Kapitel 5 - Zahlentheorie und Algebraische Strukturen

Rolf Felder

January 24, 2023

5.1 Teilen und ggT

Definition : Sind $a, b \in \mathbb{Z}$, so heißt a durch b teilbar (b teilt a, in Zeichen $b|a$), wenn es eine ganze Zahl q gibt, so daß $a = b \cdot q$ ist.

Definition : Sind $a, b, d \in \mathbb{Z}$ und gilt $d|a$ und $d|b$, so heißt d ein gemeinsamer Teiler von a und b. Der größte **positive** gemeinsame Teiler von a und b heißt **größter gemeinsamer Teiler** von a und b und wird mit **ggT(a,b)** bezeichnet.

Hilfssatz : Seien $a, b, q \in \mathbb{Z}$. Dann gilt

- Ist $a = b \cdot q$, so gilt $|b|$=ggT(a,b).
- Ist $a = b \cdot q + r$ mit $0 < r < |b|$, so gilt ggT(a,b)=ggT(b,r).

Wichtig, mitzunehmen : Der **ggT** sowie ein nicht verschwindender Rest **r** bei der Division sind positive Zahlen !!

Beispiele :

1. $a = 54, b = 18 : \ 54 = 18 \cdot 3 + 0 \Rightarrow \ \text{ggT}(54, 18) = 3$
2. $a = 7, b = 5 : \ 7 = 5 \cdot 1 + 2 \Rightarrow q = 1, r = 2$
3. $a = -7, b = 5 : \ -7 = 5 \cdot (-2) + 3 \Rightarrow q = -2, r = 3$

Nach dem obig beschriebenen Hilfssatz lässt sich der ggT iterativ bestimmen, indem man bei jedem Schritt die betrachteten Zahlen betragsmäßig kleiner macht. Der 'Abstieg' endet, sobald bei der aktuell betrachteten Division der auftretende Rest den Wert 0 besitzt. Das hierfür verwendete Verfahren ist der sog. **Euklidische Algorithmus**, dessen Mechanik an den folgenden Beispielen dargestellt werden soll.

5.1 Teilen und ggT

Beispiel 1 : Zu bestimmen ist der ggT der Zahlen 42 und 133.

1. $133 = 42 \cdot 3 + 7 \Rightarrow$ggT(133,42)=ggT(42,7)
2. $42 = 7 \cdot 6 \Rightarrow$ ggT(42,7))=7 $\Rightarrow$ **ggT(133,42)=7** (7 ist der letzte in der Folge der Divisionen nicht verschwindende Rest)

Es kann festgestellt werden, dass sich der ggT darstellen als Summe von Vielfachen der beiden ihn hervorbringenden Zahlen, den beiden 'Ausgangsakteuren' :

$$7 = 1 \cdot 133 + (-3) \cdot 42.$$

Beispiel 2 : Zu bestimmen ist der ggT der Zahlen 92 und 64.

1. $92 = 64 \cdot 1 + 28 \Rightarrow$ggT(92,64)=ggT(64,28)
2. $64 = 28 \cdot 2 + 8 \Rightarrow$ ggT(64,28))=ggT(28,8)
3. $28 = 8 \cdot 3 + 4 \Rightarrow$ ggT(28,8))=ggT(8,4)
4. $8 = 4 \cdot 2 \Rightarrow$ ggT(8,4)=4 $\Rightarrow$ **ggT(92,64)=4** (4 ist der letzte in der Folge der Divisionen nicht verschwindende Rest)

Auch hier ergibt sich wiederum die Vielfachsummendarstellung :

$$4 = 1 \cdot 28 + (-3) \cdot 8 = 1 \cdot 28 + (-3) \cdot (64 + (-2) \cdot 28) = 7 \cdot 28 + (-3) \cdot 64 =$$

$$7 \cdot (92 + (-1) \cdot 64) + (-3) \cdot 64 = 7 \cdot 92 + (-10) \cdot 64.$$

5.1 Teilen und ggT

Feststellungen / Resümee : Aus den Beispielen lassen sich plausibilisieren

1. Der ggT zweier Zahlen a und b ($a > b$) lässt sich berechnen mittels sukzessiver Durchführung der Division mit Rest. Startpunkt ist die Division mit Rest $a : b$. Der Endpunkt des Verfahrens ist erreicht, wenn kein Rest mehr auftritt. Der letzte nicht verschwindende Rest ist der gesuchte ggT.

2. Der ggT zweier Zahlen a und b ($a > b$) lässt sich immer darstellen in der Form ggT(a,b)=$\alpha \cdot a + \beta \cdot b$ mit ($\alpha, \beta \in \mathbb{Z}$) (sog. Vielfachsummendarstellung). Um diese **Vielfachsummendarstellung** zu ermitteln werden die Zwischenergebnisse aus den einzelnen Schritte des euklidischen Algorithmus verwendet.

Ergänzungen :

1. Der ggT mehrerer Zahlen kann iterativ folgendermassen bestimmt werden

$$\mathbf{ggT}(a_1, a_2, .., a_n) = \mathbf{ggT}(a_1, \mathbf{ggT}(a_2, .., a_n)).$$

2. Das kgV (**'kleinstes gemeinsames Vielfaches'**) von zwei Zahlen a, b bestimmt sich aus der Gleichung

$$\mathbf{ggt}(a, b) \cdot \mathbf{kgV}(a, b) = a \cdot b.$$

Das **kgV** ist für den weiteren Verlauf der Vorlesung nicht relevant.

5.1 Üben und Verstehen

Übung 1: Berechnen Sie den ggT(217,63) und stellen Sie den ggT als Vielfachsumme von 217 und 63 dar.

