Assoziativität bezüglich der Multiplikation: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributivgesetze: $a \cdot (b + c) = a \cdot b + a \cdot c$
  $(a + b) \cdot c = a \cdot c + b \cdot c$

In Bezug auf Ringe werden in der linearen Algebra ebenfalls Abbildungen zwischen Ringen definiert. Die Abbildung, die in dieser Arbeit von Bedeutung ist, ist der Ringhomomorphismus.

2.1.4 Definition: Eine Abbildung $f : R \to R'$ zwischen zwei Ringen R,R' wird *Ringhomomorphismus* genannt, wenn gilt:

- $f(x + y) = f(x) + f(y)\ \forall x, y \in R$
- $f(x \cdot y) = f(x) \cdot f(y)\ \forall x, y \in R$

Der *Kern* eines Ringhomomorphismus wird definiert als $Ker(f) := \{x \in R | f(x) = 0\}$. [2]

Weiterhin wird eine für die Arbeit relevante Kategorie der Ringe, der sogenannte Restklassenring, eingeführt.

2.1.5 Definition: Der *Restklassenring* $\mathbb{Z}/T\mathbb{Z}$ ist die Menge aller ganzen Zahlen von 0 bis $T - 1$, wobei jede Zahl eine Restklasse repräsentiert.

Über die Axiome des Rings hinaus, besitzt der Restklassenring $R = \mathbb{Z}/T\mathbb{Z}, T \in \mathbb{N}$ weitere folgende Eigenschaften [3]:

- R ist kommutativ: $\forall x, y \in R$ gilt: $x \cdot y \equiv_T y \cdot x$
- R ist ein Ring mit Eins, das heißt: $1 \in R$ und $1 \cdot x = x\ \forall x \in R$
- Nullelement $0 \in R$

In Restklassenringen $\mathbb{Z}/T\mathbb{Z}$ rechnet man mit dem Rest, den die Division zweier ganzer Zahlen hinterlässt. Ergeben zwei Zahlen bei der Division durch T denselben Rest, befinden sie sich in derselben Restklasse. Dies führt zur folgenden Definition.

2.1.6 Definition: Seien $x, y \in \mathbb{Z}$ und $T \in \mathbb{N}$. x und y heißen *kongruent modulo* T, wenn $y - x$ durch T teilbar ist [2].

Zur Veranschaulichung ein kurzes Beispiel:

2.1.7 Beispiel: Betrachten wir den Restklassenring $\mathbb{Z}/24\mathbb{Z} = \{0, 1, .., 23\}$. Dann gilt:

$17 + 9 \pmod{24} \equiv 26 \pmod{24} \equiv 2 \pmod{24}$.
26 und 2 sind kongruent modulo T, da $26 - 2 = 24$ und $24|24$.

Weitere gängige Schreibweisen sind:

$17 + 9\ (24) \equiv 26\ (24) \equiv 2\ (24)$

$17 + 9 \equiv_{24} 26 \equiv_{24} 2$

Diese Arbeit wird sich an der letzteren Schreibweise orientieren.

Das einzige Axiom, das den Restklassenring vom Körper unterscheidet, ist die Existenz des inversen Elements. Besitzt ein Element in dem Restklassenring eine Inverse, wird sowohl dieses Element als auch das zugehörige inverse Element *Einheit* genannt [2].

2.1.8 Definition: $a \in R$ heißt *Einheit* $\Leftrightarrow$ $as \equiv_T 1_R,\ s \in R,$ wobei 1_R das Einselement aus dem Ring R bezeichnet [2].

Eine Eigenschaft von Einheiten, die im weiteren Verlauf der Arbeit relevant sein wird, bietet der folgende Satz.

2.1.9 Satz: Ein Element $a \in R = \mathbb{Z}/T\mathbb{Z}$ ist eine Einheit, genau dann wenn a und T teilerfremd sind. Also genau dann, wenn $ggT(a, T) = 1$ [4].

Um diesen Satz zu beweisen, wird vorerst ein Algorithmus zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen a und T vorgestellt: Der erweiterte euklidische Algorithmus. Dieser berechnet neben dem größten gemeinsamen Teiler von a und T auch zwei weitere ganze Zahlen s und u, sodass gilt:

$$ggT(a, T) = s \cdot a + u \cdot T.$$

Angewandt im Restklassenring $\mathbb{Z}/T\mathbb{Z}$ fällt der zweite Summand $u \cdot T$ weg, da $T \equiv_T 0$.
Also gilt $ggT(a, T) = s \cdot a + u \cdot T \equiv_T s \cdot a + u \cdot 0 \equiv_T s \cdot a$.
Somit kann man den erweiterten euklidischen Algorithmus unter Anderem nutzen, um die Inverse zu einem Element aus dem Restklassenring zu berechnen, falls diese existiert [2].

Beweis Satz 2.1.9: Sei $R = \mathbb{Z}/T\mathbb{Z}, T \in \mathbb{N}$ ein Restklassenring. Dann ist $a \in R$ eine Einheit genau dann, wenn ein Element s aus dem Restklassenring R existiert, sodass $a \cdot s \equiv_T 1$ (Def. Einheit). Da $T \equiv_T 0$ gilt, ist $a \cdot s \equiv_T 1$ äquivalent zu $a \cdot s + u \cdot T \equiv_T 1$, $u \in R$. Nach dem erweiterten euklidischen Algorithmus ist das wiederum äquivalent zu $ggT(a, T) \equiv_T 1$. $\square$

Folglich existiert zu jedem Element aus dem Restklassenring R eine Inverse, wenn jedes Element eine Einheit ist. Das Axiom der Existenz des inversen Elements wäre folglich erfüllt und R wäre somit ein Körper. Der nachfolgende Satz beschreibt, wann dieser Fall auftritt.

2.1.10 Satz: Sei $R = \mathbb{Z}/T\mathbb{Z}$ ein Restklassenring. Dann ist R ein Körper genau dann, wenn T eine Primzahl ist [4].

Beweis: " $\Rightarrow$ " : Angenommen $R = \mathbb{Z}/T\mathbb{Z}$ sei ein Körper. Es ist zu zeigen, dass T eine Primzahl ist.
Nach dem Körperaxiom, Existenz des neutralen Elements bezüglich der Addition und der Multiplikation, ist sowohl die Null als auch die Eins in dem Restklassenring enthalten. Somit besteht der Ring aus mindestens zwei Elementen und es gilt: $T = |\mathbb{Z}/T\mathbb{Z}| > 1$.
Da in einem Körper, dem Axiom der Existenz der Inverse entsprechend, für jedes Element $a \in \{2, 3, ..., T-1\}$ ein inverses Element existiert, ist jedes Element aus dem Restkassenring eine Einheit. Demzufolge gilt nach dem Satz 2.1.8: $ggT(a, T) = 1$ für jedes Element a aus R. Also ist insbesondere jedes Element teilerfremd zu T und damit gilt, dass T eine Primzahl ist.

" $\Leftarrow$ " : Angenommen T sei eine Primzahl. Es ist zu zeigen, dass $R = \mathbb{Z}/T\mathbb{Z}$ ein Körper ist.
Weil T prim ist, nimmt T mindestens den Wert Zwei an und es gilt: $T = |\mathbb{Z}/T\mathbb{Z}| > 1$.
Somit enthält R mindestens zwei Elemente: Die Null und die Eins. Damit ist das Körperaxiom, Existenz des neutralen Elements bezüglich der Multiplikation und Addition, erfüllt.
Um zu beweisen, dass R ein Körper ist, bleibt noch zu zeigen, dass jedes Element aus dem Restklassenring ein Inverses Element besitzt.
T ist eine Primzahl, somit ist jedes Element $a \neq 0$ aus dem Ring teilerfremd zu T, also gilt insbesondere $ggT(a, T) = 1$. Nach dem Satz 2.1.8 ist jedes Element ungleich Null eine Einheit, also existiert zu jedem Element eine Inverse und somit ist $\mathbb{Z}/T\mathbb{Z}$ ein Körper. $\square$

Dieser Satz ist für den weiteren Verlauf dieser Arbeit sehr wichtig, denn er unterteilt Restklassenringe in Körper und Nicht-Körper. Über Körper lassen sich lineare Gleichungssysteme im Vergleich zu über Nicht-Körper problemlos mit Hilfe des Gauß-Algorithmus lösen, wie im nächsten Unterkapitel erläutert wird. Über Nicht-Körper ist die Anwendung des Gauß-Algorithmus nicht immer möglich. Dies wird im Kapitel 4.1 thematisiert.

Neben Einheiten gibt es in Restklassenringen die Nullteiler. Diese sind Elemente aus dem Restklassenring, die multipliziert mit einem weiteren Element aus dem Restklassenring die Null ergeben. Dabei sind beide Elemente von Null verschieden. Diesbezüglich wird folgende formale Definition eingeführt.

2.1.11 Definition: Ein Element a aus dem Restklassenring $R = \mathbb{Z}/T\mathbb{Z}$ heißt *Nullteiler,* wenn ein $b \in R, b \neq 0$ existiert, sodass $a \cdot b = 0$ [2].

Aus den Eigenschaften von Nullteilern und Einheiten folgt eine besondere Eigenschaft für Restklassenringe.

2.1.12 Satz: Der Restklassenring R=$\mathbb{Z}/T\mathbb{Z}$ besteht, abgesehen von der Null, ausschließlich aus Einheiten und Nullteilern. Weiterhin kann kein Element sowohl eine Einheit als auch ein Nullteiler sein [2].

Beweis: Sei a ein Element aus $R\backslash\{0\}$. Es wird zunächst mittels Fallunterscheidung gezeigt, dass a ein Nullteiler oder eine Einheit ist. Anschließend wird gezeigt, dass ein Element aus $R \setminus \{0\}$ nicht beide Eigenschaften annehmen kann.

Fall 1: a ist eine Einheit. Damit ist gezeigt, was zu zeigen war.
Fall 2: a ist keine Einheit. Somit ist zu zeigen, dass a ein Nullteiler ist.
Nach Satz 2.1.8 gilt, dass a und T nicht teilerfremd sind, also $ggT(a, T) \neq 1$.
Sei $d \not\equiv_T 1$ der größte gemeinsame Teiler von a und T. Dann gilt insbesondere: $d|T$ und $d|a$.
Folglich gilt auch: $\frac{T}{d} =: b \not\equiv_T 0,$ (da $d \neq 1$), und $b \in R$.
Und auch $\frac{a}{d} =: c \not\equiv_T 0,\ c \in R$.
Daraus folgt: $a \cdot b \equiv_T (c \cdot d) \cdot b \equiv_T c \cdot (d \cdot b) \equiv_T c \cdot T \equiv_T 0$. Also ist a ein Nullteiler.

Es bleibt zu beweisen, dass a nicht Nullteiler und keine Einheit zugleich sein kann. Dies wird anhand eines Widerspruchsbeweises gezeigt.
Angenommen $a \in R\backslash\{0\}$ sei ein Nullteiler. Dies bedeutet, dass ein $b \in R\backslash\{0\}$ existiert mit $a \cdot b \equiv_T 0$.
Sei a zusätzlich eine Einheit. Dann existiert ein $c \in R \setminus \{0\}$ mit $c \cdot a \equiv_T 1$.
Es gilt $0 \equiv_T c \cdot 0 = c \cdot (a \cdot b) \equiv_T (c \cdot a) \cdot b \equiv_T 1 \cdot b \equiv_T b$. Dies ist ein Widerspruch, denn b ist nach Voraussetzung ungleich Null. □

Damit ist nun bewiesen, dass ein Restklassenring $R = \mathbb{Z}/T\mathbb{Z}$ ausschließlich aus Einheiten und Nullteilern besteht. Diese Eigenschaft ist im späteren Verlauf der Arbeit, da Restklassenringe $R = \mathbb{Z}/T\mathbb{Z}$ für T nicht prim betrachtet werden, relevant.

Das folgende Kapitel führt lineare Gleichungssysteme ein. Dabei wird der Fokus auf lineare Gleichungssysteme über Körper gelegt, um einen wichtigen Algorithmus - den Gauß-Algorithmus - nahezulegen. Dieser ist ein Rechenverfahren, der sich als Bearbeitung der Problematik dieser Bachelorarbeit bietet.

2.2 Lineare Gleichungssysteme über Körpern

Lineare Gleichungen sind ein Teilgebiet der Mathematik und gehören zu dem Ursprung der linearen Algebra. Bereits 2000 v. Chr. befassten sich Babylonier mit linearen Gleichungen. Jedoch betrachteten sie in einem linearen Gleichungssystem nur zwei Unbekannte und diese traten ausschließlich in bestimmten Kenngrößen, wie Länge und Gewicht, auf. Allgemeine Lösungstheorien für n Gleichungen und n Unbekannte wurden aber erst im 18. Jahrhundert durch Gabriel Kramer (1704-1752) veröffentlicht. Dabei bezeichnet n eine

beliebige natürliche Zahl [5].
Lineare Gleichungssysteme über Körper sind heutzutage Bestandteil des Rahmenlehrplans an deutschen Schulen und man wird mit den drei Verfahren Einsetzungs-, Additions- und Gleichsetzungsverfahren vertraut. Im Mathematikstudium wird dieses Wissen vertieft. Ebenso werden Studierenden weitere Lösungsmöglichkeit nahegelegt. Zusätzlich befassen sie sich mit der Existenz und Eindeutigkeit von Lösungen. In diesem Unterkapitel werden Kenntnisse zum Verständnis dieser Arbeit wiederholt. Dafür wurde die Literatur [6] benutzt.

2.2.1 Definition: *Lineare Gleichungen* sind Gleichungen, bei denen die unbekannten Variablen höchstens in der ersten Potenz vorkommen. Dabei ist die Multiplikation von mehreren Unbekannten nicht zugelassen.

2.2.2 Beispiele: $3x + y = 4,\ x, y \in \mathbb{R}$, ist eine lineare Gleichung.
$4xy + x = 10,\ x, y \in \mathbb{R}$, ist keine lineare Gleichung, da zwei unbekannte Variablen miteinander multiplikativ verknüpft sind.
$3x^2 + 5y = 30,\ x, y \in \mathbb{R}$, ist keine lineare Gleichung, da eine unbekannte Variable in der zweiten Potenz vorkommt.

2.2.3 Definition: Ein *lineares Gleichungssystem* besteht aus mehreren linearen Gleichungen, die mindestens eine unbekannte Variable enthalten und gleichzeitig gelten.

An dieser Stelle wird einfachheitshalber das System der Matrizen eingeführt. Dabei wird in dieser Arbeit die Matrix-Vektor-Schreibweise zur Darstellung linearer Gleichungssysteme genutzt.

$A\vec{x} = \vec{b},$ wobei $A \in K^{m \times n}, \vec{x} \in K^n, \vec{b} \in K^m,$ und K ein Körper ist. $n, m \in \mathbb{N}, n > m.$

Die Matrix A enthält alle Koeffizienten des linearen Gleichungssystems und wird *Koeffizientenmatrix* genannt. Weiterhin ist $\vec{x}$ der Vektor, der alle n Unbekannten enthält.

Diese Schreibweise wurde erstmals durch chinesische Mathematiker eingeführt. Sie stellten fest, dass die Struktur eines linearen Gleichungssystems nicht von den unbekannten Variablen abhängt und allein durch die Koeffizienten berechenbar ist [5].

Man differenziert zwischen homogenen und inhomogenen linearen Gleichungssystemen. Diese Differenz wird im Folgendem beschrieben.

2.2.4 Definition: Sei $A\vec{x} = \vec{b}$ ein lineares Gleichungssystem, wobei $A \in K^{m \times n}$, $\vec{x} \in K^n,\ \vec{b} \in K^m$ und K ein Körper.

Sei weiterhin $\vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$.

Falls $b_i = 0\ \forall i \in [1, m],$ so handelt es sich um ein *homogenes* lineares Gleichungssystem. Existiert mindestens ein $b_i \neq 0$ liegt ein *inhomogenes* lineares Gleichungssystem vor.

Homogene lineare Gleichungssysteme $A\vec{x} = 0$ besitzen mindestens eine Lösung, nämlich:

$$\vec{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Bei inhomogenen linearen Gleichungssystemen hingegen kann es vorkommen, dass keine Lösung existiert [7].

Welche Voraussetzungen für die Existenz und die Eindeutigkeit von Lösungen erfüllt sein müssen und wie die Lösung gefunden wird, wird im Folgenden erläutert. Hierfür wurde die Literatur [6] verwendet.

2.2.5 Lösbarkeit linearer Gleichungssysteme über Körper

Betrachtet wird das lineare Gleichungssystem $A\vec{x} = \vec{b}$, wobei $A \in K^{m \times n}$, $\vec{x} \in K^n$ und $\vec{b} \in K^m$ sowie K ein Körper ist.

Die Frage nach der Existenz und Eindeutigkeit von Lösungen zum linearen Gleichungssystem lässt sich mit Hilfe des Rangs der Matrix A und der Koeffizientenmatrix $(A|\vec{b})$ beantworten.
Der Rang einer Matrix A wird durch die Anzahl der linear unabhängigen Zeilen dieser Matrix bestimmt und wird mit $rang(A)$ bezeichnet.