Übung 2: Berechnen Sie den ggT(672,105) und stellen Sie den ggT als Vielfachsumme von 672 und 105 dar.

5.2 Modulare Arithmetik / Modulares Rechnen

Ein weiteres Thema der diskreten Mathematik mit vielen Anwendungen in der Praxis ist das modulare Rechnen.

Definition : Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Die Zahlen a, b heißen kongruent modulo n, wenn a-b durch n teilbar ist. In Zeichen $a \equiv b \bmod n$.

Satz : Zu einem beliebig aber fest vorgegebenen n stellt '$\equiv$' auf $\mathbb{Z} \times \mathbb{Z}$ eine Äquivalenzrelation dar. Für die Äquivalenzklasse einer ganzen Zahl a gilt : $[a] = \{z \in \mathbb{Z} | z \equiv a \bmod n\} = \{z \in \mathbb{Z} | n|(z-a)\}$. Man schreibt auch $[a] = \{z \in \mathbb{Z} | z \bmod n = a \bmod n\}$. In der Äquivalenzklasse von a sind damit alle die ganzen Zahlen enthalten, die durch n geteilt den gleichen Rest ergeben, als wenn a durch n geteilt wird.

Beispiel n=5: (s. Kapitel 3, Seite 12) Es gilt

- $[0] = \{.., -5, 0, 5, 10, 15, 20, ...\}$
- $[1] = \{.., -4, 1, 6, 11, 16, 21, ...\}$
- $[2] = \{.., -3, 2, 7, 12, 17, 22, ...\}$
- $[3] = \{.., -2, 3, 8, 13, 18, 23, ...\}$
- $[4] = \{.., -1, 4, 9, 14, 19, 24, ...\}$

Somit gelten z.B. die Identitäten $[0] = [15] = [675]$ oder auch $[29] = [9]$. Die Menge der ganzen Zahlen ist somit auf 5 Äquivalenzklassen verteilt. Diese Menge der Äquivalenzklassen wird auch bezeichnet als $\mathbb{Z}/5\mathbb{Z}$ oder als $\mathbb{Z}_5$ gleich Menge der Restklassen modulo 5. Es gilt also $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

5.2 Modulare Arithmetik / Modulares Rechnen

Hervorhebung - Schreibweisen :

- Die Schreibweise '$z \equiv a \mod n$' bedeutet, daß z bei der Division durch n den gleichen Rest läßt wie a
- Die Schreibweise '$z \mod n$' bezeichnet den Rest, der bei der Division von z durch n entsteht
- Die Schreibweise '$z \mod n = a \mod n$' drückt aus, daß bei der Division von z durch n der gleiche Rest entsteht wie bei der Division von a durch n

5.2 Modulare Arithmetik / Modulares Rechnen

Definition : Es seien a, b $\in \mathbb{Z}$ und $[a], [b]$ die Restklassen modulo n von a und b. Dann sind auf $\mathbb{Z}_n$ folgende beiden Operationen $\oplus, \otimes$ definiert

- $[a] \oplus [b] := [a + b]$ (Addition)
- $[a] \otimes [b] := [a \cdot b]$ (Multiplikation)

Statt nun mit den Restklassen zu rechnen, wird der Einfachheit halber mit den ausgewählten Resten d.h. mit den Elementen der Menge $\{0, 1, 2, ..., n-1\}$, die bei der Teilung durch n auftreten, gerechnet, so dass sich für die Addition / Multiplikation von 2 Elementen a,b $\in \{0, 1, 2, ..., n-1\} = \mathbb{Z} + n\mathbb{Z} = \mathbb{Z}_n$ ergibt :

$a \oplus b = (a + b)$ mod n bzw. $a \otimes b = (a \cdot b)$ mod n.

Aus dieser Definition ergeben sich am Beispiel von $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$ bzw. $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ somit folgende Verknüpfungstabellen :

5.2 Modulare Arithmetik / Modulares Rechnen

Im Vorgriff auf das Teilkapitel 5.4 definieren machen wir uns an dieser Stelle vertraut mit der algebraischen Struktur der **Gruppe** :

Definition : Gruppenaxiome auf (G,∘) - Eine Gruppe (G,∘) besteht aus einer Menge G und einer Verknüpfung '∘' auf G mit den folgenden Eigenschaften

1. Es gibt ein Element $e \in G$ mit der Eigenschaft $a \circ e = e \circ a = a$ für alle $a \in G$. **e heißt neutrales Element von G**.
2. Zu jedem $a \in G$ gibt es ein **eindeutig bestimmtes Element** $a^{-1} \in G$ mit der Eigenschaft $a \circ a^{-1} = a^{-1} \circ a = e$. a^{-1} **heißt inverses Element zu a**.
3. Für alle a,b,c $\in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$. **G ist assoziativ bezgl. '∘'**.

Eine Gruppe (G,∘) heißt **kommutative oder auch abelsche Gruppe**, wenn zusätzlich gilt: Für alle a,b $\in G$ ist $a \circ b = b \circ a$.

Seitenblick : Wie bei den Verbänden $(\{0,1\}, \wedge, \vee)$ und $(\mathbb{P}(\Omega), \cap, \cup)$ benutzen wir hier eine ähnliche Schreibweise in einer Situation, in der wir eine Menge von Objekten vorliegen haben, die mittels einer oder mehrerer Operationen aufeinander treffen können und ein Ergebnis produzieren, welches wieder Element der Menge ist.

5.2 Modulare Arithmetik / Modulares Rechnen

Additionstabelle n=5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplikationsstabelle n=5

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Additionstabelle n=6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplikationsstabelle n=6

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

5.2 Modulares Rechnen - Beispiele

Beispiel 1 : Was ergibt $5+3+1+4$ in der Restklassengruppe $\mathbb{Z}_6$?

Beispiel 2 : Was ergibt $4 \cdot 3$ in der Restklassengruppe $\mathbb{Z}_6$? Was bedeutet $4 \cdot 3$?

Frage 1 : Welche Beziehung besteht zwischen einer positiven reellen Zahl und ihrem negativen Pendant ? Z.B. zwischen **+3 und -3** oder zwischen **+10.5 und - 10.5** ?

Beispiel 3 : Was ist -3 in der Restklassengruppe $\mathbb{Z}_5$? Was ist -5 in der Restklassengruppe $\mathbb{Z}_6$?

Beispiel 4 : Was ergibt $4-3 \cdot 2+1$ in der Restklassengruppe $\mathbb{Z}_5$?

Frage 2 : Welche Beziehung besteht zwischen den beiden rationalen Zahlen $\frac{1}{2}$ und 2 ? Welche zwischen $\frac{1}{39}$ und 39 ? Welche zwischen $\frac{1}{365}$ und 365 ?

Beispiel 5 : Was ist $\frac{1}{3}$ in der Restklassengruppe $\mathbb{Z}_5$? Was ist dort $\frac{1}{4}$?

Beispiel 6 : Was ergibt $\frac{1}{3}-\frac{1}{2}+4$ in Restklassengruppe $\mathbb{Z}_5$? Was ist $\frac{2}{3}-\frac{3}{4}+2$ in $\mathbb{Z}_5$?

Etwas ganz anderes :

Beispiel 7 : Welchen Rest erhält man, wenn man die Zahl 38^{67} durch 3 teilt ?

Beispiel 8 : Welchen Rest erhält man, wenn man die Zahl 57^{183} durch 5 teilt ?

5.3 Einsatzgebiete ggt und modulares Rechnen

Im Anwendungsbereich Kryptographie und damit insbesondere in der Praxis der IT-Sicherheit kommen bei Problemstellungen

- der Ver- und Entschlüsselung von Daten
- der Authentikationsprüfung von Daten
- der Authentikationsprüfung von Personen
- von Signaturverfahren
- der Anonymisierung von Kommunikationsbeziehungen sowie den beteiligten Kommunikationsteilnehmern

die in Ansätzen besprochenen und weitere Grundlagen der Zahlentheorie tragend zum Einsatz . Insbesondere z.B.

- Modulares Rechnen bei der Definition von Hash- und Einwegfunktionen zum Zwecke der Authentikationsprüfung von Daten
- ggT-Berechnung und modulares Rechnen bei der Umsetzung des RSA-Verfahrens, welches z.B. bei der Ver- und Entschlüsselung von Daten sowie bei bestimmten Signaturverfahren zum Einsatz kommt

Modulares Rechnen ist die Grundrechenart der gesamten modernen Kryptographie. Der **euklidische Algorithmus** sowie die **ggT-Bestimmung** sind **wesentliche Bestandteile** verbreiteter **kryptographischer Verfahren der Gegenwart**.

Der Einsatz des modularen Rechnens in der Kryptographie soll auf den Folgeseiten an ein paar wenigen, ganz einfachen Verschlüsselungsverfahren gezeigt werden.

5.3 Einsatzgebiete ggT und modulares Rechnen

Verschiebechiffre (Cäsarchiffrierung) zur Ver- und Entschlüsselung von Texten :
Bestandteile des Verfahrens bezogen auf einen einzelnen Buchstaben

- **Verschlüsselungsvorgang :**
  1. Schritt : Ermittle Position y_x des zu verschlüsselnden Buchstaben x
  2. Schritt : Ermittle Position u_x des verschlüsselten Buchstaben nach der Formel $u_x = f_K(x) = y_x + K \mod 26, K \in \{0, 1, 2, ..., 25\}$ $(f_K : \mathbb{Z}_{26} \to \mathbb{Z}_{26})$.
  3. Schritt : Ermittle verschlüsselten Buchstaben u aus seiner Position u_x

- **Entschlüsselungsvorgang :**
  1. Schritt : Ermittle Position v_u des verschlüsselten Buchstaben u
  2. Schritt : Ermittle Position y_x des entschlüsselten Buchstabens nach der Formel $y_x = f_K^{-1}(u) = v_u + (26 - K) \mod 26$ $(f_K^{-1} : \mathbb{Z}_{26} \to \mathbb{Z}_{26})$
  3. Schritt : Ermittle entschlüsselten Buchstaben x aus der Position y_x

Buchstaben-Tabelle :

A	0	H	7	O	14	V	21
B	1	I	8	P	15	W	22
C	2	J	9	Q	16	X	23
D	3	K	10	R	17	Y	24
E	4	L	11	S	18	Z	25
F	5	M	12	T	19		
G	6	N	13	U	20		

5.3 Einsatzgebiete ggT und modulares Rechnen

Charakterisierung und Bewertung der Verschiebe-Chiffre :

- Das Verfahren ist denkbar einfach - daher auch nicht besonders sicher
- Es handelt sich um ein sogenanntes monoalphabetisches Verschlüsselungsverfahren - ein bestimmter Buchstabe wird immer zu ein und dem gleichen Buchstaben verschlüsselt
- Im Vergleich hierzu gibt es sogenannte polyalphabetische Verschlüsselungsverfahren, bei denen ein Buchstabe nach dem Zufallsprinzip in verschiedene Buchstaben verschlüsselt wird (2 bekannte Arten : Homophone Chiffre und Vigenère Chiffre)

5.3 Einsatzgebiete ggT und modulares Rechnen

Die Multiplikative Chiffre besteht aus den folgenden Komponenten

- **Schlüssel :** Faktor $s \in \mathbb{N}; 0 \leq s < 26$; s teilerfremd zu 26, d.h. $s \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$
- **Algorithmus - Chiffrieren :** Wenn y_x die laufende Nummer eines Klartextbuchstaben x im deutschen Alphabet ist, so ist $v_u = y_x \cdot s \bmod 26$ die laufende Nummer des Geheimtextbuchstabens u im deutschen Alphabet
- **Algorithmus - Dechiffrieren :** Wenn v_u die laufende Nummer eines Geheimtextbuchstaben u im deutschen Alphabet ist, so ist $y_x = v_u \cdot s' \bmod 26$ die laufende Nummer des Klartextbuchstabens x im deutschen Alphabet. Hierbei ist $s' \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ die Zahl, für die $s \cdot s' \bmod 26 = 1$ gilt.