Das lineare Gleichungssystem $A\vec{x} = \vec{b}$ ist genau dann lösbar, wenn der Rang der Koeffizientenmatrix A dem Rang der erweiterten Koeffizientenmatrix $(A|\vec{b})$ entspricht. Mathematisch formuliert: $A\vec{x} = \vec{b}$ ist *lösbar* $\Leftrightarrow \text{rang}(A) = \text{rang}(A|b)$.
Weiterhin ist die Lösung des linearen Gleichungssystems $A\vec{x} = \vec{b}$ genau dann *eindeutig,* wenn der Rang von A und der Rang von $(A|\vec{b})$ zusätzlich noch der Anzahl der Unbekannten entspricht.

$A\vec{x} = \vec{b}$ ist *eindeutig lösbar* $\Leftrightarrow \text{rang}(A) = \text{rang}(A|b) = n =$ Anzahl der Unbekannten.

Nachdem die Existenz- und die Eindeutigkeitsbedingungen einer Lösung bekannt sind, kann auch der im Allgemeinen genutzte Lösungsweg eingeführt werden. Dieser wird ebenfalls in den nächsten Kapiteln relevant sein.

2.2.6 Lösungsweg

Carl Friedrich Gauß (1777-1855) entwickelte 1811 den Gauß-Algorithmus. Dieser beschreibt das erste Verfahren zur Berechnung linearer Gleichungssysteme, bei denen die Anzahl der unbekannten Variablen nicht unbedingt mit der Anzahl der Gleichungen übereinstimmen muss. Durch den Gauß-Algorithmus wird die Koeffizientenmatrix in die Zeilenstufenform überführt. Zugelassen sind alle elementaren Zeilenumformungen:

- Vertauschung zweier Zeilen
- Addition des λ-Vielfachen einer Zeile zu einer anderen, $\lambda \in K \backslash \{0\}$

- Multiplikation einer Zeile mit einem Skalar $\lambda \in K \backslash \{0\}$

Eine Matrix ist in der Zeilenstufenform, falls alle Einträge unterhalb der Hauptdiagonalen Null sind.

Sei $A\vec{x} = \vec{b}$ das zu lösende lineare Gleichungssystem, wobei $A \in K^{m \times n}$ und $\vec{x} \in K^n, \vec{b} \in K^m$ und K ein Körper ist.

Dann löst man das lineare Gleichungssystem nach dem Gauß-Algorithmus wie folgt:

Schritt 1: Überführung der erweiterten Koeffizientenmatrix $(A|b)$ mit Hilfe elementarer Zeilenumformungen in die Zeilenstufenform.

Schritt 2: Bestimmung der Unbekannten durch Vorwärts- oder Rückwärtssubstitution.

Zur Veranschaulichung werden nun Beispiele vorgeführt und der Gauß-Algorithmus auf diese angewandt. Dabei ist zu beachten, dass diese Beispiele über Körper betrachtet werden.

2.2.7 Beispiel: Sei $A = \begin{pmatrix} 2 & 4 & 1 & 2 \\ 2 & 0 & 1 & 2 \\ 0 & 4 & 1 & 0 \end{pmatrix} \in \mathbb{R}^{3\times 4}$, $\vec{b} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \in \mathbb{R}^3$, $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \mathbb{R}^4$

Gesucht ist die Lösungsmenge $L = \{\vec{x} \,| A\vec{x} = \vec{b}\}$.

Schritt 1: $\left(\begin{array}{cccc|c} 2 & 4 & 1 & 2 & 1 \\ 2 & 0 & 1 & 2 & 2 \\ 0 & 4 & 1 & 0 & 3 \end{array}\right) \xrightarrow{\text{II.-I.}} \left(\begin{array}{cccc|c} 2 & 4 & 1 & 2 & 1 \\ 0 & -4 & 0 & 0 & 1 \\ 0 & 4 & 1 & 0 & 3 \end{array}\right) \xrightarrow{\text{III.+II.}} \left(\begin{array}{cccc|c} 2 & 4 & 1 & 2 & 1 \\ 0 & -4 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 4 \end{array}\right)$

Damit ist die Matrix in der Zeilenstufenform und man erkennt sofort:
$rang(A) = rang(A|b) = 3 \neq 4 =$ Anzahl der Unbekannten.

$\Rightarrow L \neq \{\varnothing\}$. Es existiert zwar eine Lösung, diese ist aber nicht eindeutig.

Schritt 2: Durch Vorwärtssubstitution erhalten wir:

$$\begin{array}{c} x_3 = 4 \\ x_2 = -\frac{1}{4} \\ 2x_1 + 3 + 2x_4 = 1 \Leftrightarrow x_4 = -x_1 - 1 \end{array} \quad \Rightarrow \quad L = \{ \begin{pmatrix} x_1 \\ -\frac{1}{4} \\ 4 \\ -x_1 - 1 \end{pmatrix}, x_1 \in \mathbb{R}\}.$$

Mit diesem Beispiel wurde der Gauß-Algorithmus über den reellen Zahlen verdeutlicht. Durch die schrittweise Anwendung des Algorithmus hat man eine eindeutig bestimmte Lösungsmenge erhalten. Im folgendem Beispiel wird der Gauß-Algorithmus über den Restklassenkörper $\mathbb{F}_3$ angewandt.

2.2.8 Beispiel: Sei $A = \begin{pmatrix} 2 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 1 & 2 \end{pmatrix} \in \mathbb{F}_3$, $b = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \in \mathbb{F}_3$ und $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in \mathbb{F}_3$.

Gesucht ist die Lösungsmenge $L = \{x|Ax = b\}$.

Schritt 1: Die Matrix A wird durch elementare Zeilenumformungen in die Zeilenstufenform gebracht. Dabei werden die Einträge nach jeder Umformung auf modulo 3 reduziert.

$$\left(\begin{array}{cccc|c} 2 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 2 & 1 & 2 & 1 \end{array}\right) \xrightarrow[\text{III.-II.}]{\text{I.-II.}} \left(\begin{array}{cccc|c} 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{array}\right) \xrightarrow{\text{I.+III.}} \left(\begin{array}{cccc|c} 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 2 & 0 & 0 & 1 \end{array}\right)$$
$$\xrightarrow[\text{vertauschen}]{\text{II.\&III.}} \left(\begin{array}{cccc|c} 2 & 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 & 0 \end{array}\right).$$

Aus der Zeilenstufenform erkennt man sofort:
$rang(A) = rang(A|b) = 3 \neq 4 =$ Anzahl der Unbekannten.

Demnach ist die Lösungsmenge nicht leer und die Lösung ist nicht eindeutig.

Schritt 2: Durch Vorwärtssubstitution erhält man:

$$\begin{array}{c} 2x_1 \equiv_3 2 \Leftrightarrow x_1 \equiv_3 1 \\ 2x_2 \equiv_3 1 \Leftrightarrow x_2 \equiv_3 2 \\ x_3 + 2x_4 \equiv_3 0 \Leftrightarrow x_3 \equiv_3 -2x_4 \end{array} \quad \Rightarrow \quad L = \{ \begin{pmatrix} 1 \\ 2 \\ -2x_4 \\ x_4 \end{pmatrix}, x_4 \in \mathbb{F}_3 \}.$$

Wie im vorherigen Beispiel erhält man auch in diesem Beispiel nach Anwendung des Gauß-Algorithmus über einen Körper eine eindeutig bestimmte Lösungsmenge. Diese Lösungsmenge ist über $\mathbb{F}_3$ eindeutig bestimmt.

In diesem Kapitel wurde das Lösen linearer Gleichungssysteme über einem Körper wiederholt. Insbesondere wurde auf die Existenz und Eindeutigkeit solcher Lösungen eingegangen. Durch Beispiele wurde der Gauß-Algorithmus verdeutlicht, da dieser im weiteren Verlauf der Arbeit wieder aufgegriffen wird.

Diese Arbeit thematisiert lineare Gleichungssysteme über Nicht-Körper, insbesondere Restklassenringe. Wobei hier zu unterscheiden ist, ob es sich bei dem Restklassenring um einen Körper oder Nicht-Körper handelt. In den folgenden Kapiteln wird dies behandelt und einige Verfahren zum Lösen linearer Gleichungssysteme modulo T vorgestellt.
Zunächst werden lineare diophantische Gleichungssysteme eingeführt, um den Definitionsbereich auf ganze Zahlen zu beschränken.

3 Lineare diophantische Gleichungssysteme

In diesem Kapitel werden lineare diophantische Gleichungssysteme vorgestellt und zwei Lösungsverfahren, welche auch zum Berechnen linearer Gleichungssysteme modulo T $\in \mathbb{N}$ verwendet werden können, betrachtet. Dafür werden die zwei Normalformen, die Hermite- und Smith-Normalform, eingeführt. Als Literatur für dieses Kapitel wurde [1] genutzt.

3.0.1.Definition: *Lineare diophantische Gleichungssysteme* sind lineare Gleichungssysteme mit nur ganzzahligen Koeffizienten und Lösungen.

Hier gilt ebenfalls die übliche Matrix-Vektor-Schreibweise:

$$A\vec{x} = \vec{b} \text{ wobei } A \in (\mathbb{Z})^{m\times n} \text{ und } \vec{x} \in (\mathbb{Z})^n, \vec{b} \in (\mathbb{Z})^m$$

Lineare diophantische Gleichungssysteme lassen sich mit Hilfe von zwei Normalformen berechnen: Die Hermite- und die Smith-Normalform.

Bevor diese Normalformen beschrieben werden, wird erst einmal der euklidische Algorithmus (GCD) näher betrachtet. Dieser bildet eine wichtige Grundlage zur Berechnung beider Normalformen. Anders als der erweiterte euklidische Algorithmus berechnet der euklidische Algorithmus nur den größten gemeinsamen Teiler zweier natürlicher Zahlen. Durch die Verwendung des Algorithmus können Matrixeinträge nur durch unimodulare Spaltenumformungen eliminiert werden. Diese sind:

- Vertauschung zweier Spalten
- Multiplikation einer Spalte mit ± 1
- Addition eines von Null verschiedenen Vielfachen einer Spalte zu einer anderen

Zur Wiederholung des euklidischen Algorithmus und zur Veranschaulichung des Eliminationsverfahren durch diesen wird folgendes Beispiel betrachtet.

Sei $A = \begin{pmatrix} 20 & 108 \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}^{2x2}$. Durch ausschließlich unimodulare Spaltenoperationen soll der Eintrag oben rechts, a_{12} mit Hilfe des euklidischen Algorithmus eliminiert werden. Dafür wird der größte gemeinsame Teiler von 20 und 108 berechnet. Man geht wie folgt vor:

Die größere Zahl wird durch die kleinere geteilt und der ganzzahlige Rest wird dann der neue Divisor, der den alten teilt.

$108 = 5 * 20 + 8$
$20 = 2 * 8 + 4$
$8 = 2 * 4 + 0$. Somit ist der größte gemeinsame Teiler 4.

Die farbig markierten Zahlen geben an, welches Vielfache der ersten/zweiten Spalte man von der anderen Spalte abzieht.

$$\begin{pmatrix} 20 & 108 \\ 0 & 1 \end{pmatrix} \xrightarrow{\text{II. - 5 I.}} \begin{pmatrix} 20 & 8 \\ 0 & 1 \end{pmatrix} \xrightarrow{\text{I. - 2 II.}} \begin{pmatrix} 4 & 8 \\ -2 & 1 \end{pmatrix} \xrightarrow{\text{II. - 2 I.}} \begin{pmatrix} 4 & 0 \\ -2 & 3 \end{pmatrix}$$

Der gewünschte Eintrag wurde eliminiert.

Nachdem nun alle nötigen Grundlagen wiederholt wurden, können die Normalformen eingeführt werden.

3.1 Hermite-Normalform

Charles Hermite formulierte 1851 erstmals eine Definition für die Hermite-Normalform und diese wurde nachträglich nach ihm benannt. Mittlerweile gibt es eine Vielzahl an Definitionen. Diese Arbeit richtet sich nach der Definition von [1].

3.1.1 Definition: Sei $A \in \mathbb{Z}^{mxn}$ eine Matrix mit vollem Zeilenrang. A ist in der Hermite-Normalform (HNF), wenn sie die Form $(B\ 0)$ hat, wobei gilt:

- B ist nicht singulär, nicht negativ und eine untere Dreiecksmatrix.
- Jede Zeile von B hat ein eindeutiges maximales Element auf der Hauptdiagonalen.

Die Hermite-Normalform von A sieht demnach folgendermaßen aus:

$$HNF(A) = \begin{pmatrix} b_{11} & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & & \vdots \\ b_{m1} & \cdots & b_{mm} & 0 & \cdots & 0 \end{pmatrix},$$

wobei die $b_{ij} > 0\ \forall i, j,\ i \in [1, m], j \in [1, n]$ und $b_{ii} > b_{ij}$ wobei $i > j$.

Außerdem existiert eine unimodulare Matrix $C \in \mathbb{Z}^{nxn}$, sodass $HNF(A) = AC$, wobei C die Spaltenumformungen speichert, die an A durchgeführt werden.

3.1.2 Satz: Jede ganzzahlige Matrix mit vollem Rang kann durch unimodulare Spaltenumformungen in die Hermite-Normalform gebracht werden.

Beweis: Der Satz wird durch die Vorstellung des Algorithmus zur Berechnung der Hermite-Normalform bewiesen:

Sei $A \in \mathbb{Z}^{mxn}$ gegeben

Schritt 1: Man betrachtet die erste Zeile von A und eliminiert alle Elemente rechts vom Diagonalelement mit Hilfe des GCD.

Schritt 2: Falls das Diagonalelement negativ ist, wird die erste Spalte mit -1 multipliziert. Falls nicht, weiter mit Schritt 3.

Schritt 3: Die zweite Zeile wird nun betrachtet und alle Elemente rechts vom Diagonalelement mit Hilfe des GCD eliminiert.

Schritt 4: Falls das Diagonalelement negativ ist, wird die zweite Spalte mit -1 multipliziert. Falls nicht, weiter mit Schritt 5.

Schritt 5: Falls das Element links vom Diagonalelement kleiner als das Diagonalelement ist, wird normalisiert.

Die Schritte 3-5 werden für die Zeilen i=3 bis n wiederholt. □

Somit ist die Existenz der Hermite-Normalform für jede ganzzahlige Matrix mit vollem Rang garantiert. Wie man mit Hilfe der Hermite-Normalform nun ein lineares diophantisches Gleichungssystem löst, wird im folgenden Abschnitt diskutiert.

3.1.3 Lösen linearer diophantischer Gleichungssysteme mit HNF

Sei $A\vec{x} = \vec{b}$, wobei $A \in \mathbb{Z}^{m\times n}$, $\vec{x} \in \mathbb{Z}^n$ und $\vec{b} \in \mathbb{Z}^m$ das zu lösende lineare diophantische Gleichungssystem.

Sei $HNF(A) = AC$ die bereits berechnete Hermite-Normalform von A und C die unimodulare Matrix. Dann löst man ein lineares diophantisches Gleichungssystem mit der Hermite-Normalform wie folgt:

Schritt i: $HNF(A) = AC$ wird nach A umgeformt, sodass gilt $A = HNF(A)C^{-1}$.

Schritt ii: $A = HNF(A)C^{-1}$ wird in das lineare diophantische Gleichungssystem $A\vec{x} = \vec{b}$ eingesetzt und man erhält $HNF(A)C^{-1}\vec{x} = \vec{b}$.

Schritt iii: $C^{-1}\vec{x}$ wird als ein Vektor $\vec{y} \in \mathbb{Z}^n$ definiert, sodass $HNF(A)\vec{y} = \vec{b}$ gilt.

Schritt iv: $\vec{y}$ kann durch Vorwärtssubstitution bestimmt werden.

Schritt v: $\vec{y} = C^{-1}\vec{x}$ wird nach $\vec{x}$ umgestellt, sodass $\vec{x}$ durch $\vec{x} = C\vec{y}$ berechnet werden kann.

Nachdem der Algorithmus zum Lösen linearer diophantischer Gleichungssysteme mit Hilfe der Hermite-Normalform vorgestellt wurde, wird im folgenden Abschnitt die Lösbarkeit und Eindeutigkeit einer Lösung diskutiert.

3.1.4 Lösbarkeit linearer diophantischer Gleichungssysteme mit HNF

Die Lösbarkeit eines linearen diophantischen Gleichungssystems mit Hilfe der Hermite-Normalform, lässt sich an der Hermite-Normalform ablesen.

Sowohl die unimodulare Matrix C als auch die Inverse C^{-1} haben ausschließlich ganzzahlige Einträge. Dann folgt daraus und aus *Schritt 4* (siehe Abschnitt 3.1.3) , dass $\vec{y}$ genau dann ganzzahlige Einträge besitzen kann und damit bestimmbar ist, wenn auch $\vec{x}$ ausschließlich ganzzahlige Einträge enthält.
Dies bedeutet, dass das lineare diophantische Gleichungssystem $A\vec{x} = \vec{b}$ genau dann lösbar,

wenn ein $\vec{y} \in \mathbb{Z}^n$ existiert, sodass $HNF(A)\vec{y} = \vec{b}$. Das ist genau dann der Fall, wenn jeder Eintrag aus der i-ten Zeile der Hermite-Normalform den i-ten Eintrag des Vektors $\vec{b}$ ohne Rest teilt.
Die Lösungsmenge ist genau dann eindeutig, wenn, zusätzlich zu den bereits genannten Bedingungen, der Rang von A der Anzahl der Unbekannten entspricht. Folgende Proposition fasst das gesagte formal zusammen.