Die Zahl s muss teilerfremd zu 26 sein, weil andernsfalls die Ver-/Entschlüsselung nicht bijektiv wären. Da s teilerfremd zu 26 sein muss, gilt für s (s.o. in der Definition des Verfahrens) $s \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$.

Für die multiplikative Chiffre gibt es also nur 12 Möglichkeiten.

Die Buchstaben des Geheimtextalphabetes sind bei der multiplikativen Chiffre relativ zu den ihnen jeweils zugeordneten Zahlen, im Vergleich zum deutschen Alphabet, nicht mehr gleich geordnet. Diese Eigenschaft war aufgrund der 'Linearität' bei der Verschiebe-Chiffre gegeben.

5.3 Üben und Verstehen

Beispiel / Übung 1 : Unterwerfen Sie das Wort 'KARLSRUHE' einer Cäsar-Verschlüsselung mit K=23. Wie lauten die ersten drei Buchstaben des verschlüsselten Wortes ?

Beispiel / Übung 2 : Entschlüsseln Sie das verschlüsselte 'BIPGKFCFXZV' einer Cäsar-Verschlüsselung mit K=17. Wie lauten die ersten drei Buchstaben des entschlüsselten Wortes ?

Beispiel / Übung 3 : Verschlüsseln Sie die Abkürzung 'DHBW' mittels einer multiplikativen Chiffre mit $s = 15$. Wie lautet der Geheimtext ?

Buchstabentabelle :

A	0	H	7	O	14	V	21
B	1	I	8	P	15	W	22
C	2	J	9	Q	16	X	23
D	3	K	10	R	17	Y	24
E	4	L	11	S	18	Z	25
F	5	M	12	T	19		
G	6	N	13	U	20		

5.3 Einsatzgebiete ggT und modulares Rechnen

RSA-Verfahren : Vorhaben : Text soll möglichst sicher verschlüsselt übermittelt werden.

- Man wählt : 2 große Primzahlen p und q
- Man berechnet : $n = p \cdot q$
- Man berechnet : $\phi(n) = (p-1) \cdot (q-1)$
- Man wählt : e teilerfremd zu $\phi(n)$
- Man ermittelt $d \in \mathbb{N}$, für das gilt : $d \cdot e + c \cdot \phi(n) = 1$ (Vielfachsummendarstellung nach Berechnung ggT$(e, \phi(n))$ mittels euklidischem Algorithmus)

Zugewiesene Rollen bei der Verschlüsselung

- Geheime Parameter bei der Schlüsselerzeugung : $p, q, \phi(n)$
- Privater Schlüssel des Teilnehmers : d (Empfänger)
- Öffentlicher Schlüssel des Teilnehmers : e,n (Sender)

5.3 Einsatzgebiete ggT und modulares Rechnen

Das Vorgehen zur Übermittlung eines Textes erfolgt in den folgenden Schritten

Auf der Senderseite :

- **1. Schritt :** Umwandlung des Textes in Zeichenfolge
- **2. Schritt :** Umwandlung der Zeichenfolge in eine Folge von Zahlen x_i
- **3. Schritt :** Berechne nacheinander für jede Zahl x_i der Zahlenfolge die Zahl y_i gemäß $x_i^e \equiv y_i \mod n$
- **4. Schritt :** Übermittlung der Zahlenfolge y_i an den Empfänger

Auf der Empfängerseite :

- **1. Schritt :** Empfang der Zahlenfolge y_i vom Sender
- **2. Schritt :** Berechne nacheinander für jede Zahl y_i der Zahlenfolge die Zahl x_i gemäß $y_i^d \equiv x_i \mod n$
- **3. Schritt :** Rückumwandlung der Zahlenfolge x_i in eine Zeichenfolge
- **4. Schritt :** Umwandlung Zeichenfolge in Text

5.3 Einsatzgebiete ggT und modulares Rechnen

Beispiel RSA-Verfahren für ein einzelnes Zeichen (mit kleinen Primzahlen) :
Einmalige Aktivität bei Implementierung des Verschlüsselungsverfahrens :

- Man wählt : 2 'große' Primzahlen p und q - Wähle $p = 13, q = 19$
- Man berechnet : $n = p \cdot q$ - Berechne : $n = 13 \cdot 19 = 247$
- Man berechnet : $\phi(n) = (p-1) \cdot (q-1)$ - Berechne $\phi(247) = 12 \cdot 18 = 216$
- Man wählt : e teilerfremd zu $\phi(n)$ - Wähle : $e = 5$
- Man ermittelt $d \in \mathbb{N}$, für das gilt : $d \cdot e + c \cdot \phi(n) = 1$ - Ermittle : $173 \cdot 5 - 4 \cdot 216 = 1$. Erhalte also $d = 173$.

Vorgehen auf der Senderseite bei der Verschlüsselung der Zahl $x = 30$ (Beispiel):

- Berechne $30^5 \equiv y \bmod 247$ und erhalte $y = 140$
- Übermittle 140 an den Empfänger

Vorgehen auf der Empfängerseite :

- Berechne $140^{173} \equiv x \bmod 247$ und erhalte $x = 30$
  (Geschicktes Vorgehen ist z.B. das nach dem Square- and Multiply-Verfahren $173 = 2^7 + 2^5 + 2^3 + 2^2 + 2^0 = 128 + 32 + 8 + 4 + 1$ - Rechne dann

$$\begin{array}{cc} 140^1 \equiv 140 \bmod 247 & 140^2 \equiv 87 \bmod 247 \\ 140^4 \equiv 87^2 \equiv 159 \bmod 247 & 140^8 \equiv 159^2 \equiv 87 \bmod 247 \\ 140^{16} \equiv 87^2 \equiv 159 \bmod 247 & 140^{32} \equiv 159^2 \equiv 87 \bmod 247\,' \\ 140^{64} \equiv 87^2 \equiv 159 \bmod 247 & 140^{128} \equiv 159^2 \equiv 87 \bmod 247 \end{array}$$

was impliziert $140^{173} \equiv 140 \cdot 159 \cdot 87 \cdot 87 \cdot 87 \equiv 30 \bmod 247$ Damit hat der Empfänger die 'Klartextzahl' 30 aus der übermittelten verschlüsselten Zahl 140 wiedergewonnen.

5.4 Algebraische Strukturen

Im Kapitel 5.4. sollen die algebraischen Strukturen

- Gruppen
- Ringe
- Körper

in ihren Grundzügen definiert und an einfachen Beispielen beobachtet werden.

5.4.1 Algebraische Strukturen - Gruppen / Gruppenaxiome

Definition : Gruppenaxiome auf (G,$\circ$) - Eine Gruppe (G,$\circ$) besteht aus einer Menge G und einer Verknüpfung '$\circ$' auf G mit den folgenden Eigenschaften

1. Es gibt ein Element $e \in G$ mit der Eigenschaft $a \circ e = e \circ a = a$ für alle $a \in G$. **e heißt neutrales Element von G**.
2. Zu jedem $a \in G$ gibt es ein **eindeutig bestimmtes Element** $a^{-1} \in G$ mit der Eigenschaft $a \circ a^{-1} = a^{-1} \circ a = e$. a^{-1} **heißt inverses Element zu a**.
3. Für alle a,b,c $\in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$. **G ist assoziativ bezgl. '$\circ$'**.

Eine Gruppe (G,$\circ$) heißt **kommutative oder auch abelsche Gruppe**, wenn zusätzlich gilt: Für alle a,b $\in G$ ist $a \circ b = b \circ a$,

Beispiele :

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ sind (kommutative) Gruppen.
- $(\mathbb{N}, +)$ ist keine Gruppe - warum nicht ?
- $(\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$ sind (kommutative) Gruppen.
- $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist keine Gruppe - warum nicht ?
- $(\mathbb{Z}_5, +)$ und $(\mathbb{Z}_6, +)$ sind (kommutative) Gruppen - **anhand der Additionstabellen auf Seite 11 klarmachen**.
- $(\mathbb{Z}_5 \setminus \{0\}, \times)$ ist eine (kommutative) Gruppe - **anhand der Multiplikationstabelle auf Seite 11 klarmachen**.
- $(\mathbb{Z}_6 \setminus \{0\}, \times)$ ist keine Gruppe - warum nicht ? **Anhand der Multiplikationstabelle auf Seite 11 begründen**.

5.4.1 Algebraische Strukturen - Gruppen / Gruppenaxiome

Warum ist $(\mathbb{Z}, +)$ eine Gruppe ? Antwort :

1. Es gibt ein Element $0 \in \mathbb{Z}$ mit der Eigenschaft $a + 0 = 0 + a = a$ für alle $a \in \mathbb{Z}$. Die 0 ist also das neutrale Element in $\mathbb{Z}$.
2. Zu jedem $a \in \mathbb{Z}$ gibt es ein eindeutig bestimmtes Element $-a \in \mathbb{Z}$ mit der Eigenschaft $a + (-a) = (-a) + a = 0$. $-a$ heißt inverses Element zu a.
3. Für alle a,b,c $\in \mathbb{Z}$ gilt $a + (b + c) = (a + b) + c$. $\mathbb{Z}$ ist assoziativ bezgl. '+'.

Warum ist $(\mathbb{Q} \setminus \{0\}, \cdot)$ eine Gruppe ? Antwort :

1. Es gibt ein Element $1 \in \mathbb{Q}$ mit der Eigenschaft $a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Q}$. 1 heißt neutrales Element von $\mathbb{Q}$.
2. Zu jedem $a \in \mathbb{Q}$ gibt es ein eindeutig bestimmtes Element $a^{-1} \in \mathbb{Q}$ mit der Eigenschaft $a \cdot a^{-1} = a^{-1} \cdot a = 1$. a^{-1} heißt inverses Element zu a.
3. Für alle a,b,c $\in \mathbb{Q}$ gilt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. $\mathbb{Q}$ ist assoziativ bezgl. '$\cdot$'.