3.1.4.1 Proposition Sei $A\vec{x} = \vec{b}$, wobei $A \in \mathbb{Z}^{m\times n}$ und $\vec{x} \in \mathbb{Z}^n, \vec{b} \in \mathbb{Z}^m$, ein lineares diophantisches Gleichungssystem. Sei weiterhin $(h_{ij}) = HNF(A) = AC$ die Hermite-Normalform von A und C die unimodulare Matrix. Außerdem sei $\vec{y}$ definiert als $\vec{y} := C^{-1}\vec{x}$. Dann gilt:

$$A\vec{x} = \vec{b} \text{ ist lösbar } \Leftrightarrow \exists \vec{y} \in \mathbb{Z}^n \text{ sodass } HNF(A)\vec{y} = \vec{b} \Leftrightarrow h_{ij} | b_i \forall i \in [1, m]$$

und

$$A\vec{x} = \vec{b} \text{ ist eindeutig lösbar } \Leftrightarrow A\vec{x} = \vec{b} \text{ ist lösbar und } rang(A) = n.$$

Nachdem der Lösungsweg, sowie die Bedingungen zur Existenz und Eindeutigkeit der Lösungen erläutert wurden, wird dies anhand eines Beispiels veranschaulicht.

3.5 Beispiel: Gesucht ist die Lösungsmenge für das lineare diophantische Gleichungssystem

$$A\vec{x} = \vec{b} \text{ mit } A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 5 & -10 & 2 \end{pmatrix} \in \mathbb{Z}^{3x4},\ \vec{b} = \begin{pmatrix} -5 \\ 0 \\ 2 \end{pmatrix} \in \mathbb{Z}^3,\ \vec{x} \in \mathbb{Z}^4$$

Schritt 1: In der ersten Zeile sind alle Elemente rechts vom Diagonalelement bereits Null.

Schritt 2: Man betrachte $a_{11} = 1 > 0$. Das Diagonalelement ist positiv und somit kann mit Schritt 3 fortgefahren werden

Schritt 3:
$$\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 5 & -10 & 2 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \xrightarrow{\text{IV.-6II.}} \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & -10 & -28 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Die Einträge rechts vom Diagonalelement in der zweiten Zeile wurden eliminiert.

Schritt 4: Man betrachte $a_{22} = 1 > 0$. Das Diagonalelement ist positiv, weiter mit Schritt 5.

Schritt 5: Man betrachte die Elemente links vom Diagonalelement. $a_{21} = 0 < 1 = a_{22}$. Der Eintrag links vom Diagonalelement ist kleiner als das Diagonalelement selbst. Weiter mit der dritten Zeile.

Schritt 6: $\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & -10 & -28 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \overset{\text{IV.-2III.}}{\Longrightarrow} \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & -10 & -8 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 \end{array}\right) \overset{\text{III.-IV.}}{\Longrightarrow} \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & -2 & -8 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 6 & -6 \\ 0 & 0 & 3 & -2 \\ 0 & 0 & -1 & 1 \end{array}\right)$

$\overset{\text{IV.-4III.}}{\Longrightarrow} \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & -2 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 6 & -30 \\ 0 & 0 & 3 & -14 \\ 0 & 0 & -1 & 5 \end{array}\right)$. Der Eintrag rechts vom Diagonalelement wurde eliminiert.

Schritt 7: $a_{33} = -2 < 0$. Der Diagonaleintrag ist negativ. Die dritte Spalte wird mit -1 multipliziert:

$\overset{\text{-1III.}}{\Longrightarrow} \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 5 & 2 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & -6 & -30 \\ 0 & 0 & -3 & -14 \\ 0 & 0 & 1 & 5 \end{array}\right)$.

Schritt 8: Man betrachte $a_{31} = 0 < 2 = a_{33},\ a_{32} = 5 > 2 = a_{33}$ Der Eintrag a_{32} ist kleiner als das Diagonalelement.

Normalisierung: II.-2III.: $\left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 13 & -6 & -30 \\ 0 & 6 & -3 & -14 \\ 0 & -2 & 1 & 5 \end{array}\right) = \left(\begin{array}{c} HNF(A) \\ \hline C \end{array}\right)$.

Sowohl die Hermite-Normalform als auch die unimodulare Matrix C wurden bestimmt. An dieser Stelle kann die Existenz von Lösungen festgestellt werden. Dazu können die Hermite-Normalform und der Vektor $\vec{b}$ betrachtet werden.

$$HNF(A) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix},\ \vec{b} = \begin{pmatrix} -5 \\ 0 \\ 2 \end{pmatrix}.$$

Offensichtlich teilt jeder Beitrag aus der i-ten
Zeile der Hermite-Normalform den i-ten Beitrag von $\vec{b}$: $1|-5,\ \ 1|0,\ \ 1|2$ und $\ \ 2|2$.
Laut Proposition 3.1.4.1 existiert mindestens eine Lösung zu $A\vec{x} = \vec{b}$.
Für die Eindeutigkeit wird der Rang der Hermite-Normalform betrachtet. Der Rang kann

an der Anzahl der von Null verschiedenen Zeilen abgelesen werden: $rang(HNF(A)) = 3$. Die Anzahl der gesuchten Unbekannten ist 4. Also gilt:

$$rang(HNF(A)) = 3 \neq 4 = \text{Anzahl der Unbekannten.}$$

Somit ist die Lösungsmenge nicht eindeutig.

Mit Hilfe der Hermite-Normalform und der unimodularen Matrix C wird nun das lineare diophantische Gleichungssystem gelöst.

Schritt i: Es wird nach A umgestellt.
$HNF(A) = AC \Leftrightarrow A = HNF(A)C^{-1}$

Schritt ii: $A = HNF(A)C^{-1}$ wird in das ursprüngliche Problem eingesetzt.
$A\vec{x} = \vec{b} \Leftrightarrow HNF(A)C^{-1}\vec{x} = \vec{b}$.

Schritt iii: Definiere $\vec{y}$ als $\vec{y} := C^{-1}\vec{x}$ Dann gilt

$$HNF(A)\vec{y} = \vec{b} \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} -5 \\ 0 \\ 2 \end{pmatrix}$$

Schritt iv: Durch Vorwärtssubstitution wird $\vec{y}$ bestimmt.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} -5 \\ 0 \\ 2 \end{pmatrix} \Leftrightarrow \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} -5 \\ 0 \\ 1 \\ a \end{pmatrix},\ a \in \mathbb{N}.$$

Schritt v: Die Lösung $\vec{x}$ kann schließlich durch $\vec{x} = C\vec{y}$ bestimmt werden.

$$\vec{x} = C\vec{y} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 13 & -6 & -30 \\ 0 & 6 & -3 & -14 \\ 0 & -2 & 1 & 5 \end{pmatrix} \begin{pmatrix} -5 \\ 0 \\ 1 \\ a \end{pmatrix} = \begin{pmatrix} -5 \\ -6 - 30a \\ -3 - 14a \\ 1 + 5a \end{pmatrix},\ a \in \mathbb{N}.$$

Somit ist die Lösungsmenge $L = \{ \begin{pmatrix} -5 \\ -6 - 30a \\ -3 - 14a \\ a + 5a \end{pmatrix} \mid a \in \mathbb{N} \}$.

Wie erwartet ist die Lösungsmenge nicht eindeutig. Die Lösung hängt von einem Parameter a ab.

Die Hermite-Normalform ist eine von zwei Verfahren, die in dieser Bachelorarbeit zur Berechnung linearer diophantischer Gleichungssysteme vorgestellt werden. Wie in Satz 3.1.2. gezeigt, ist es möglich die Hermite-Normalform zu jeder ganzzahligen Matrix mit vollem Rang zu bilden. Dies bedeutet auch, dass es möglich ist, die Hermite-Normalform in

jedem linearen diophantischen Gleichungssystem zu bilden. Wie an dem Beispiel verdeutlicht, kann mit wenig Aufwand direkt an der Hermite-Normalform die Existenz und Eindeutigkeit von Lösungen abgelesen werden.
Eine ähnliche Methode bietet die Smith-Normalform.

3.2 Smith-Normalform

In diesem Kapitel wird die Smith-Normalform, ein weiteres Verfahren zur Berechnung linearer diophantischer Gleichungssysteme, vorgestellt. Die Smith-Normalform wurde nach Henry John Stephen Smith (1826-1883) benannt und wird folgendermaßen definiert.

3.2.1 Definition: Sei $S \in \mathbb{Z}^{m \times n}$ eine Matrix mit vollem Zeilenrang. Dann ist S in der *Smith-Normalform*(SNF), wenn

- S ist eine Diagonalmatrix mit positiven Einträgen
- Die Diagonalelemente von S sind Elementarteiler, das heißt $s_{ii}|s_{jj} \forall i < j$

Die Smith-Normalform von A hat demnach folgende Gestalt :

$$SNF(A) = \begin{pmatrix} s_{11} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & 0 & s_{mm} & 0 & \cdots & 0 \end{pmatrix}, s_{ii} > 0,\ s_{ii}|s_{jj} \forall i < j;\ i, j \in [1, m].$$

Anders als bei der Hermite-Normalform sind bei der Berechnung der Smith-Normalform unimodulare Spalten- und Zeilenumformungen zugelassen. Aus diesem Grund brauchen wir auch zwei unimodulare Matrizen $U, V \in \mathbb{Z}^{nxn}$, wobei U die Spaltenumformungen und V die Zeilenumformungen speichert. Dann gilt: $SNF(A) = VAU$.
Auch die Existenz der Smith-Normalform ist für Matrizen mit vollem Zeilenrang garantiert.

3.2.2 Satz: Jede ganzzahlige Matrix A mit vollem Zeilenrang kann durch unimodulare Spalten- und Zeilenoperationen in die Smith-Normalform gebracht werden.

Beweis: Ebenfalls wie bei der Hermite-Normalform wird der Satz mittels des Algorithmus bewiesen.

Schritt 1:

- Ein Eintrag s wird in A hergestellt, der alle anderen Einträge in A teilt. $(*)$
- s wird in den ersten Diagonaleintrag a_{11} gesetzt.
- Alle Einträge in der ersten Zeile und Spalte werden bis auf s mit Hilfe GCD eliminiert

Schritt 2: Weiter per Induktion.

Doch wie wird $(*)$ verwirklicht?

Sei s ein Eintrag in A mit einer minimalen Anzahl an Primfaktoren in S. Zwei Fälle sind zu unterscheiden.

Fall 1: s teilt alle Einträge. In diesem Fall wäre $(*)$ bereits erfüllt.

Fall 2: Es existiert ein Eintrag t in A, den s nicht teilt. Dann kämen ebenfalls zwei Fälle in Frage.

> Guter Fall 2.1: t ist in der selben Zeile/Spalte wie s. Dann kann der euklidische Algorithmus angewandt und der Eintrag t auf einen gemeinsamen Teiler reduziert werden.
>
> Schlechter Fall 2.2: t ist nicht in der selben Zeile/Spalte wie s. In der Zeile und Spalte von s seien nur s-Vielfache (falls nicht $\rightarrow$ Fall 2.1). Dann können alle Elemente bis auf s in dieser Zeile und Spalte eliminiert werden, sodass:
>
> $$A = \begin{pmatrix} & 0 & & & \\ & \vdots & & & \\ 0 \cdots & s & 0 & \cdots & 0 \\ & 0 & & & \\ & \vdots & t & & \\ & 0 & & & \end{pmatrix}.$$
>
> Durch unimodulare Zeilenoperationen erhält man:
>
> $$\begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix} \rightarrow \begin{pmatrix} s & 0 \\ s & t \end{pmatrix} \rightarrow \text{ Fall 2.1} \qquad \square$$

Damit ist gezeigt, dass jede ganzzahlige Matrix mit vollem Zeilenrang durch unimodulare Zeilen- und Spaltenumformungen in die Smith-Normalform gebracht werden kann.

Die Frage nach der Existenz und Eindeutigkeit von Lösungen zu linearen diophantischen Glei- chungssystemen wird im folgenden Abschnitt diskutiert.

3.2.3 Lösbarkeit linearer diophantischer Gleichungssysteme mit SNF

Sei $A\vec{x} = \vec{b}$ das zu lösende lineare diophantische Gleichungssystem, wobei $A \in \mathbb{Z}^{mxn}$ $\vec{x} \in \mathbb{Z}^n$ und $\vec{b} \in \mathbb{Z}^m$. Weiterhin sei $SNF(A)$ die bereits berechnete Smith-Normalform von A und V sowie U die unimodularen Matrizen mit $SNF(A) = VAU$.
Dann löst man ein lineares diophantisches Gleichungssystem mit der Smith-Normalform wie folgt.

Schritt i: An die Gleichung $A\vec{x} = \vec{b}$ wird von links die unimodulare Matrix V multipliziert, sodass gilt $VA\vec{x} = V\vec{b}$

Schritt ii: Ein Vektor $\vec{y} \in \mathbb{Z}^n$ wird definiert als $\vec{y} := U^{-1}\vec{x}$, sodass gilt $VAU\vec{y} = V\vec{b}$.
Aus $SNF(A) = VAU$ folgt $SNF(A)\vec{y} = V\vec{b}$.

Schritt iii: Ein weiterer Vektor $\vec{z}$ wird zur Einfachheit definiert als $\vec{z} := V\vec{b}$,

wobei $\vec{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix}$.

Schritt iv: $SNF(A)$ ist eine Diagonalmatrix mit $SNF(A) = diag(d_1, ...d_m)$.
Der Vektor $\vec{y}$ kann folglich durch Vor- oder Rückwärtssubstitution bestimmt werden.

Schritt v: Die Lösung $\vec{x}$ wird durch $\vec{x} = U\vec{y}$ berechnet.

Die Existenz und Eindeutigkeit einer Lösung kann bereits in *Schritt ii* ermittelt werden. Weil die Smith-Normalform eine Diagonalmatrix mit ganzzahligen Einträgen ist, existiert genau dann eine Lösung $\vec{y}$ zu $SNF(A)\vec{y} = \vec{z}$, wenn jeder Eintrag aus der i-ten Zeile der Smith-Normalform von A den i-ten Eintrag des Vektors $\vec{z}$ ohne Rest teilt. Weiterhin ist das lineare diophantische Gleichungssystem $A\vec{x} = \vec{b}$ genau dann lösbar, wenn auch das lineare diophantische Gleichungssystem $SNF(A)\vec{y} = \vec{z}$ lösbar ist. Die Lösung ist genau dann eindeutig, wenn zusätzlich der Rang von A der Anzahl der Unbekannten entspricht. Der Rang von A kann an der Smith-Normalform abgelesen werden.

3.2.3.1 Proposition: Sei $A\vec{x} = \vec{b}$, wobei $A \in \mathbb{Z}^{m \times n}$ und $\vec{x} \in \mathbb{Z}^n, \vec{b} \in \mathbb{Z}^m$ ein lineares diophantisches Gleichungssystem. Sei weiterhin $(d_{ii}) = SNF(A) = VAC$ die Smith-Normalform von A, wobei V und U die zugehörigen unimodularen Matrizen sind.
Außerdem sei $\vec{y}$ definiert als $\vec{y} := U^{-1}\vec{x}$ und $\vec{z}$ als $\vec{z} := V\vec{b}$. Dann gilt

$$A\vec{x} = \vec{b} \text{ ist } \textit{lösbar} \Leftrightarrow \exists\, \vec{y} \in \mathbb{Z}^n \text{ sodass } SNF(A)\vec{y} = \vec{z} \Leftrightarrow d_i | z_i \ \forall i \in [1, m].$$

und

$$A\vec{x} = \vec{b} \text{ ist } \textit{eindeutig lösbar} \Leftrightarrow A\vec{x} = \vec{b} \text{ ist lösbar und } rang(A) = n.$$

Zur Verdeutlichung und zum Verständnis wird ein Beispiel vorgeführt.

3.2.4 Beispiel: Gesucht ist die Smith-Normalform der Matrix $A = \begin{pmatrix} 4 & 8 & 12 \\ 8 & 6 & -4 \end{pmatrix} \in \mathbb{Z}^{2x3}$ sowie die zugehörigen unimodularen Matrizen $U \in \mathbb{Z}^{3x3}$ und $V \in \mathbb{Z}^{2x2}$.

Schritt 1: Die 4 teilt, bis auf die 6, alle Einträge aus A. Der größte gemeinsame Teiler dieser beiden Zahlen ist $ggT(4, 6) = 2$ und die 2 teilt alle Einträge in A.
Da $ggt(8, 6) = 2$, kann mit Hilfe des euklidischen Algorithmus durch unimodulare Zeilen- und Spaltenumformungen die 2 erzeugt werden:

$$\left(\begin{array}{ccc|cc} 4 & 8 & 12 & 1 & 0 \\ 8 & 6 & -4 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \Rightarrow \left(\begin{array}{ccc|cc} -4 & 2 & 16 & 1 & -1 \\ 8 & 6 & -4 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right)$$

Nun wird die 2 in den ersten Diagonaleintrag gebracht:

$$\left(\begin{array}{ccc|cc} 2 & -4 & 16 & 1 & -1 \\ 6 & 8 & -4 & 0 & 1 \\ \hline 0 & 1 & 0 & & \\ 1 & 0 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right).$$

Jetzt können alle Einträge in der ersten Zeile und Spalte bis auf die 2 eliminiert werden und man erhält:

$$\left(\begin{array}{ccc|cc} 2 & 0 & 0 & 1 & -1 \\ 0 & 20 & -52 & -3 & 4 \\ \hline 0 & 1 & 0 & & \\ 1 & 2 & -8 & & \\ 0 & 0 & 1 & & \end{array}\right).$$

Schritt 2: Elimination aller Einträge in der zweiten Zeile bis auf das Diagonalelement:

$$\left(\begin{array}{ccc|cc} 2 & 0 & 0 & 1 & -1 \\ 0 & 4 & 0 & -3 & 4 \\ \hline 0 & -5 & 13 & & \\ 1 & 6 & -14 & & \\ 0 & -2 & 5 & & \end{array}\right) = \left(\begin{array}{c|c} S & V \\ \hline U & \end{array}\right)$$

S hat wie erwünscht ausschließlich positive Einträge, die Elementarteiler sind. Damit ist SNF(A) eindeutig bestimmt.