5.4.2 Algebraische Strukturen - Körper / Körperaxiome

Definition : Eine Menge G mit den Operationen $+$ und $\times$, also eine Struktur $(G, +, \times)$ wird **Körper** genannt, wenn

- $(G, +)$ eine kommutative Gruppe mit neutralem Element 0 darstellt
- $(G \setminus \{0\}, \times)$ eine kommutative Gruppe mit neutralem Element 1 darstellt
- $\forall a, b, c \in G : a \times (b + c) = a \times b + a \times c$ (Distributiv-Gesetz)

Beispiele :

- $(\mathbb{Q}, +, \cdot)$ ist ein Körper
- $(\mathbb{R}, +, \cdot)$ ist ein Körper
- $(\mathbb{Z}_5, +, \cdot)$ ist ein Körper
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper
- $(\mathbb{Z}_6, +, \cdot)$ ist kein Körper

Bemerkungen :

- Es gibt unendliche Körper wie $(\mathbb{Q}, +, \cdot)$ oder $(\mathbb{R}, +, \cdot)$.
- Es gibt endliche Körper wie $(\mathbb{Z}_5, +, \cdot)$.
- $(\mathbb{Z}_n, +, \cdot)$ ist i.a. kein Körper. $(\mathbb{Z}_n, +, \cdot)$ ist ein Körper genau dann, wenn n eine Primzahl ist.

5.4.3 Algebraische Strukturen - Ringe und Ringaxiome

Definition : Ringaxiome

Ein **Ring** (R,$\oplus$,$\otimes$) besteht aus einer Menge R und zwei Verknüpfungen $\oplus$,$\otimes$ auf R mit den folgenden Eigenschaften

1. $(R, \oplus)$ ist eine kommutative Gruppe
2. Für alle a,b,c $\in$ R gilt $a \otimes (b \otimes c) = (a \otimes b) \otimes c$. R ist assoziativ bezgl. $\otimes$.
3. Für alle a,b,c $\in$ R gilt $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$. R ist distributiv.

Ein Ring (R,$\oplus$,$\otimes$) heißt kommutativ, wenn zusätzlich gilt : Für alle a,b $\in G$ ist $a \otimes b = b \otimes a$. Ein Ring heisst 'Ring mit Eins', wenn in R ein Einselement bezgl. der Operation $\otimes$ enthalten ist.

Beispiele für Ringe: $(\mathbb{Z}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sind allesamt kommutative Ringe.

Beispiele für Ringe mit Eins : $(\mathbb{Z}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sind allesamt kommutative Ringe mit Eins.

Ringe mit Eins, die Körper sind : $(\mathbb{R}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$(n Primzahl)

Ringe mit Eins, die keine Körper sind : $(\mathbb{Z}, +, \cdot), (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$(n keine Primzahl)

5.4.3 Algebraische Strukturen - Ringe und Ringaxiome

In Ringen wie beispielsweise $(\mathbb{Z}, +, \cdot)$ (s. Kapitel 5.1) kann man definieren und durchführen

- Division mit Rest und Restklassen (i.S. von Äquivalenzklassen)
- euklidischen Algorithmus
- ggT-Bestimmung

was nun auf einen weiteren Spezialfall übertragen werden soll.

5.5 Polynome und Polynomringe

Im Kapitel 5.5 soll festgestellt werden, dass sich die bereits betrachtete und untersuchte Struktur $(\mathbb{Z}, +, \cdot)$ in die Welt der aus der Schule bekannten **Polynome** übertragen lässt.

Polynome spielen in nennenswerten Bereichen der angewandten Mathematik wie z.B.

- bei Approximationen und Interpolationen in der numerischen Mathematik
- bei der mathematischen Konzeption leistungsfähiger und sicherer kryptographischer Verfahren
- bei der Diagonalisierung von quadratischen Matrizen (s. Kapitel 13)

eine wichtige Rolle.

5.5.1 Polynome und Polynomringe - Definitionen

Definition : Sei K ein beliebiger Körper (z.B. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_2, \mathbb{Z}_5$). Eine Abbildung $p : K \to K$ der Form $p(x) = \sum_{i=0}^{n} a_i \cdot x^i = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0$ (mit $n \in \mathbb{N} \cup \{0\}$) heißt **Polynom über dem Körper K**. Die Zahlen $a_i \in K$ werden Koeffizienten des Polynoms genannt.

Damit gilt : $K[x] = \{p(x) = \sum_{i=0}^{n} a_i \cdot x^i | a_n \neq 0, a_i \in K(i \in \{0, ..n\}), n \in \mathbb{N} \cup \{0\}\}$

Definition : Unter der Voraussetzung $a_n \neq 0$ nennt man n=deg(p) den Grad des Polynoms. Der **Grad eines Polynoms** ist also der **höchste vorkommende Exponent**. Ein Polynom, bei dem der **Koeffizient der höchsten x-Potenz** $a_n \neq 0$ den **Wert 1** hat, nennt man **normiert**.

Beispiele :

- Polynome aus $\mathbb{R}[x]$ sind z.B. $\pi x^5 + 2x^3 - 34, \sqrt{2}x^2 - x + 3, x^3 + 1$ (nicht normiert)
- Polynome aus $\mathbb{Q}[x]$ sind z.B. $\frac{1}{4}x^5 + 1.1x^3 - 34, -0.34x^2 - x + 3, x^3 + 1$ (nicht normiert)
- Polynome aus $\mathbb{Z}_2[X]$ sind z.B. $x^5 + x^3 + x + 1, x^2 + x + 1$ (normiert)
- Polynome aus $\mathbb{Z}_5[X]$ sind z.B. $4x^5 + 3x^3 + 2x^2 + 4, 3x^2 + 2x + 4$ (nicht normiert)

5.5.2 Polynome und Polynomringe - Grundrechenarten

$(K[x], +, \cdot)$ stellt bezgl. der in K definierten Addition und Multiplikationen einen **kommutativen Ring mit 1** dar.