In diesem Kapitel wurden zwei Möglichkeiten zum Lösen lineare diophantische Gleichungssysteme präsentiert. Da sich diese Arbeit insbesondere mit den linearen Gleichungssystemen über Restklassenringen $\mathbb{Z}/T\mathbb{Z}$ für T nicht prim beschäftigt, widmet sich folgendes Kapitel genau diesem Inhalt. Dazu werden relevante Informationen vermittelt. Anschließend werden mögliche Lösungsansätze vorgestellt und Beispiele herangezogen.

4 Lineare Gleichungssysteme modulo T

Nachdem das nötige Wissen für das Hauptthema dieser Bachelorarbeit in den vorherigen Kapitel angeeignet wurde, werden nun lineare Gleichungssysteme modulo T behandelt. Es wird zunächst anhand eines Beispiels das eigentliche Problem, welches die Verwendung des Gauß-Algorithmus auf lineare Gleichungssysteme modulo T einschränkt, geschildert. Anschließend werden die Rechenverfahren, die in den vorherigen Kapitel vorgestellt wurden, auf lineare Gleichungssysteme modulo T angewandt und Bedingungen zur Existenz und Eindeutigkeit der Lösungen dieser Verfahren aufgestellt. Jedes Verfahren wird zusätzlich mit einem Beispiel veranschaulicht. Literatur bezüglich linearen Gleichungssystemen über Restklassenringe ist nicht auffindbar. Lineare Gleichungssysteme über einen Restklassenring $\mathbb{Z}/T\mathbb{Z}$ sind lineare diophantische Gleichungssysteme, bei denen sowohl die Koeffizienten als auch die Lösungen auf modulo T reduziert werden. Prinzipiell kann man diese mit Hilfe der in dieser Arbeit bereits vorgestellten Verfahren lösen. Eine weitere Möglichkeit bietet der Chinesische Restsatz, der zum Abschluss dieses Kapitels erläutert wird. In Kapitel 2.2 wurde bereits ein Beispiel zum Lösen linearer Gleichungssysteme bei Restklassenkörper vorgeführt. Die Koeffizientenmatrix wurde wie gewohnt in die Zeilenstufenform gebracht und die Lösung wurde anschließend durch Vorwärtssubstitution ermittelt.
Betrachtet man Restklassenringe, die keinen Körper bilden, funktioniert diese Vorgehensweise nicht garantiert. Dies wird mit folgendem Beispiel illustriert:

4.0.1 Beispiel: Sei $A = \begin{pmatrix} 6 & 8 \\ 5 & 5 \end{pmatrix} \in \mathbb{Z}/10\mathbb{Z}$.

Bei dem Gauß-Algorithmus wird üblicherweise die Zeilenstufenform berechnet, in dem alle Einträge unterhalb des Diagonalelements von A mit dem Pivotelement eliminiert werden. In diesem Fall kann die 5 nicht durch ein Vielfaches der 6 modulo 10 eliminiert werden, da 5 und 6 teilerfremd sind.
Eine weitere Möglichkeit wäre, die Zeile mit einem Nullteiler zu multiplizieren. Jedoch würde dies in diesem Beispiel zu einer Veränderung des Rangs führen:

$$\begin{pmatrix} 6 & 1 \\ 5 & 5 \end{pmatrix} \overset{2\cdot \text{II.}}{\Longrightarrow} \begin{pmatrix} 6 & 1 \\ 0 & 0 \end{pmatrix}.$$

Wie kann dieses Problem umgangen werden?

Offensichtlich kann der Gauß-Algorithmus bei solchen Gegebenheiten nicht zur Bestimmung einer Lösung verwendet werden. Es muss auf andere Verfahren zurückgegriffen werden. Die Hermit- und Smith-Normalform wurden bereits im vorigen Kapitel eingeführt und bilden jeweils eine gute Alternative.

Bei linearen Gleichungssystemen über Restklassenringe, die keine Körper bilden, wird ebenfalls zwischen homogenen und inhomogenen linearen Gleichungssystemen unterschieden. Diese ähneln den in Kapitel 2 bereits eingeführten Definitionen.

4.0.2 Definition: Sei $A\vec{x} \equiv_T \vec{b}$ ein lineares Gleichungssystem, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}$, $\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$, $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$ und T nicht prim ist.

Sei weiterhin $\vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. Falls $b_i \equiv_T 0 \; \forall i \in [1, m]$ gilt, so handelt es sich um ein *homogenes* lineares Gleichungssystem. Existiert mindestens ein $b_i \not\equiv_T 0$, so liegt ein *inhomogenes* lineares Gleichungssystem vor.

Aus dieser Definition lassen sich bereits einige Aussagen bezüglich der Existenz von Lösungen in linearen Gleichungssystemen modulo T treffen.

4.0.3 Proposition: Homogene lineare Gleichungssysteme $A\vec{x} \equiv_T \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ über Restklassenringe $\mathbb{Z}/T\mathbb{Z}$ haben mindestens eine Lösung, der Form $\vec{x} \equiv_T \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Inhomogene lineare Gleichungssysteme, wie beispielsweise $A\vec{x} \equiv_T \vec{b} \not\equiv_T 0$, besitzen hingegen nicht immer eine Lösung.

Die Existenz- und Eindeutigkeitsbedingungen sind mit den verschiedenen Lösungsverfahren verknüpft. Es lässt sich nicht im Allgemeinen sagen, wann eine Lösung zu einem linearen Gleichungssystem modulo T existiert und wann diese eindeutig ist. Welche Bedingungen erfüllt sein müssen, werden in Abhängigkeit der Verfahren erläutert.

4.1 Gauß-Algorithmus

In diesem Kapitel wird der Gauß-Algorithmus in Bezug auf lineare Gleichungssysteme über Restklassenringe, die keine Körper bilden, vorgestellt. Es wird auf die Existenz- und Eindeutigkeitsbedingungen eingegangen, der Algorithmus wiederholt und an einem Beispiel vorgeführt.

Der Gauß-Algorithmus dient als häufig verwendeter Algorithmus zur Berechnung linearer Gleichungssysteme. Über Restklassenringe, die keinen Körper bilden, kann dieses Verfahren jedoch aufwendig oder ungünstig sein, wie in Beispiel 4.0.1 gezeigt wurde. Bei größeren Matrizen ist es von vornherein oft nicht ersichtlich, ob die Matrix in Zeilenstufenform ausschließlich durch Zeilenumformungen in Zeilenstufenform überführt werden kann.

Existiert die Zeilenstufenform und wurde die Matrix in diese Form gebracht, dann kann die Lösung durch Rückwärts- oder Vorwärtssubstitution bestimmt werden.

4.1.1 Existenz und Eindeutigkeit von Lösungen

Die Existenz- und Eindeutigkeitsbedingungen von Lösungen bei dem Gauß-Verfahren über Körper reichen über Restklassenringe $\mathbb{Z}/T\mathbb{Z}$, die keine Körper bilden, nicht mehr aus. Es muss zusätzlich darauf geachtet werden, dass die ganzzahlige Eigenschaft aller Beiträge erhalten bleibt. Dies wird durch die Teilbarkeit von jedem Eintrag aus der i-ten Spalte der Zeilenstufenform und dem i-ten Eintrag des Lösungsvektors garantiert. Das lineare Gleichungssystem besitzt erst dann mindestens eine Lösung. Gilt zusätzlich, dass jeder

Eintrag der Zeilenstufenform teilerfremd zu T ist, dann besitzt das lineare Gleichungssystem eine eindeutige Lösung. Diese Bedingungen sind lediglich hinreichend.

4.1.1.1 Proposition: Sei $A\vec{x} \equiv_T \vec{b}$ das zu lösende lineare Gleichungssystem, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}$, $\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$, $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$ und T nicht prim ist. Sei weiterhin $(a_{ij})' = A'$ die Zeilenstufenform von A. Dann gilt:

$$A\vec{x} \equiv_T \vec{b} \text{ ist } \textit{lösbar}, \text{ wenn } rang(A) = rang(A|\vec{b}) \text{ und } a'_{ij}|b'_i \; \forall\, i \in [1,m].$$

$$A\vec{x} \equiv_T \vec{b} \text{ ist eindeutig lösbar, wenn } A\vec{x} \equiv_T \vec{b} \text{ lösbar ist und } ggT(a_{ij}, T) = 1,$$
$$\forall i \in [1,m], j \in [1,n].$$

4.1.2 Algorithmus: Die Vorgehensweise zur Bestimmung der Lösungsmenge eines linearen Gleichungssystems $A\vec{x} \equiv_T \vec{b}$ ist identisch zu der über Körper.

Schritt 1 (Zeilenstufenform): Die erweiterte Koeffizientenmatrix $(A|\vec{b})$ wird mit Hilfe elementarer Zeilenumformungen und dem euklidischen Algorithmus in die Zeilenstufenform überführt.

Schritt 2 (Vor-/Rückwärtssubstitution): Der Vektor $\vec{x}$ mit den Unbekannten wird durch Vor- oder Rückwärtssubstitution bestimmt.

4.1.3 Beispiel:

Sei $A \equiv_{10} \begin{pmatrix} 3 & 7 \\ 9 & 4 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^{2\times 2}$ und $\vec{b} \equiv_{10} \begin{pmatrix} 3 \\ 9 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^2$. Gesucht ist die Lösung $\vec{x} \in (\mathbb{Z}/10\mathbb{Z})^2$, sodass $A\vec{x} \equiv_{10} \vec{b}$.

Schritt 1: Sei $\left(\begin{array}{cc|c} 3 & 7 & 3 \\ 9 & 4 & 8 \end{array}\right)$ die erweiterte Koeffizientenmatrix. Durch Anwendung von einer elementaren Zeilenoperation kann die Zeilenstufenform bereits erzeugt werden:

$$\left(\begin{array}{cc|c} 3 & 7 & 3 \\ 9 & 4 & 8 \end{array}\right) \xRightarrow{\text{II.-3I.}} \left(\begin{array}{cc|c} 3 & 7 & 3 \\ 0 & 3 & -1 \end{array}\right) \equiv_{10} \left(\begin{array}{cc|c} 3 & 7 & 3 \\ 0 & 3 & 9 \end{array}\right).$$

Der Rang von A und von der Koeffizientenmatrix kann nun abgelesen werden. Es gilt

$$rang(A) = rang(A|\vec{b}) = 2.$$

Damit ist das lineare Gleichungssystem lösbar.
Weiterhin sind alle Einträge der Matrix teilerfremd zu $T = 10$. Die Lösung ist also eindeutig.

Schritt 2: Die Lösung wird durch Rückwärtssubstitution berechnet:

$$\begin{pmatrix} 3 & 7 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \equiv_{10} \begin{pmatrix} 3 \\ 9 \end{pmatrix}$$

$$3x_2 \equiv_{10} 9 \Leftrightarrow x_2 \equiv_{10} 3$$
$$3x_1 + 7x_2 \equiv_{10} 9 \Leftrightarrow 3x_1 + 1 \equiv_{10} 9 \Leftrightarrow 3x_1 \equiv_{10} 8 \Leftrightarrow x_1 \equiv_{10} 6.$$

Die Lösungsmenge L ist dann

$$L = \left\{ \begin{pmatrix} 6 \\ 3 \end{pmatrix} \right\}.$$

In diesem Kapitel wurde gezeigt, wie ein lineares Gleichungssystem über einen Restklassenring $\mathbb{Z}/T\mathbb{Z}$, mit Hilfe des Gauß-Algorithmus gelöst werden kann. Es wurde ein Beispiel vorgeführt, an dem der Gauß-Algorithmus problemlos funktioniert. Im Großen und Ganzen unterscheidet sich der Algorithmus nicht zu dem über Körper. Der Unterschied liegt viel mehr in der Existenz der Zeilenstufenform und den Bedingungen zur Existenz und Eindeutigkeit von Lösungen.

Man betrachte erneut das Beispiel 4.0.1. Nach den Vorschriften des Gauß-Algorithmus kann die Matrix A nicht in die Zeilenstufenform überführt werden, da das Pivotelement 6 teilerfremd zu 5 ist. In Kapitel 3 wurde der euklidische Algorithmus eingeführt, durch den Einträge eliminiert werden können, indem der größte gemeinsame Teiler bestimmt wird. Dasselbe Prinzip ist auch in diesem Fall anwendbar, indem der größte gemeinsame Teiler von 6 und 5 durch den erweiterten euklidischen Algorithmus bestimmt wird.

$$\begin{gathered} 6 \equiv_8 1 \cdot 5 + 1 \\ 5 \equiv_8 5 \cdot 1 + 0. \\ (\Rightarrow ggT(6,5) \equiv_8 1). \end{gathered}$$

Dass 6 und 5 teilerfremd sind, war bereits bekannt. Aus der Rechnung werden jedoch, wie in Kapitel 3 erläutert, die für die Zeilenstufenform erforderlichen Zeilenoperationen ersichtlich:

$$\begin{pmatrix} 6 & 1 \\ 5 & 5 \end{pmatrix} \xrightarrow{\text{I.-II.}} \begin{pmatrix} 1 & 4 \\ 5 & 5 \end{pmatrix} \xrightarrow{\text{II.-5I.}} \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}.$$

Prinzipiell wurde ausschließlich durch Anwendung von elementaren Zeilenoperationen die Zeilenstufenform berechnet. Der Gauß-Algorithmus sieht diese Vorgehensweise jedoch nicht vor, da hierbei das Pivotelement verändert wird.

Trotz dessen führt diese Vorgehensweise zur Zeilenstufenform, welche die Bestimmung der Lösung durch Vor- oder Rückwärtssubstitution ermöglicht. Dieses Verfahren wird bei der Hermite-Normalform genutzt, wobei statt Zeilenumformungen Spaltenumformungen durchgeführt werden. Wie ein Gleichungssystem modulo T explizit mit Hilfe der Hermite-Normalform berechnet werden kann, wird im folgenden Kapitel präsentiert.

4.2 Hermite-Normalform

Die Hermite-Normalform wurde bereits in Kapitel 3 vorgestellt. Sie wurde dazu genutzt, lineare diophantische Gleichungssysteme zu lösen. Über Restklassenringe $\mathbb{Z}/T\mathbb{Z}$ kann diese Normalform ebenfalls angewandt werden, um lineare Gleichungssysteme modulo T zu berechnen.

Allerdings existiert die Hermite-Normalform über Restklassenringe, im Gegensatz zu linearen diophantischen Gleichungssystemen, nicht zu jeder Matrix $A \in \mathbb{Z}/T\mathbb{Z}$, wie folgendes Beispiel zeigt.

Gegenbeispiel: Die Hermite-Normalform der Matrix $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 6 \\ 0 & 5 & -10 & 2 \end{pmatrix}$ ist $HNF(A) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 \end{pmatrix}$ (siehe Beispiel 3.1.4).

Betrachtet man die Matrix nun im Restklassenring $\mathbb{Z}/2\mathbb{Z}$, erhält man

$$HNF(A) \equiv_2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Diese Form entspricht nicht den in der Definition 3.1.1 genannten Eigenschaften einer Hermite-Normalform. Das größte Element in der dritten Zeile, die 1, ist nicht das Diagonalelement. Durch unimodulare Spaltenoperationen kann dies offensichtlich auch nicht behoben werden.

Um die Existenz der Hermite-Normalform über Restklassenringe zu garantieren, muss die Matrix $A \in \mathbb{Z}/T\mathbb{Z}$ vollen Zeilenrang besitzen.

Die Berechnung der Hermite-Normalform über Restklassenringe erfolgt völlig analog zu der über $\mathbb{Z}$. Hierbei kann zunächst über $\mathbb{Z}$ gerechnet werden und anschließend die Hermite-Normalform auf modulo T reduziert werden. Empfehlenswert ist es jedoch im Restklassenring zu rechnen, da so das Auftreten großer Zahlen verhindert werden kann.

4.2.1 Algorithmus

In diesem Abschnitt wird der Algorithmus zur Berechnung linearer Gleichungssysteme modulo T mit Hilfe der Hermite-Normalform vorgestellt.

Existiert die Hermite-Normalform für eine Matrix $A \in \mathbb{Z}/T\mathbb{Z}$, wird, wie in 3.1.3 für lineare diophantische Gleichungssysteme erläutert, vorgegangen, um lineare Gleichungssysteme über Restklassenringe zu lösen.

Sei $A\vec{x} \equiv_T \vec{b}$ das zu lösende lineare Gleichungssystem, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m \times n}$, $\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$ und $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$. Weiterhin sei $T \in \mathbb{N}$ und nicht prim.

Schritt 1 ***(Berechnung der Hermite-Normalform)*:** Durch unimodulare Spaltenoperationen wird die Hermite-Normalform mittels des euklidischen Algorithmus, wie im Beweis des Satzes 3.1.2 beschrieben, berechnet. Außerdem wird die unimodulare Matrix C bestimmt, welche die Spaltenumformungen speichert.

Schritt 2 ***(Äquivalente Umformungen)*:** $HNF(A) \equiv_T AC$ wird nach A umgeformt, sodass $A \equiv_T HNF(A)C^{-1}$ gilt. Eingesetzt in das lineare Gleichungssystem $A\vec{x} \equiv_T \vec{b}$ erhält man $HNF(A)C^{-1}\vec{x} \equiv_T \vec{b}$. Weiterhin wird $C^{-1}\vec{x}$ als $\vec{y} \in \mathbb{Z}^n$ definiert, sodass $HNF(A)\vec{y} \equiv_T \vec{b}$ gilt.

Schritt 3 ***(Berechnung von $\vec{y}$)*****:** $HNF(A)$ ist eine Matrix in der Zeilenstufenform. Der Vektor $\vec{y}$ kann folglich durch Vorwärtssubstitution bestimmt werden.

Schritt 4 ***(Bestimmung der Lösungsmenge)*****:** Die Lösung $\vec{x}$ wird durch $\vec{x} \equiv_T C\vec{y}$ berechnet. Abschließend kann die Lösungsmenge L wie folgt angegeben werden:

$$L = \{\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n | A\vec{x} \equiv_T \vec{b}\}.$$

4.2.2 Existenz und Eindeutigkeit von Lösungen

Die Existenz und Eindeutigkeit einer Lösung kann bereits in *Schritt 2* ermittelt werden. Weil die Hermite-Normalform eine Matrix in Zeilenstufenform mit ganzzahligen Einträgen ist, existiert eine Lösung $\vec{y}$ zu $HNF(A)\vec{y} \equiv_T \vec{b}$, wenn jeder Eintrag aus der i-ten Zeile der Hermite-Normalform von A den i-ten Eintrag des Vektors $\vec{b}$ ohne Rest teilt. Weiterhin ist das lineare Gleichungssystem $A\vec{x} \equiv_T \vec{b}$ genau dann lösbar, wenn auch das lineare Gleichungssystem $HNF(A)\vec{y} \equiv_T \vec{b}$ lösbar ist. Die Lösung ist genau dann eindeutig, wenn zusätzlich der Rang von A der Anzahl der Unbekannten entspricht und jeder Eintrag der Hermite-Normalform teilerfremd zu T ist.

4.2.2.1 Proposition: Sei $A\vec{x} \equiv_T \vec{b}$, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}, \vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$ und $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$ein lineares Gleichungssystem. Sei weiterhin $(h_{ij}) = HNF(A) \equiv_T AC$ die Hermite-Normalform von A, wobei C die zugehörige unimodularen Matrix ist. Außerdem sei $C^{-1}\vec{x}$ definiert als $C^{-1}\vec{x} :\equiv_T \vec{y}$. Dann gilt

$$A\vec{x} \equiv_T \vec{b} \text{ ist } \textit{lösbar} \Leftrightarrow \exists\, \vec{y} \in (\mathbb{Z}/T\mathbb{Z})^n \text{ sodass } HNF(A)\vec{y} \equiv_T \vec{b} \Leftrightarrow h_{ij}|b_i \;\forall i \in [1,m]$$

und

$$A\vec{x} = \vec{b} \text{ ist } \textit{eindeutig lösbar} \Leftrightarrow A\vec{x} = \vec{b} \text{ ist lösbar, } rang(A) = n \text{ und } ggT(h_{ij}, T) = 1 \; \forall i \in [1,m], j \in [1,n].$$

4.2.3 Beispiel: Sei $A = \begin{pmatrix} 3 & 6 \\ 7 & 5 \end{pmatrix} \in (\mathbb{Z}/8\mathbb{Z})^{2\times 2}$ und $\vec{b} = \begin{pmatrix} 6 \\ 1 \end{pmatrix} \in (\mathbb{Z}/8\mathbb{Z})^2$

Zu lösen ist das lineare Gleichungssystem $A\vec{x} = \vec{b},\ x \in \mathbb{Z}^2$.

Schritt 1: Die Matrix A wird durch unimodulare Spaltenumformungen in die Hermite-Normalform überführt. Hierfür wird zunächst der Eintrag in der ersten Zeile rechts vom Diagonalelement eliminiert. Dies wird durch Subtraktion des zweifachen der ersten Spalte von der zweiten Spalte erreicht:

$$\left(\begin{array}{cc} 3 & 6 \\ 7 & 5 \\ \hline 1 & 0 \\ 0 & 1 \end{array}\right) \xRightarrow{\text{II.-2I.}} \left(\begin{array}{cc} 3 & 0 \\ 7 & 7 \\ \hline 1 & 6 \\ 0 & 1 \end{array}\right).$$

Die Matrix ist jetzt zwar eine untere Dreiecksmatrix, jedoch muss in der zweiten Zeile das Element links vom Diagonalelement reduziert werden, sodass es kleiner als das Diagonalelement ist.
Hierfür wird die erste Spalte von der zweiten abgezogen:

$$\left(\begin{array}{cc} 3 & 0 \\ 7 & 7 \\ \hline 1 & 6 \\ 0 & 1 \end{array}\right) \xrightarrow{\text{I.-2II.}} \left(\begin{array}{cc} 3 & 0 \\ 0 & 7 \\ \hline 3 & 6 \\ 7 & 1 \end{array}\right) = \left(\begin{array}{c} HNF(A) \\ \hline C \end{array}\right).$$

Schritt 2: Definiere $C^{-1}\vec{x} := \vec{y}$, wobei $\vec{y} \in \mathbb{Z}^2$. Dann gilt:

$$HNF(A)\vec{y} \equiv_8 \vec{b} \Leftrightarrow \begin{pmatrix} 3 & 0 \\ 0 & 7 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv_8 \begin{pmatrix} 6 \\ 1 \end{pmatrix}.$$

Schritt 3: Der Vektor $\vec{y}$ kann sowohl durch Vorwärts- als auch durch Rückwärtssubstitution bestimmt werden, da die Hermite-Normalform Diagonalgestalt hat.

$$3y_1 \equiv_8 6 \Leftrightarrow y_1 \equiv_8 2$$
$$7y_2 \equiv_8 1 \Leftrightarrow y_2 \equiv_8 7.$$

Der Vektor $\vec{y}$ ist eindeutig bestimmt mit $\vec{y} \equiv_8 \begin{pmatrix} 2 \\ 7 \end{pmatrix}$. Somit existiert eine eindeutige Lösung zu $HNF(A)\vec{y} \equiv_8 \vec{b}$ und damit ist das lineare Gleichungssystem $A\vec{x} \equiv_8 \vec{b}$ ebenfalls eindeutig lösbar.

Schritt 4: Die Lösung $\vec{x}$ kann nun durch $\vec{x} \equiv_8 C\vec{y}$ bestimmt werden:

$$\vec{x} \equiv_8 C\vec{y} \equiv_8 \begin{pmatrix} 3 & 6 \\ 7 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 7 \end{pmatrix} \equiv_8 \begin{pmatrix} 0 \\ 5 \end{pmatrix}$$

Abschließend kann die Lösungsmenge L angegeben werden:

$$L = \left\{ \begin{pmatrix} 0 \\ 5 \end{pmatrix} \right\}.$$

4.3 Smith Normalform

In Kapitel 3.2 wurde die Smith-Normalform eingeführt und beschrieben, wie man lineare diophantische Gleichungssysteme mit Hilfe dieser löst. Ist die gegebene Matrix A in der Smith-Normalform, kann man recht schnell sehen, ob eine Lösung existiert und diese eindeutig ist. Dasselbe gilt für lineare Gleichungssysteme über Restklassenringe. Wir werden sehen, dass auch über Restklassenringe jede Matrix A in die Smith-Normalform gebracht werden kann. Nur hat hier die $SNF(A)$ nicht unbedingt vollen Zeilenrang. Was ändert sich in diesem Fall?
Zunächst einmal wird die Existenz der Smith-Normalform für alle Matrizen über Restklassenringe bewiesen.

4.3.1 Satz: Jede Matrix $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}$ kann in die Smith-Normalform überführt werden.

Beweis: Sei $A \in \mathbb{Z}^{mxn}$ eine Matrix mit vollem Zeilenrang. Dann existiert nach Satz 3.3.2

$$SNF(A) = \begin{pmatrix} d_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & d_m & 0 \cdots & 0 \end{pmatrix},\ d_1|...|d_m,\ d_i \neq 0\ \forall i \in [1,r]$$

Es gilt:

$$\begin{pmatrix} d_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & d_m & 0 \cdots & 0 \end{pmatrix} \equiv_T \begin{pmatrix} \tilde{d}_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & \tilde{d}_m & 0 \cdots & 0 \end{pmatrix} = SNF(\tilde{A}) \in (\mathbb{Z}/T\mathbb{Z})^{m \times n},$$

$d_i \equiv_T \tilde{d}_i \forall i \in [1, m]$

Da $\tilde{A}\tilde{\vec{x}} \equiv_T \tilde{\vec{b}}$ gilt, wenn $A\vec{x} = \vec{b}$, reicht es zu zeigen, dass die Reduktion der Smith-Normalform $SNF(\tilde{A})$immer noch alle Eigenschaften einer Smith-Normalform besitzt.
$\mathbb{Z}/T\mathbb{Z}$ enthält nur positive Einträge. Somit ist die erste Eigenschaft, $SNF(\tilde{A})$ ist eine Diagonalmatrix mitpositiven Einträgen, erfüllt. Es bleibt zu zeigen, dass die Diagonaleinträge Elementarteiler sind.
Drei Fälle sind zu unterscheiden:

Fall 1: Angenommen T teilt keinen Eintrag von $SNF(A)$, also $T \not| d_i \ \forall i \in [1, m]$. Dann sind alle Einträge reduziert auf modulo T ungleich Null: $\tilde{d}_i \not\equiv_T 0, \ i \in [1, r]$.
Laut der Definition der Smith-Normalform sind die Einträge von $SNF(A)$ Elementarteiler, das heißt $d_1|...|d_m$. Insbesondere gilt $\frac{d_s}{d_i} \in \mathbb{Z} \setminus \{0\}$ für alle $i < s$, wobei $s, i \in [1, m]$.
Folglich muss auch der Quotient der Reduktion $\frac{\tilde{d}_s}{\tilde{d}_i}$ eine ganze Zahl sein:
$\frac{d_s}{d_i} \equiv_T \frac{\tilde{d}_s}{\tilde{d}_i} \in \mathbb{Z}\backslash\{0\}$. Das ist genau dann der Fall, wenn $\tilde{d}_i$ den Eintrag $\tilde{d}_s$ ohne Rest teilt. Weil das für alle $i < s$ gilt, folgt daraus wiederum, dass die Einträge der reduzierten Smith-Normalform $SNF(\tilde{A})$ Elementarteiler sind: $\tilde{d}_1|...|\tilde{d}_m$.

Fall 2: Angenommen T teilt den ersten Eintrag, d_1, der Smith-Normalform von A.
Dann ist dieser Eintrag kongruent 0 modulo T, also $\tilde{d}_1 \equiv_T 0$.
Weil $d_1, .., d_r$ Elementarteiler sind, teilt T jeden einzelnen Eintrag und es gilt: $\tilde{d}_2 \equiv_T ... \equiv_T \tilde{d}_m \equiv_T 0$. $SNF(\tilde{A})$ ist die Nullmatrix und somit sind alle Einträge Elementarteiler.

Fall 3: Angenommen T teilt den i-ten Diagonaleintrag von $SNF(A)$, wobei $i \in [2, m]$.
Weiterhin sei T kein Teiler der vorherigen Einträge, also $T \not| d_s$ für alle $s \in [1, i-1]$.
Dann sind alle Einträge ab dem i-ten Eintrag kongruent modulo T (siehe Fall 2).
Also gilt $\tilde{d}_i \equiv_T ... \equiv_T \tilde{d}_m \equiv_T 0$.
Die restlichen Einträge, $\tilde{d}_s$, sind aufgrund der Nicht-Teilbarkeit von T ungleich Null: $\tilde{d}_s \not\equiv_T 0, \forall s \in [1, i-1]$.
Durch unimodulare Zeilen- und Spaltenoperationen können alle Diagonaleinträge der Größe nach sortiert werden, wobei der letzte Eintrag der Größte ist. Dann hat die Smith-Normalform von $\tilde{A}$ die Form

$$SNF(\tilde{A}) = \begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & & & & \vdots \\ \vdots & \ddots & 0 & \ddots & & & & & \vdots \\ \vdots & & \ddots & \tilde{d}_1 & 0 & & & & \vdots \\ \vdots & & & \ddots & \ddots & \ddots & & & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & \tilde{d}_{i-1} & 0 & \cdots & 0 \end{pmatrix}.$$

$\tilde{d}_1 \cdots \tilde{d}_{i-1}$ sind Elementarteiler (siehe Fall 1) und weil jede ganze Zahl ein Teiler von Null ist, sind alle Einträge Elementarteiler. □

Lineare Gleichungssysteme über Restklassenringe kann man folglich mit Hilfe der Smith-Normalform lösen. Die Vorgehensweise entspricht hier der, die in Kapitel 3 für lineare diophantische Gleichungssysteme eingeführt wurde.

4.3.2 Algorithmus

Es gibt zwei Möglichkeiten, die Smith-Normalform über einen Restklassenring zu bestimmen. Zum einen kann der Fakt, dass man sich in einem Restklassenring befindet, zunächst außer Acht gelassen werden. Die Smith-Normalform wird über $\mathbb{Z}$ bestimmt und erst zum Schluss auf modulo T reduziert. Zum anderen bietet sich natürlich auch an, von Anfang an im Restklassenring zu rechnen. Diese Vorgehensweise würde unter anderem das Auftreten großer Zahlen verhindern. Letztendlich wird bei beiden Methoden, abgesehen von der Reduzierung auf modulo T, identisch vorgegangen.

Sei $A\vec{x} \equiv_T \vec{b}$ das zu lösende lineare Gleichungssystem, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}$, $\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$ und $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$. Weiterhin sei $T \in \mathbb{N}$ und nicht prim.

Schritt 1 ***(Berechnung der Smith-Normalform)*:** Durch unimodulare Zeilen-und Spaltenoperationen wird die Smith-Normalform mittels des euklidischen Algorithmus, wie im Beweis des Satzes 3.2.2 beschrieben, berechnet. Außerdem werden die unimodularen Matrizen U und V bestimmt. U speichert die Spaltenumformungen und V die Zeilenumformungen.

Schritt 2 ***(Äquivalente Umformungen)* :** An die Gleichung $A\vec{x} \equiv_T \vec{b}$ wird von links die unimodulare Matrix V multipliziert, sodass $VA\vec{x} \equiv_T V\vec{b}$ gilt. Anschließend wird ein Vektor $\vec{y} \in (\mathbb{Z}/T\mathbb{Z})^n$ als $\vec{y} :\equiv_T U^{-1}\vec{x}$ definiert, sodass gilt $VAU\vec{y} = V\vec{b}$.
Aus $SNF(A) = VAU$ folgt $SNF(A)\vec{y} = V\vec{b}$.

Schritt 3 ***(Berechnung von $\vec{y}$)*:** $SNF(A)$ ist eine Diagonalmatrix mit $SNF(A) = diag(d_1, ...d_m)$.
Der Vektor $\vec{y}$ kann folglich durch Vor- oder Rückwärtssubstitution bestimmt werden.

Schritt 4 ***(Bestimmung der Lösungsmenge)*:** Die Lösung $\vec{x}$ wird durch $\vec{x} \equiv_T U\vec{y}$ berechnet. Abschließend kann die Lösungsmenge L angegeben werden:
$L = \{\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n | A\vec{x} \equiv_T \vec{b}\}$.

4.3.3 Existenz und Eindeutigkeit von Lösungen

Die Existenz und Eindeutigkeit einer Lösung kann bereits in *Schritt 2* ermittelt werden. Weil die Smith-Normalform eine Diagonalmatrix mit ganzzahligen Einträgen ist, existiert genau dann eine Lösung $\vec{y}$ zu $SNF(A)\vec{y} \equiv_T \vec{z}$, wenn jeder Eintrag aus der i-ten Zeile der Smith-Normalform von A den i-ten Eintrag des Vektors $\vec{z}$ ohne Rest teilt. Weiterhin ist das lineare Gleichungssystem $A\vec{x} \equiv_T \vec{b}$ genau dann lösbar, wenn auch das lineare Gleichungssystem $SNF(A)\vec{y} \equiv_T \vec{z}$ lösbar ist. Die Lösung ist genau dann eindeutig, wenn zusätzlich der Rang von A der Anzahl der Unbekannten entspricht und jeder Eintrag der Smith-Normalform teilerfremd zu T ist.