Beispiel für Addition in $\mathbb{R}[x]$:
$(x^3 - 4x^2 + 5x + 24) + (-x^4 - 2x^3 + 16) = -x^4 - x^3 - 4x^2 + 5x + 40$

Beispiel für Multiplikation in $\mathbb{R}[x]$:
$(x^2 + 2x + 2) \cdot (x^2 - 3x - 3) = x^4 - x^3 - 7x^2 - 12x - 6$

Beispiel für Addition in $\mathbb{Z}_2[x]$: $(x^3 + x^2 + x + 1) + (x^4 + x^3 + x^2) = x^4 + x + 1$

Beispiel für Multiplikation in $\mathbb{Z}_5[x]$: $(2x^2 + 4x + 3) \cdot (3x + 4) = x^3 + 2$

Zur Begründung, dass beispielsweise $(\mathbb{R}[x], +, \cdot)$ einen Ring mit 1 darstellt, lässt sich feststellen

1. $(\mathbb{R}[x], +)$ ist eine kommutative Gruppe. Das Nullpolynom ist das Nullelement, zu $p(x)$ ist $-p(x)$ das inverse Element.
2. Für alle $p_1(x), p_2(x), p_3(x) \in \mathbb{R}[X]$ gilt
   $p_1(x) \cdot (p_2(x) \cdot p_3(x)) = (p_1(x) \cdot p_2(x)) \cdot p_3(x)$.
3. Für alle $p_1(x), p_2(x), p_3(x) \in \mathbb{R}[X]$ gilt
   $p_1(x) \cdot (p_2(x) + p_3(x)) = p_1(x) \cdot p_2(x) + p_1(x) \cdot p_3(x)$.
4. Das Einselement ist das Polynom $p(x) = 1 \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + \ldots = 1$.

5.5.3 Polynome und Polynomringe - Division und ggT

Über die mittels Addition und Multiplikation definierten 'normalen' Operationen in $(K[x], +, \cdot)$ hinausgehend, kann wie auf der Struktur $(\mathbb{Z}, +, \cdot)$ eine **Division mit Rest**, ein **Euklidscher Algorithmus** und eine **ggT-Bestimmung** definiert werden.

Satz Polynomdivision (Division mit Rest) :

Sind p(x) und q(x) Polynome aus $K[x]$ mit deg(q) $\leq$ deg(p), dann gibt es Polynome s(x) und r(x), so daß gilt : $p(x) = s(x) \cdot q(x) + r(x)$. Der Grad von s(x) ist gleich der Differenz deg(p)-deg(q), der Grad des Restpolynoms r(x) ist kleiner als der des Polynoms q(x), d.h. es gilt deg(r) $<$ deg(q).

Satz zum Euklidschen Algorithmus für Polynome :

Auch zu 2 Polynomen p(x), q(x) kann der ggT bestimmt werden. Aus der Gleichung $p(x) = s(x) \cdot q(x) + r(x)$ ergibt sich sofort die Erkenntnis ggT(p(x),q(x))=ggT(q(x),r(x)), so dass sich analog zum Vorgehen bei der Bestimmung des ggT von zwei ganzen Zahlen nach endlich vielen Schritten ein Divisionsrest 0 ergibt. Der im Iterationsschritt davor sich ergebende, nicht verschwindende Rest ist (ggf. nach Durchführung einer Normierung) der ggT(p(x),q(x)).

Der **ggT von zwei Polynomen p(x) und q(x)** ist das **normierte Polynom höchsten Grades, das beide Polynome teilt**.

5.5.4 Polynome und Polynomringe - Division und ggT - Üben und Verstehen

Beispiele/Übung Polynomdivision und ggT-Bestimmung :

Folgende Polynomdivsionen mit Rest sind vorzunehmen, indem s(x) und r(x) aus dem Satz zur Polynomdivision bestimmt werden

1. $(x^3 + 2x) : (x + 1)$ in $\mathbb{R}[x]$
2. $(x^3 + 1) : (x + 1)$ in $\mathbb{R}[x]$
3. $(x^3 + 1) : (x + 1)$ in $\mathbb{Z}_2[x]$
4. $(x^3 + 2x + 2) : (x + 4)$ in $\mathbb{Z}_5[x]$
5. $(x^3 + 2x + 2) : (x + 4)$ in $\mathbb{Z}_7[x]$
6. $(x^3 + 2x + 2) : (x + 4)$ in $\mathbb{Z}_{11}[x]$

Beispiele/Übung Euklidscher Algorithmus / ggT-Bestimmung :

1. Zu berechnen ist der ggT $(x^3 + 3x^2 - 28x - 60, x^3 + 7x^2 + 4x - 12)$ in $\mathbb{R}[x]$
2. Zu berechnen ist der ggT $(x^3 + x^2 + x + 1, x^3 + x + 1)$ in $\mathbb{Z}_2[x]$

5.5.5 Polynome und Polynomringe - Zwischenstand

Zusätzliche Informationen :

1. Der ggT zweier Polynome kann analog der ggT-Darstellung bei Zahlen, d.h. analog zum Vorgehen in der Struktur $(\mathbb{Z}, +, \cdot)$ als Vielfachsumme der beiden Polynome dargestellt werden. Die Vielfachen sind Elemente von $K[X]$. Das Vorgehen hierfür wird aus Zeitgründen in der Vorlesung nicht besprochen.

2. Der ggT von mehr als zwei Polynomen ist iterativ wie bei Zahlen zu ermitteln - s. hierzu **Ergänzung, Seite 5**.

3. Analog zu den Restklassen $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ im Ring der ganzen Zahlen $\mathbb{Z}$ kann man auch Restklassen im Ring $K[X]$ definieren und betrachten. Diese Restklassen können dann zusammen mit geeigneten Operationen $+$ und $\cdot$ zu Körpern werden. Bei $\mathbb{Z}_n$ war das dann der Fall, wenn n eine Primzahl war.