4.3.3.1 Proposition: Sei $A\vec{x} \equiv_T \vec{b}$, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}, \vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$ und $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$ ein lineares Gleichungssystem. Sei weiterhin $(d_{ii}) = SNF(A) \equiv_T VAU$ die Smith-Normalform von A, wobei V und U die zugehörigen unimodularen Matrizen sind. Außerdem sei $\vec{y}$ definiert als $\vec{y} :\equiv_T U^{-1}\vec{x}$ und $\vec{z}$ als $\vec{z} :\equiv_T V\vec{b}$. Dann gilt:

$$A\vec{x} \equiv_T \vec{b} \text{ ist } \textit{lösbar} \Leftrightarrow \exists\, \vec{y} \in (\mathbb{Z}/T\mathbb{Z})^n, \text{ sodass } SNF(A)\vec{y} \equiv_T \vec{z} \Leftrightarrow d_{ii} | z_i \ \forall i \in [1, m]$$

und

$$A\vec{x} = \vec{b} \text{ ist eindeutig lösbar } \Leftrightarrow A\vec{x} = \vec{b} \text{ ist lösbar, } rang(A) = n \text{ und } ggT(d_{ii}, T) = 1 \ \forall i \in [1, m].$$

Dementsprechend kommen eindeutige Lösungen nur bei quadratischen Matrizen vor. Über $\mathbb{Z}$ wurde voller Zeilenrang für A, also $rang(A) = m$, vorausgesetzt. Über Restklassenringe ist jedoch $rang(A) < m$ möglich. So sind über $\mathbb{Z}$ stets m Unbekannte eindeutig festgelegt und $n - m$ frei wählbar. Über Restklassenringe hingegen kann es vorkommen, dass weniger Unbekannte eindeutig bestimmt sind. Die Anzahl dieser hängt hier nicht mehr ausschließlich vom Rang ab, sondern auch von der Teilbarkeit jedes Eintrags mit T. Das lässt sich folgendermaßen erklären:
Angenommen es existiere eine Lösung, aber d_i und T seien nicht teilerfremd, $d_i \neq 0$. Dann werden alle Lösungen für y_i wie folgt berechnet:
Durch Vorwärts- oder Rückwärtssubstitution kommt man auf die Gleichung $d_i y_i = z_i$. Teilt man beide Seiten durch d_i, erhält man $y_i = \frac{z_i}{d_i}$. Jedoch sind dies nicht alle Lösungen für y_i. Die restlichen Lösungen erhält man, indem auf der linken Seite ein Element aus dem Kern des Ringhomomorphismus $\mathbb{Z}/T\mathbb{Z} \xrightarrow{\cdot d_i} \mathbb{Z}/T\mathbb{Z}$ addiert wird.
Das sind alle Elemente, die multipliziert mit d_i Null ergeben. Dann gilt:
$y_i = \frac{z_i}{d_i} + r$, wobei $r \in ker(\mathbb{Z}/T\mathbb{Z} \xrightarrow{\cdot d_i} \mathbb{Z}/T\mathbb{Z})$. Sind d_i und T teilerfremd, würde der Kern nur aus dem Nullelement bestehen, denn aus $ggT(d_i, T) = 1$ folgt, dass d_i eine Einheit ist (Satz 2.1.8). Folglich ist d_i kein Nullteiler (Satz 2.1.11). Dementsprechend existiert kein Element a aus dem Restklassenring, sodass gilt $d_i \cdot a = 0$. Also ist $y_i = \frac{z_i}{d_i} + 0$ eindeutig.

4.3.4 Beispiel: Sei $A = \begin{pmatrix} 1 & 9 & 2 & 0 \\ 5 & 0 & 5 & 5 \\ 4 & 1 & 3 & 5 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^{3x4}$ und $\vec{b} = \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^3$

Zu lösen ist das lineare Gleichungssystem $A\vec{x} = \vec{b},\ x \in \mathbb{Z}^4$.

Schritt 1: Durch unimodulare Spalten- und Zeilenumformungen wird die Smith-Normalform der Matrix A erzeugt. Der Eintrag $a_{11} = 1$ teilt alle Einträge in A. Somit können die Einträge in der ersten Spalte mit diesem Eintrag eliminiert werden:

$$\left(\begin{array}{cccc|ccc} 1 & 9 & 2 & 0 & 1 & 0 & 0 \\ 5 & 0 & 5 & 5 & 0 & 1 & 0 \\ 4 & 1 & 3 & 5 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right) \xrightarrow[\text{III.S-2I.S}]{\text{II.S+I.S}} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 5 & 5 & 5 & 5 & 0 & 1 & 0 \\ 4 & 5 & 5 & 5 & 0 & 0 & 1 \\ \hline 1 & 1 & 8 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right)$$

$$\xrightarrow[\text{III.Z+6I.Z}]{\text{II.Z+5I.S}} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 5 & 5 & 5 & 5 & 1 & 0 \\ 0 & 5 & 5 & 5 & 6 & 0 & 1 \\ \hline 1 & 1 & 8 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right) \xrightarrow[\text{III.Z+II.Z}]{\text{III.Z+II.S, IV.Z+II.S}} \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 5 & 0 & 0 & 5 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 1 & 1 & 9 & 1 & & & \\ 0 & 1 & 1 & 1 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \end{array}\right)$$

Die Smith-Normalform sowie die beiden Unimodularen Matrizen U und V wurden bestimmt:

$$SNF(A) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},\ V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},\ U = \begin{pmatrix} 6 & 1 & 9 & 1 \\ 5 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Der Rang von A ist, wie man aus der Smith-Normalform unmittelbar ablesen kann, 2. Da $\vec{x} \in \mathbb{Z}^4$, ist die Lösung (falls sie existiert) nicht eindeutig.

Schritt 2: Um die Existenz der Lösung zu untersuchen, wird die $SNF(A)$ und V in die Gleichung

$SNF(A)\vec{y} = V\vec{b},\ \vec{y} \in (\mathbb{Z}/10\mathbb{Z})^4$ eingesetzt und man erhält:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \\ 3 \end{pmatrix} \equiv_{10} \begin{pmatrix} 2 \\ 5 \\ 0 \end{pmatrix}.$$

Schritt 3: Offensichtlich gilt $1|2$ und $5|5$. Somit existiert eine Lösung. Weiterhin gilt $ggT(1, 10) = 1$ und $ggT(5, 10) = 5 \neq 1$. Demnach ist y_1 eindeutig bestimmt, y_2 jedoch nicht. Durch Vorwärtssubstitution erhält man:

$$y_1 \equiv_{10} 2;$$
$$5y_2 \equiv_{10} 5 \Leftrightarrow y_2 \equiv_{10} 1 + r,\ \text{wobei } r \in ker(\mathbb{Z}/10\mathbb{Z} \xrightarrow{\cdot 5} \mathbb{Z}/10\mathbb{Z}) = \{0, 2, 4, 6, 8\}$$
$$y_3, y_4 \in \mathbb{Z}/10\mathbb{Z} \text{ beliebig.}$$

Somit existiert auch keine eindeutige Lösung $\vec{x}$ zu $A\vec{x} \equiv_{10} \vec{b}$.

Schritt 4: Um $\vec{x}$ zu bestimmen, wird $\vec{y}$ in $\vec{x} \equiv_{10} U\vec{y}$ eingesetzt:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \equiv_{10} \begin{pmatrix} 6 & 1 & 9 & 1 \\ 5 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1+r \\ y_3 \\ y_4 \end{pmatrix} \equiv_{10} \begin{pmatrix} 3+r+9y_3+y_4 \\ 1+r+y_3+y_4 \\ y_3 \\ y_4 \end{pmatrix}.$$

$$\Rightarrow L = \left\{ \begin{pmatrix} 3 \\ 1 \\ 0 \\ 0 \end{pmatrix} + r \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + y_3 \begin{pmatrix} 9 \\ 1 \\ 1 \\ 0 \end{pmatrix} + y_4 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \middle| r \in ker(\mathbb{Z}/10\mathbb{Z} \xrightarrow{\cdot 5} \mathbb{Z}/10\mathbb{Z}),\ y_3, y_4 \in \mathbb{Z}/10\mathbb{Z} \right\}.$$

Die Lösungsmenge ist wie erwartet nicht leer und nicht eindeutig.

4.3.5 Beispiel: Sei A$= \begin{pmatrix} 4 & 8 & 12 \\ 8 & 6 & -4 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^{2x3}$ und $\vec{b} = \begin{pmatrix} 9 \\ 4 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^2$.

Die Smith-Normalform von A ist gegeben durch $SNF(A) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$ (siehe Beispiel 3.2.4.).

A hat also vollen Rang. Falls eine Lösung zum linearen Gleichungssystem $A\vec{x} \equiv_{10} \vec{b}$, $\vec{x} \in (\mathbb{Z}/10\mathbb{Z})^3$ existiert, kann diese eindeutig sein. Um die Existenz zu untersuchen, wird das lineare Gleichungssystem $SNF(A)\vec{y} \equiv_{10} V\vec{b}$ betrachtet, wobei $\vec{y} :\equiv_{10} U^{-1}\vec{x}$.
Die unimodularen Matrizen U und V sind gegeben durch:

$$U = \begin{pmatrix} 0 & -5 & 13 \\ 1 & 6 & -14 \\ 0 & -2 & 5 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^{3\times 3},\ V = \begin{pmatrix} 1 & -1 \\ -3 & 4 \end{pmatrix} \in (\mathbb{Z}/10\mathbb{Z})^{2\times 2} (\text{ siehe Beispiel 3.2.4.})$$

$SNF(A)\vec{y} = V\vec{b},\ \vec{y} \in (\mathbb{Z}/10\mathbb{Z})^3$ liefert: $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \equiv_{10} \begin{pmatrix} 1 & -1 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} 9 \\ 4 \end{pmatrix}$

Offensichtlich ist 2 teilerfremd zu 5. Es existiert also kein y_1, sodass $2y_1 \equiv_{10} 5$ gilt. Damit existiert keine Lösung zu $SNF(A)\vec{y} \equiv_{10} V\vec{b}$ und somit ist ebenfalls das lineare Gleichungssystem $A\vec{x} \equiv_{10} \vec{b}$ nicht lösbar. Für die Lösungsmenge gilt folglich

$$L = \{\varnothing\}.$$

4.4 Chinesischer Restsatz

Eine weitere Möglichkeit, lineare Gleichungssysteme modulo T $\in \mathbb{N}_{>0}$ zu lösen, liefert der chinesische Restsatz: Sei T eine in Primfaktoren zerlegbare natürliche Zahl. Dann kann man T schreiben als $T = p_1 \cdots p_n,$ wobei $p_1 \neq \ldots \neq p_n$ Primzahlen sind . Die Abbildung

$$\mathbb{Z}/T\mathbb{Z} \to \mathbb{Z}/p_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n\mathbb{Z}, x \mapsto (x \bmod p_1, \ldots, x \bmod p_n)$$

ist ein Isomorphismus von Ringen [6].

Somit kann das lineare Gleichungssystem zunächst über jeden Körper $\mathbb{Z}/p_i\mathbb{Z},\ i \in [1,n]$ mittels des Gauß-Algorithmus gelöst werden. Anschließend werden die Lösungen durch Anwendung des chinesischen Restsatzes zusammengesetzt.

4.4.1 Satz *Chinesischer Restsatz*

Sei T eine natürliche Zahl, die in n paarweise verschiedene Primfaktoren $p_1, \ldots, p_n$ zerlegbar ist. Weiterhin seien $y_1 \ldots y_n \in \mathbb{Z}$. Dann existiert ein $x \in \mathbb{Z}$, sodass

$$\begin{aligned} x &\equiv_{p_1} y_1 \\ &\vdots \\ x &\equiv_{p_n} y_n. \end{aligned}$$

x ist eindeutig bestimmt [2].

Bezogen auf lineare Gleichungssysteme $A\vec{x} \equiv_T \vec{b}$, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n}, \vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$ und $\vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$ werden $y_1 \ldots y_n$ und x entsprechend aus $\mathbb{Z}^n$ betrachtet.

4.4.2 Algorithmus

Sei $A\vec{x} \equiv_T \vec{b}$ das zu lösende lineare Gleichungssystem, wobei $A \in (\mathbb{Z}/T\mathbb{Z})^{m\times n},\ \vec{x} \in (\mathbb{Z}/T\mathbb{Z})^n$ und $\vec{b} \in (\mathbb{Z}/T\mathbb{Z})^m$. Weiterhin sei $T \in \mathbb{N}$ nicht prim und in paarweise teilerfremde Primfaktoren, $p_1, \ldots, p_n,$ zerlegbar.

Schritt 1 *Lösung modulo* p_i: Das lineare Gleichungssystem wird über $\mathbb{Z}/p_i\mathbb{Z}$ für jedes $i \in [1,n]$ gelöst. Der Ring $\mathbb{Z}/p_i\mathbb{Z}$ bildet einen Körper. Demnach kann die Lösungsmenge mit Hilfe des Gauß-Algorithmus bestimmt werden.

Schritt 2 *Zusammensetzung der Lösungsmengen*: Sei T_i definiert als $T_i := \frac{T}{p_i}, i \in [1,n]$. Weil T_i und p_i teilerfremd sind, können durch den erweiterten euklidischen Algorithmus $a_i, b_i \in \mathbb{Z}$ berechnet werden, sodass $a_i \cdot p_i + b_i \cdot T_i = 1$ gilt. $\vec{x}$ wird durch $\vec{x} = \sum_{i=1}^{3} \vec{x}_i \cdot b_i \cdot T_i$ bestimmt.
Die Existenz von a_i und b_i wird durch das Lemma von Bézout garantiert.

4.4.3 Lemma von Bézout: Seien $T_1, .., T_n$ n ganze Zahlen. Dann existieren n ganzzahlige Koeffizienten, $a_1, \ldots, a_n$, sodass der größte gemeinsame Teiler als Linearkombination dieser Koeffizienten darstellbar ist: $ggT(T_1, \ldots, T_n) = a_1 \cdot T_1 + \ldots + a_n \cdot T_n$.

Insbesondere existieren für alle Primzahlen, $p_1, \ldots, p_n$ ganzzahlige Koeffizienten $a_1, \ldots, a_n,$ sodass gilt: $ggT(p_1, \ldots, p_n) = 1 = a_1 \cdot p_1 + \ldots + a_n \cdot p_n$. [6]

Die Koeffizienten lassen sich durch den erweiterten euklidischen Algorithmus berechnen.

4.4.4 Beispiel: Sei $A = \begin{pmatrix} 9 & 4 \\ 1 & 2 \end{pmatrix} \in (\mathbb{Z}/30\mathbb{Z})^{2\times 2}$ und $\vec{b} = \begin{pmatrix} 7 \\ 5 \end{pmatrix} \in (\mathbb{Z}/30\mathbb{Z})^2$.
Gesucht ist eine Lösung $\vec{x} \in (\mathbb{Z}/30\mathbb{Z})^2,$ sodass $A\vec{x} \equiv_{30} \vec{b}$ gilt.

$T = 30$ ist zerlegbar in $30 = 2 \cdot 3 \cdot 5$.

Schritt 1: Das lineare Gleichungssystem wird zunächst über $\mathbb{Z}/2\mathbb{Z}$, dann über $\mathbb{Z}/3\mathbb{Z}$ und anschließend über $\mathbb{Z}/5\mathbb{Z}$ gelöst.

$\mathbb{Z}/2\mathbb{Z} : A = \begin{pmatrix} 9 & 4 \\ 1 & 2 \end{pmatrix} \equiv_2 \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$. Durch Abziehen der ersten Zeile von der zweiten Zeile erhält man die Zeilenstufenform der Koeffizientenmatrix: $\left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 0 & 0 \end{array}\right)$.

Durch Vorwärtssubstitution kommt man auf die Lösungsmenge $L = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$.

$\mathbb{Z}/3\mathbb{Z} : A = \begin{pmatrix} 9 & 4 \\ 1 & 2 \end{pmatrix} \equiv_3 \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ Durch Vertauschen der beiden Zeilen erhält man die Zeilenstufenform der Koeffizientenmatrix: $\left(\begin{array}{cc|c} 1 & 2 & 0 \\ 0 & 1 & 1 \end{array}\right)$.

Durch Rückwärtssubstitution kommt man auf die Lösungsmenge $L = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$.

$\mathbb{Z}/5\mathbb{Z} : A = \begin{pmatrix} 9 & 4 \\ 1 & 2 \end{pmatrix} \equiv_3 \begin{pmatrix} -1 & 4 \\ 1 & 2 \end{pmatrix}$ Durch Addition der ersten Zeile zur zweiten Zeile erhält man die Zeilenstufenform der Koeffizientenmatrix: $\left(\begin{array}{cc|c} -1 & 4 & 2 \\ 0 & 1 & 2 \end{array}\right)$.

Durch Rückwärtssubstitution kommt man auf die Lösungsmenge $L = \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right\}$.

Schritt 2: In Schritt 1 wurden folgende Lösungen für $\vec{x}$ bestimmt:

$\vec{x}_1 \equiv_2 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + s \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\vec{x}_2 \equiv_3 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ und $\vec{x}_3 \equiv_5 \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

Nun werden die Lösungen zu einer Lösungsmenge modulo 30 mit Hilfe des chinesischen Restsatzes zusammengesetzt. Dafür werden T_1, T_2, T_3 definiert als

$$T_1 := \tfrac{T}{p_1} = \tfrac{30}{2} = 15$$

$$T_2 := \tfrac{T}{p_2} = \tfrac{30}{3} = 10$$

$$T_3 := \tfrac{T}{p_3} = \tfrac{30}{5} = 6.$$

Durch den euklidischen Algorithmus können zwei ganze Zahlen a_i und b_i gefunden werden, sodass gilt: $a_i \cdot p_i + b_i \cdot T_i = 1$. Man erhält:

$$\begin{gathered} a_1 \cdot p_1 + b_1 \cdot T_1 = 8 \cdot 2 + (-1) \cdot 15 = 1 \\ a_2 \cdot p_2 + b_2 \cdot T_2 = -3 \cdot 3 + 1 \cdot 10 = 1 \\ a_3 \cdot p_3 + b_3 \cdot T_3 = -1 \cdot 5 + 1 \cdot 6 = 1. \end{gathered}$$

Die Lösung für $A\vec{x} \equiv_{30} \vec{b}$ kann nun durch $\vec{x} = \sum_{i=1}^{3} \vec{x}_i \cdot b_i \cdot T_i$ bestimmen.
Damit gilt:

$$\vec{x} = \sum_{i=1}^{3} \vec{x}_i \cdot b_i \cdot T_i = \begin{pmatrix} -15 \\ 0 \end{pmatrix} + s \begin{pmatrix} 0 \\ -15 \end{pmatrix} + \begin{pmatrix} 0 \\ 10 \end{pmatrix} + \begin{pmatrix} 6 \\ 12 \end{pmatrix} = \begin{pmatrix} -9 \\ 22 \end{pmatrix} + s \begin{pmatrix} 0 \\ -15 \end{pmatrix}, s \in (\mathbb{Z}/2\mathbb{Z}).$$

Abschließend kann die Lösungsmenge für $A\vec{x} \equiv_{30} \vec{b}$ angegeben werden.

$$L = \left\{ \begin{pmatrix} -9 \\ 22 \end{pmatrix} + s \begin{pmatrix} 0 \\ -15 \end{pmatrix} \middle| s \in (\mathbb{Z}/2\mathbb{Z}) \right\}.$$

4.4.5 Beispiel: Sei $A = \begin{pmatrix} 9 & 4 \\ 1 & 2 \end{pmatrix} \in (\mathbb{Z}/60\mathbb{Z})^{2\times 2}$ und $\vec{b} = \begin{pmatrix} 7 \\ 5 \end{pmatrix} \in (\mathbb{Z}/60\mathbb{Z})^2$.
Gesucht ist eine Lösung $\vec{x} \in (\mathbb{Z}/60\mathbb{Z})^2$, sodass $A\vec{x} \equiv_{60} \vec{b}$ gilt.

$T = 60$ lässt sich nicht in paarweise verschiedene Primzahlen zerlegen: $T = 2 \cdot 2 \cdot 3 \cdot 5$.
Der chinesische Restsatz kann somit nicht angewandt werden.

Das Lösen linearer Gleichungssysteme über Restklassenringe, die keine Körper bilden, mit Hilfe des chinesischen Restsatzes bietet einen Vorteil: Es wird überwiegend über Körper gerechnet und die gewohnte Methode des Gauß-Algorithmus kann ohne große Schwierigkeiten angewandt werden. Jedoch besitzt der Großteil der natürlichen Zahlen keine Primfaktorzerlegung mit paarweise verschiedenen Primfaktoren. Die kleinste zusammengesetzte Zahl, die solch eine Primfaktorzerlegung besitzt, ist die 6. Darauf folgt die 30 und dann kommt schon die 210. Lineare Gleichungssysteme modulo 210 oder größer kommen eher selten vor. Hinzu kommt, dass mit jedem zusätzlichen Faktor, das lineare Gleichungssystem über einen zusätzlichen Restklassenkörper berechnet werden muss.

In Bezug auf die Erstellung periodischer Taktfahrpläne wird meist der Restklassenring $\mathbb{Z}/60\mathbb{Z}$ betrachtet. Weil 60 bekanntlich nicht in paarweise verschiedene Primfaktoren zerlegbar ist, muss dementsprechend auf eins der weiteren in dieser Arbeit vorgestellten Verfahren zurückgegriffen werden.

5 Periodische Taktfahrpläne

In diesem Kapitel wird ein aktuelles Problem vorgestellt, mit welchem sich heute noch Mathematiker beschäftigen: Die Berechnung periodischer Taktfahrpläne der öffentlichen Verkehrsmittel. Ziel ist es, periodische Taktfahrpläne zu erstellen, die die Reisezeit der Passagiere minimieren. Das Mathematische Model *Periodic Event Scheduling Problem* wird vorgestellt und an einem Beispiel ausführlich illustriert. Der Bezug zu linearen Gleichungssystemen modulo T und deren Lösungsverfahren, die in Kapitel 4 behandelt wurden, wird dabei verdeutlicht.

In einem Fahrplan werden die Abfahrtszeiten des jeweiligen Verkehrsmittels an jeder Haltestelle festgelegt. Dabei werden Fahrten mit mindestens teilweise gleichem Verlauf von einer Linie repräsentiert [8]. Bei periodischen Taktfahrplänen wird die Abfahrts- und Ankunftszeit an einer Station in regelmäßigen Abständen, die sich periodisch wiederholen, festgelegt [9]. Abbildung 5.1 stellt einen periodischen Taktfahrplan der Zugline Z an der Station S dar. Jede halbe Stunde fährt ein Zug der Zuglinie Z von der Station S ab. Der Takt beträgt also 30 Minuten.

Abfahrtszeiten Zug Z an Station S	
h	Montag - Sonntag
0	00’ 30’
⋮	⋮
23	00’ 30’

Abbildung 5.1: *Periodischer Taktfahrplan*

Bereits 1902 wurden in Berlin Taktfahrpläne für U- und S-Bahnen eingeführt. Für lange Strecken wurden noch keine realisiert. Vermutlich liegt das daran, dass Züge für lange Strecken sehr selten (einmal pro Tag) fahren. [10]

5.1 Periodic Event Scheduling Problem

Bei periodischen Taktfahrplänen wird ein Ereignis nach einer festgesetzten Laufzeit T wiederholt. Üblicherweise beträgt diese Laufzeit eine Stunde beziehungsweise 60 Minuten. Eine Linie wird in der Regel in zwei gerichtete Linien aufgeteilt: Die Hin- und die Rückrichtung. Auf Ringlinien wird nur in eine Richtung gefahren, es gibt dementsprechend nur eine gerichtete Linie. In dieser Arbeit werden Ringlinien außer Acht gelassen und ausschließlich Linien, die in zwei Richtungen verkehren, betrachtet. Für die Erstellung eines Taktfahrplans müssen die Ankunfts- und Abfahrtszeiten von den Zügen auf beiden Linien an jeder Station innerhalb der Taktzeit in Betracht gezogen werden. [8]

In diesem Kapitel wird das mathematische Problem *Periodic Event Scheduling Problem* vorgestellt, mit welchem anhand von gerichteten Graphen ein Taktfahrplan berechnet werden kann. Im Jahre 1989 wurde es von Serafini und Ukovich veröffentlicht.

Bevor das Periodic Event Scheduling Problem erläutert wird, müssen noch einige Begriffe zum Verständnis definiert werden.

5.1.1 Definition: Ein *gerichteter Graph* $G = (V, A)$ besteht aus einer Knotenmenge V und einer Kantenmenge A. Die Kanten sind gerichtet und verlaufen in eine Richtung. In dieser Arbeit werden die Kanten mit Pfeilen dargestellt, die die Richtung angeben [11].

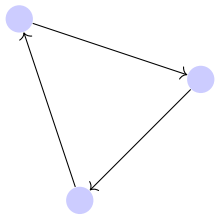


Abbildung 5.1.1: *Gerichteter Graph mit 3 Knoten und 3 gerichteten Kanten*

5.1.2 Definition: Sei $G = (V, A)$ ein gerichteter Graph, mit der Knotenmenge V und der Kantenmenge A. Weiterhin sei $\gamma \in \{-1, 0, 1\}^A$, sodass für alle $v \in V$ gilt:
$\sum_{uv \in A} \gamma_{uv} = \sum_{vw \in A} \gamma_{vw}$, wobei γ die Kanten a
vorwärts benutzt, falls $\gamma_a = 1$, rückwärts, falls $\gamma_a = -1$ und gar nicht, falls $\gamma_a = 0$.
γ ist dann ein *orientierter Kreis* [12].

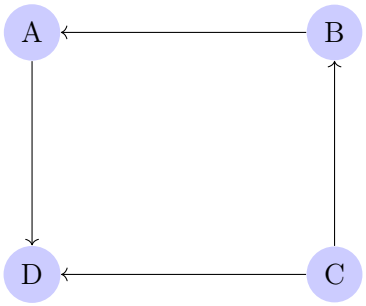


Abbildung 5.1.2: *Orientierter Kreis, wobei* $\gamma_{AD} = \gamma_{CB} = \gamma_{BA} = 1$ *und* $\gamma_{CD} = -1$

5.1.3 Definition: Sei B eine Menge mit gerichteten Kreisen. B heißt *Kreisbasis,* wenn B eine Basis des von allen orientierten Kreisen aufgespannten $\mathbb{Q}$ bildet [12].

5.1.4 Definition: Eine *Kreismatrix* ist eine Matrix $\Gamma \in \{-1, 0, 1\}^{B \times A}$, die aus den orientierten Kreisen der Kreisbasis B besteht [12].

Nachdem die nötigen Begriffe erklärt wurden, kann das Periodic Event Scheduling Problem eingeführt werden.

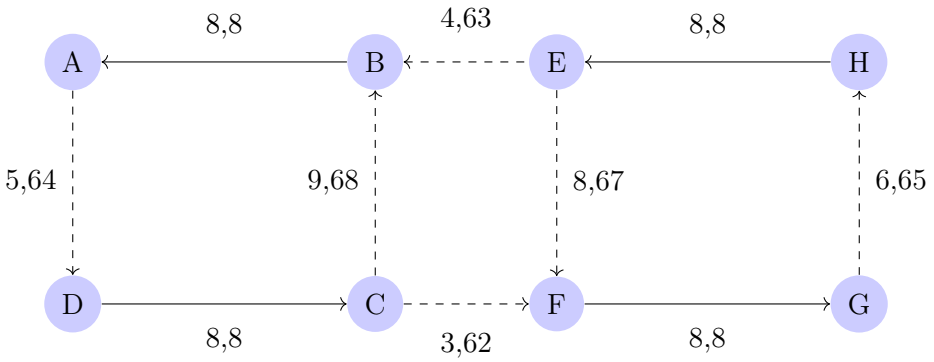
5.1.5 Definition Periodic Event Scheduling Problem (PESP)
Sei $G = (V, A)$ ein gerichteter Graph, wobei V die Knotenmenge und A die Kantenmenge bezeichnet. Ein Knoten steht für eine Station und eine Kante für ein Ereignis. Jedes Ereignis wird zeitlich durch eine untere Schranke $l_a \in \{0,...,T\text{-}1\}$ und eine obere Schranke $u_a \in \{l_a,...,T + l_a - 1\}$, $T \in \mathbb{N}$ beschränkt. Weiterhin sei jeder Kante ein Gewicht $w_a \geq 0$ zugewiesen.

Dann lautet das *Periodic Event Scheduling Problem (PESP):*

Minimiere $\sum_{a \in A} w_a y_a$, sodass $\Gamma \vec{y} \equiv_T -\Gamma l$ und $y_a \in \{0, ..., u_a - l_a\}$ für jedes $a \in A$.

Hierbei ist $\Gamma \in \mathbb{Z}^{B \times A}$ die Kreismatrix einer ganzzahligen Kreisbasis B von G [13].

5.1.6 Beispiel: Sei folgender Graph gegeben.

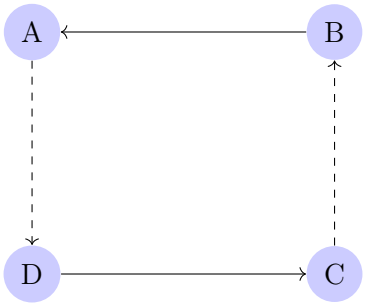


Jeder Knoten repräsentiert eine Station. Jede durchgezogene Kante stellt eine Zuglinie dar und jede gestrichelte Kante hingegen gibt Umsteigeoptionen an. Weiterhin ist jede Kante mit einer unteren und oberen Schranke (l_a, u_a) beschriftet. Die Fahrzeiten zwischen zwei Stationen sind üblicherweise festgelegt, weshalb hier keine Abweichungen zwischen unterer und oberer Schranke auftreten können. Für die Umsteigezeit jedoch lässt sich kein eindeutiger Zeitpunkt festlegen. Aus diesem Grund wird die Umsteigezeit in einem Intervall, wobei die Schranken die Intervallgrenzen sind, angegeben. Die Intervallgröße soll nun mit Hilfe des PESP minimiert werden. Hierfür wird erst die Kreismatrix durch die Kreisbasis aufgestellt und anschließend durch das lineare Gleichungssystem der Vektor mit den Wartezeiten $\vec{y}$ berechnet. Abschließend wird die kleinste Wartezeit durch das PESP bestimmt.

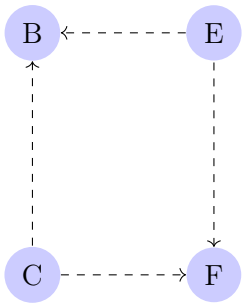
Alle Kanten besitzen hier das selbe Gewicht $w_a, a \in A$. Sei dementsprechend $w_a =: w$.

Der Graph besteht aus 10 Kanten und 8 Knoten. Die Größe der Kreisbasis kann dann wie folgt berechnet werden: #Kanten-#Knoten+1=10-8+1=**3**.
Seien $\Gamma_1, \Gamma_2, \Gamma_3$ die gerichteten Kreise, die die Kreisbasis aufstellen.

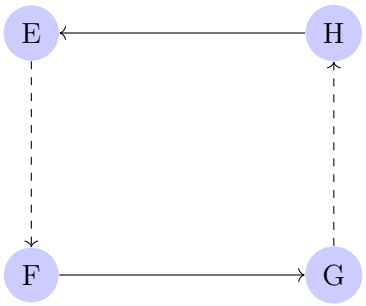
Wähle Γ_1=



Γ_2=



Γ_3=



$\Gamma_1, \Gamma_2\Gamma_3$ decken alle Kanten und Knoten ab und sind offensichtlich linear unabhängig.
$\Gamma_1, \Gamma_2\Gamma_3$ bilden jeweils orientierte Kreise. Die Richtung der Kanten dieser Kreise geben die Einträge der Kreismatrix an. In diesem Beispiel lässt sich die Kreismatrix wie folgt aufstellen.

	γ_{BA}	γ_{AD}	γ_{DC}	γ_{CB}	γ_{EB}	γ_{EF}	γ_{CF}	γ_{HE}	γ_{FG}	γ_{GH}
Γ_1	1	1	1	1	0	0	0	0	0	0
Γ_2	0	0	0	−1	1	−1	1	0	0	0
Γ_3	0	0	0	0	0	1	0	1	1	1

Also $\Gamma = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$.

Mithilfe der in Kapitel 4 vorgestellten Rechenverfahren kann das lineare Gleichungssystem
$\Gamma\vec{y} \equiv_{60} -\Gamma\vec{l}$ gelöst und anschließend $\sum_{a \in A} w_a y_a$ minimal minimiert werden.

$$\text{Sei } \vec{y} = \begin{pmatrix} y_{BA} \\ y_{AD} \\ y_{DC} \\ y_{CB} \\ y_{EB} \\ y_{EF} \\ y_{CF} \\ y_{HE} \\ y_{FG} \\ y_{GH} \end{pmatrix} := \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \end{pmatrix}.$$

Laut der Definition des PESP Modells gilt $y_a \in \{0, ..., u_a - l_a\}$ für jedes $a \in A$. Da bei den Fahrzeiten zwischen zwei Stationen keine Abweichungen zwischen unterer und oberer Schranke auftreten, gilt $y_{BA} \equiv_{60} y_{DC} \equiv_{60} y_{HE} \equiv_{60} y_{FG} \equiv_{60} 0$ und somit

$$\vec{y} \equiv_{60} \begin{pmatrix} 0 \\ y_2 \\ 0 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ 0 \\ 0 \\ y_{10} \end{pmatrix}.$$

Weiterhin ist $\vec{l}$ gegeben durch

$$\vec{l} \equiv_{60} \begin{pmatrix} 8 \\ 5 \\ 8 \\ 9 \\ 4 \\ 8 \\ 3 \\ 8 \\ 8 \\ 6 \end{pmatrix}.$$

Die rechte Seite des linearen Gleichungssystem lässt sich demnach berechnen durch

$$-\Gamma\vec{l} = -\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 8 \\ 5 \\ 8 \\ 9 \\ 4 \\ 8 \\ 3 \\ 8 \\ 8 \\ 6 \end{pmatrix} \equiv_{60} \begin{pmatrix} -30 \\ 10 \\ -30 \end{pmatrix}.$$

Um das lineare Gleichungssystem $\Gamma\vec{y} \equiv_{60} \begin{pmatrix} -30 \\ 10 \\ -30 \end{pmatrix}$ zu lösen, werden die in Kapitel 4 vorgestellten Methoden angewandt. Jedes einzelne Lösungsverfahren werde ich im Folgenden systematisch betrachten. Zunächst den Gauß-Algorithmus, anschließend die Hermite-Normalform, darauffolgend die Smith-Normalform und abschließend den chinesische Restsatz.

1. Gauß-Algorithmus

Die Matrix Γ ist bereits in der Zeilenstufenform.

Der Gauß-Algorithmus kann daher als Lösungsverfahren eingesetzt werden.

Aus $\Gamma\vec{y} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_{10} \end{pmatrix} \equiv_{60} \begin{pmatrix} -30 \\ 10 \\ -30 \end{pmatrix}$ erhält man

$$\text{I.:} \quad y_2 + y_4 \equiv_{60} -30,$$

$$\text{II.:} \quad -y_4 + y_5 - y_6 + y_7 \equiv_{60} 10$$

und

$$\text{III.:} \ y_6 + y_{10} \equiv_{60} -30 \Leftrightarrow y_6 \equiv_{60} -y_{10} - 30 \equiv_{60} -y_{10} + 30.$$

Dann erhält man als Lösungsmenge

$$L = \left\{ \left. \begin{pmatrix} 0 \\ 30 - y_4 \\ 0 \\ y_4 \\ y_5 \\ 30 - y_{10} \\ y_7 \\ 0 \\ 0 \\ y_{10} \end{pmatrix} \right| y_4, y_5, y_7, y_{10} \in \mathbb{Z}/60\mathbb{Z} \right\}.$$

Der Vektor $\vec{y}$ enthält Wartezeiten, die so gewählt werden, dass die Gewichtsfunktion $\sum_{a \in A} w_a y_a$ minimiert wird. Weil Wartezeiten selbstverständlich nicht negativ sind, dies bei y_2 und y_6 jedoch vorkommen kann, müssen 4 Fälle für y_4 und y_{10} unterschieden werden:

Fall 1: $0 \leq y_4, y_{10} \leq 30$. Sind sowohl y_4 als auch y_{10} zwischen 0 und 30, gilt $y_2 = 30 - y_4 \geq 0$ und $y_6 = 30 - y_{10} \geq 0$ und für die Gewichtsfunktion gilt folglich.

$$\sum_{a \in A} w_a y_a = w(30 - y_4 + y_4 + y_5 + 30 - y_{10} + y_7 + y_{10}) = w(60 + y_5 + y_7).$$

Um die Summe zu minimieren, muss zusätzlich $y_5 = y_7 = 0$ gewählt werden.

Fall 2: $30 < y_4 < 60$ und $0 \leq\ y_{10} \leq\ 30$. In diesem Fall wäre y_2 nicht mehr positiv. Um dem entgegenzuwirken werden 60 Minuten dazu addiert.

$$30 - y_4 \equiv_{60} 30 - y_4 + 60$$

Für den Vektor $\vec{y}$ ändert sich nichts, da dieser aus dem Restklassenring $\mathbb{Z}/60\mathbb{Z}$ kommt. Die Gewichtsfunktion jedoch befindet sich in den reellen Zahlen und wird demzufolge nicht auf modulo 60 reduziert. Daraus folgt:

$$\sum_{a \in A} w_a y_a = w(30 - y_4 + 60 + y_4 + y_5 + 30 - y_{10} + y_7 + y_{10}) = w(120 + y_5 + y_7)$$

Um die Summe zu minimieren, muss zusätzlich $y_5 = y_7 = 0$ gewählt werden.

Fall 3: $0 \leq\ y_4 \leq\ 30$ und $30 < y_{10} < 60$. Analog zu Fall 4 nimmt hier y_6 einen negativen Wert an. Demnach wird 60 dazuaddiert, sodass gilt

$$30 - y_{10} \equiv_{60} 30 - y_{10} + 60$$

Für die Gewichtsfunktion folgt dementsprechend
$$\sum_{a \in A} w_a y_a = w(30 - y_4 + y_4 + y_5 + 30 - y_{10} + 60 + y_7 + y_{10}) = w(120 + y_5 + y_7)$$

Um die Summe zu minimieren, muss zusätzlich $y_5 = y_7 = 0$ gewählt werden.

Fall 4: $30 < y_4, y_{10} < 60$. In diesem Fall ist sowohl y_2 als auch y_6 negativ. Folglich muss auf beide 60 addiert werden, sodass gilt

$$\begin{aligned} 30 - y_4 &\equiv_{60} 30 - y_4 + 60, \\ 30 - y_{10} &\equiv_{60} 30 - y_{10} + 60. \end{aligned}$$

Für die Gewichtsfunktion gilt dann:

$$\sum_{a \in A} w_a y_a = w(30 - y_4 + 60 + y_4 + y_5 + 30 - y_{10} + 60 + y_7 + y_{10}) = w(180 + y_5 + y_7).$$

Um die Summe zu minimieren, muss zusätzlich $y_5 = y_7 = 0$ gewählt werden.

In Anbetracht der 4 Fälle nimmt die Gewichtsfunktion im ersten Fall minimalen Wert an. Somit sieht die Lösungsmenge L, für die $\sum_{a \in A} w_a y_a$ minimal wird, wie folgt aus.

$$L_{PESP} = \left\{ \left(\begin{array}{c} 0 \\ 30 - y_4 \\ 0 \\ y_4 \\ 0 \\ 30 - y_{10} \\ 0 \\ 0 \\ 0 \\ y_{10} \end{array} \right) \middle| \, y_4, y_{10} \in \mathbb{Z}/60\mathbb{Z}, 0 \leq\ y_4, y_{10} \leq\ 30 \right\}.$$

Das *Periodic Event Scheduling Problem* konnte mit Hilfe des Gauß-Algorithmus gelöst werden. Die Umsteigezeit sowohl von Station E nach Station B als auch von Station C nach Station F wird so kurz wie möglich gehalten, weil die Intervallgröße zu diesen Kanten auf Null minimiert wurde. Somit setzt man die Umsteigezeit für γ_{EB} auf 4 Minuten und für γ_{CF} auf 3 Minuten. Die Intervallgröße der Umsteigezeit der Kanten γ_{CB} und γ_{GH} wurde von 59 auf 30 reduziert, da y_4 und y_{10} wie berechnet zwischen 0 und 30 gewählt werden müssen.

2. Hermite-Normalform

Die Matrix Γ hat vollen Rang. Somit kann das lineare Gleichungssystem ebenfalls über die Hermite-Normalform gelöst werden. Durch unimodulare Spaltenumformungen kommt man auf die folgende Hermite-Normalform:

$$HNF(A) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\text{wobei } C = \begin{pmatrix} 1 & 0 & 0 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Sei $\vec{x} = C^{-1}\vec{y}$. Dann gilt

$$HNF(\Gamma)\vec{x} \equiv_{60} -\Gamma\vec{l} \equiv_{60} \begin{pmatrix} -30 \\ 10 \\ -30 \end{pmatrix} \Leftrightarrow \vec{x} \equiv_{60} \begin{pmatrix} -30 \\ 10 \\ -30 \\ x_4 \\ \vdots \\ x_{10} \end{pmatrix}.$$

Der Vektor $\vec{y}$ lässt sich dann bestimmen durch:

$$\vec{y} \equiv_{60} C\vec{x} \equiv_{60} \begin{pmatrix} 30 - x_4 - x_5 \\ x_5 \\ 0 \\ x_4 \\ 40 + x_4 - x_7 - x_{10} \\ 30 - x_{10} \\ x_7 \\ 0 \\ 0 \\ x_{10} \end{pmatrix}, \text{ wobei } x_4, x_5, x_7, x_{10} \in \mathbb{Z}/60\mathbb{Z}.$$

Somit ist die Lösungsmenge

$$L = \left\{ \left(\begin{array}{c} 30 - y_4 - y_5 \\ y_5 \\ 0 \\ y_4 \\ 40 + y_4 - y_7 - y_{10} \\ 30 - y_{10} \\ y_7 \\ 0 \\ 0 \\ y_{10} \end{array} \right) \middle| y_4, y_5, y_7, y_{10} \in \mathbb{Z}/60\mathbb{Z} \right\}.$$

y_1 ist bekanntlich Null. Damit gilt

$$-30 - y_4 - y_5 \equiv_{60} 0 \Leftrightarrow y_5 \equiv_{60} 30 + y_4$$

Weiterhin gilt

$$40 + y_4 - y_7 - y_{10} \equiv_{60} y_5.$$

Eingesetzt in den Lösungsvektor ergibt dies

$$\vec{y} \equiv_{60} \begin{pmatrix} 0 \\ 30 + y_4 \\ 0 \\ y_4 \\ y_5 \\ 30 - y_{10} \\ y_7 \\ 0 \\ 0 \\ y_{10} \end{pmatrix}.$$

Die Lösung des Verfahrens der Hermite-Normalform für das lineare Gleichungssystem entspricht damit der Lösung des Gauß-Algorithmus.
Folglich ist ebenso die Lösung für das Periodic Event Scheduling Problem identisch. Die Gewichtsfunktion $\sum_{a \in A} w_a y_a$ ist für $y_5{=}y_7{=}0$ und $0 \leq \ y_4, y_{10} \leq \ 30$ minimal. Es gilt

$$L_{PESP} = \left\{ \left(\begin{array}{c} 0 \\ 30 + y_4 \\ 0 \\ y_4 \\ 0 \\ 30 - y_{10} \\ 0 \\ 0 \\ 0 \\ y_{10} \end{array} \right) \middle| y_4, y_{10} \in \mathbb{Z}/60\mathbb{Z}, 0 \leq \ y_4, y_{10} \leq \ 30 \right\}.$$

3. Smith-Normalform

Eine weitere Möglichkeit, das Problem zu lösen, bietet die Smith-Normalform. Weil die Matrix Γ ausschließlich aus den Zahlen 1,-1 und 0 besteht, muss Γ lediglich in eine Diagonalmatrix mit positiven Einträgen überführt werden, die der Hermite-Normalform entspricht:

$$SNF(\Gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\text{wobei } U = \begin{pmatrix} 1 & 0 & 0 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{und } V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Im Vergleich zur Hermite-Normalform nichts verändert, denn $U = C$ und $SNF(\Gamma)V = HNF(\Gamma)$.

Folglich ändert sich die Lösungsmenge ebenfalls nicht:

$$L = \left\{ \left(\begin{array}{c} 0 \\ 30 + y_4 \\ 0 \\ y_4 \\ y_5 \\ 30 - y_{10} \\ y_7 \\ 0 \\ 0 \\ y_{10} \end{array} \right) \middle| \, y_4, y_5, y_7, y_{10} \in \mathbb{Z}/60\mathbb{Z} \right\}.$$

Analog zum Gauß-Algorithmus und zum Lösungsverfahren der Hermite-Normalform ist die Lösung des Minimierungsproblems

$$L_{PESP} = \left\{ \left(\begin{array}{c} 0 \\ 30 + y_4 \\ 0 \\ y_4 \\ 0 \\ 30 - y_{10} \\ 0 \\ 0 \\ 0 \\ y_{10} \end{array} \right) \middle| y_4, y_{10} \in \mathbb{Z}/60\mathbb{Z}, 0 \leq \ y_4, y_{10} \leq \ 30 \right\}.$$

4. Chinesischer Restsatz

Die Zahl 60 ist nicht in paarweise verschiedene Primfaktoren zerlegbar. Somit kann der chinesische Restatz, wie in Kapitel 4.4 erläutert, nicht angewandt werden. Damit ist das Periodic Event Scheduling Problem mit dem chinesischen Restsatz nicht lösbar.

In diesem Kapitel wurde das System der periodischen Taktfahrpläne vorgestellt. Es wurde anhand eines Beispiels vorgeführt, wie das mathematische Modell, Periodic Event Scheduling Problem, funktioniert. Mit Hilfe der in dieser Arbeit vorgestellten Rechenverfahren wurde das gegebene lineare Gleichungssystem modulo 60 gelöst und die Lösungsmenge, für welche die Gewichtsfunktion minimiert wird, angegeben.
Bei einem praktischen Problem wird die Lösung mit dem geringsten Gewicht gesucht. Die Herausforderung dabei ist, dass die Gewichtsfunktion bezüglich der modulo Rechnung nicht linear ist. Es ist somit schwierig an der Lösungsmenge zu erkennen, welche Lösung das geringste Gewicht aufweist.

6 Fazit

Im Rahmen dieser Bachelorarbeit wurde auf das Lösen linearer Gleichungssysteme über Restklassenringe $\mathbb{Z}/T\mathbb{Z}$, wobei T keine Primzahl ist, und das aktuelle Problem der periodischen Taktfahrpläne eingegangen. Zuerst wurden algebraische und zahlentheoretische Grundlagen wiederholt. In diesem Kapitel wurden Restklassenringe, Modulo-Rechnungen und das Lösen linearer Gleichungssysteme über Körper mittels Gauß-Algorithmus zentralisiert und anhand von Beispiele veranschaulicht. Im anschließenden Kapitel wurden die linearen diophantischen Gleichungssysteme betrachtet. Dabei ist jedes Element aus diesem Gleichungssystem aus der Menge der ganzen Zahlen. Da die ganzen Zahlen keinen Körper bilden, betrachtet man hierbei das Lösen jener Gleichungssysteme über Nicht-Körpern. Dies wurde mittels zwei bekannten Rechenverfahren von den Mathematikern Charles Hermite und Henry John Stephen Smith dargestellt. Zum einen die Hermite-Normalform und zum anderen die Smith-Normalform. Darauffolgend wurden lineare Gleichungssysteme modulo T, wobei T keine Primzahl ist, eingeführt. In diesem Kapitel wurden die bereits eingeführten Rechenverfahren beim Lösen dieser Gleichungssysteme genutzt. Zusätzlich wurde der chinesische Restzsatz als eine weitere Lösungsmöglichkeit eingeführt. Bei jedem Rechenverfahren wurde die Existenz und Eindeutigkeit der Lösung gezeigt. Außerdem wurden die Algorithmen zur Berechnung der Lösungen schrittweise erklärt. Abschließend wurden graphentheoretische Inhalte vermittelt, um das System der periodischen Taktfahrpläne zu erläutern. Dabei wurde auf das sogenannte „Periodic Event Scheduling Problem“, auch PESP, eingegangen. Hierbei handelt es sich um ein mathematisches Modell, welches sich mit der Minimierung der Wartezeit der Passagiere beschäftigt. Zu diesem Modell wurde ein Beispiel präsentiert, welches sich den vier bereits vorgestellten Rechenverfahren bedient. Diese Bachelorarbeit, entstanden aus der Motivation lineare Gleichungssysteme über Nicht-Körper zu lösen, soll unter anderem die Relevanz dieses Themenbereichs zeigen. Insbesondere erweist das mathematische Modell PESP die Möglichkeit der Zeiteinsparung für jeden Bürger, der öffentliche Verkehrsmittel nutzt. Ebenfalls bieten die linearen Gleichungssysteme über Nicht-Körper eine hohe Vielfalt an Anwendbarkeit. Dies kann als Motivation für weitere Studien dienen.

Literaturverzeichnis

[1] J.A. De Loera, R. Hemmecke, and M. KÓppe. *Algebraic and Geometric Ideas in the Theory of Discrete Optimization.* MOS-SIAM Series on Optimization. Society for Industrial and Applied Mathematics, 2013.

[2] Janko Böhm. *Grundlagen der Algebra und Zahlentheorie.* Springer-Verlag, Berlin Heidelberg New York, 2016.

[3] A. Scholz and B. Schoeneberg. *Einführung in die Zahlentheorie.* Sammlung Göschen. De Gruyter, 1966.

[4] Friedrich Schwarz. *Einführung in die Elementare Zahlentheorie - Interaktives Buch mit CD-ROM.* Springer-Verlag, Berlin Heidelberg New York, 2013.

[5] Dipl.-Inform. Wolfgang Globke. Kurze Geschichte der linearen Algebra.

[6] Albrecht Beutelspacher. *Zahlen, Formeln, Gleichungen - Algebra für Studium und Unterricht.* Springer-Verlag, Berlin Heidelberg New York, 2017.

[7] K.-D. Drews. *Lineare Gleichungssysteme und lineare Optimierungsaufgaben.* Springer-Verlag, Berlin Heidelberg New York, 2013.

[8] Elmar Swarat. Taktfahrplanoptimierung , Neue Lösungsmethoden im Praxiseinsatz. Diplomarbeit, Technischen Universität Berlin, 2008.

[9] Jian Qin. *Mathematische Modellierung & Optimierung für das Stop Location Problem im ÖPNV - am Praxisbeispiel: Bahnstrecke Weimar-Jena.* disserta Verlag, Hamburg, 2014.

[10] K. Nachtigall. Taktfahrplanoptimierung , Neue Lösungsmethoden im Praxiseinsatz. Institutionsbericht, Deutsche Forschungsanstalt für Luft- und Raumfahrt e.V., 1999.

[11] Reinhard Diestel. *Graphentheorie.* Springer Berlin Heidelberg, Wiesbaden, 2017.

[12] Christian Liebchen and Leon Peeters. Integral cycle bases for cyclic timetabling. *Discrete Optimization*, 6(1):98 – 109, 2009.

[13] P. Serafini and W. Ukovich. A mathematical model for periodic scheduling problems. *SIAM J. Discret. Math.*, 2(4):550–581, November 1989.

Freie Universität Berlin

Selbstständigkeitserklärung

Name:	(Nur Block- oder Maschinenschrift verwenden.)
Vorname:	
geb.am:	
Matr.Nr.:	

Ich erkläre gegenüber der Freien Universität Berlin, dass ich die vorliegende _____ selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch bei keiner anderen Universität als Prüfungsleistung eingereicht.

Datum: _____ Unterschrift: _____