5.5.6 Polynome und Polynomringe - Restklassen

Beispiel zu (3) von Seite 32 : Wir betrachten den Körper $(\mathbb{Z}_2, +, \cdot)$ und das Polynom $m(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[X]$. Betrachte dann die Restklasse $\mathbb{Z}_2[X]_{m(x)}$ und die hierzu passende Struktur $(\mathbb{Z}_2[X]_{m(x)}, +, \cdot)$, von der sich herausstellt, dass diese einen Körper darstellt. Dieser Körper wird auch mit $GF[2^8]$ bezeichnet.

Charakteristika dieses Körpers :

1. Wieviele Elemente besitzt $GF[2^8]$? $GF[2^8]$ beinhaltet alle Polynome vom Grad ≤ 7, deren Koeffizienten jeweils nur die Werte 0 oder 1 annehmen können. Demzufolge hat $GF[2^8]$ genau $2^8 = 256$ Elemente.
2. Wie wird addiert ? Antwort : So wie wir es auf der Seite 29 schon festgestellt hatten - Beispiel :
$$(x^5 + x^3 + 1) + (x^6 + x^5 + x^2 + x + 1) = x^6 + x^3 + x^2 + x.$$
3. Wie wird multipliziert ? Antwort : Genauso, wie wir das bei den Restklassen $\mathbb{Z}_n$ auch gemacht haben - in 2 Schritten : **1. Schritt :** Wie gewohnt multiplizieren, **2. Schritt :** Dividieren, um den Rest zu ermitteln, der das Ergebnis der Multiplikation darstellt - Beispiel : Zu berechnen ist $(x^3 + 1) \cdot (x^6 + x^2 + 1)$
   1. $(x^3 + 1) \cdot (x^6 + x^2 + 1) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$
   2. $(x^9 + x^6 + x^5 + x^3 + x^2 + 1) : (x^8 + x^4 + x^3 + x + 1) = x$ Rest $x^6 + x^4 + x^3 + x + 1$, was das Ergebnis der Multiplikation darstellt.

5.5.7 Polynome und Polynomringe - Ideale

Zum Abschluss des Teilkapitels soll noch auf den wesentlichen Begriff des Ideals im Ring $K[X]$ eingegangen werden (Hinweis : Der Begriff des Ideals kann für jeden Ring gebildet werden - wir tun dies nur für den Spezialfall $K[X]$).

Definition : Eine Teilmenge $I \subseteq K[X]$ heisst **Ideal** von $K[X]$, wenn folgende Eigenschaften erfüllt sind

1. $I \neq \emptyset$
2. (Additivität) Wenn $p, q \in I$, so sind auch $p - q, p + q \in I$.
3. (magnetische Anziehungskraft) Wenn $q \in I$ und $p \in K[X]$, so ist auch $p \cdot q \in I$.

Beispiele für Ideale : Folgende Mengen sind Ideale von $K[X]$

1. $I = \{0\}$
2. $I = K[X]$
3. $I = \{x \cdot f | f \in K[X]\}$
4. $I = \{p_1 \cdot q_1 + p_2 \cdot q_2 + ... + p_n \cdot q_n | p_1, p_2, .., p_n \in K[X]\}$ mit irgendwelchen Elementen $q_1, q_2, .., q_n \in K[X]$ - dieses Ideal wird auch das von $q_1, q_2, .., q_n$ erzeugte Ideal von $K[X]$ genannt und mit $I(q_1, q_2, .., q_n)$ bezeichnet.
5. $I = \{p \cdot q | p \in K[X]\}$ mit $q \in K[X]$, was einen Spezialfall von **(4)** (n=1) darstellt. Ideale dieses Type werden **Hauptideale** genannt. Das Polynom q wird der **Erzeuger des Hauptideales** genannt.

Es gilt nun der folgende wichtige **Satz :** Jedes von einer endlichen Menge von Polynomen $q_1, q_2, .., q_n \in K[X]$ erzeugte Ideal ist ein Hauptideal. Der Erzeuger des Hauptideals ist der **ggT** der Polynome $q_1, q_2, .., q_n$.

5.5. Polynome und Polynomringe

Zusätzliche Informationen zu Polynomen :

1. Das Analogon zu Primzahlen in $\mathbb{Z}$ sind bei den Polynomen die sogenannten irreduziblen Polynome. Ein Polynom $p(x) \in K[X]$ heisst irreduzibel, wenn es ausser durch 1 und sich selbst von keinem anderen normierten Polynom in $K[X]$ geteilt wird.

2. Der ggT zweier Polynome kann analog der ggT-Darstellung bei Zahlen als Vielfachsumme der beiden Polynome dargestellt werden. Die Vielfachen sind in diesem Fall Elemente von $K[X]$.

3. Zur numerischen Berechnung der Funktionswerte von Polynomfunktionen gibt es bzgl. Rundungsabweichungen numerisch gutartige Verfahren - hier ist das Horner'sche Schema zu nennen (wenn überhaupt, ist das ein Thema des Modules Mathematik 2 - Numerik)

4. Polynome, Polynomringe und deren Ideale spielen auch eine Rolle bei der Diagonalisierung von Matrizen - das ist Thema im Kapitel 13 und wird dort wieder aufgegriffen.

5.5. Polynome und Polynomringe - Anwendungsgebiete

Polynome, Polynomdivisionen sowie ggT-Bestimmung von Polynomen sind elementar und wesentlich in zahlreichen kryptographischen Themengebieten

- Stromchiffren - hier wird aus den Eigenschaften von Polynomen auf Eigenschaften von Schlüsselgeneratoren (Periodizität) geschlossen

- Block-Chiffren - AES (Advanced Encryption Standard) : Hier wird mit Restklassen von Polynomen ein Körper definiert, der genau 256 Elemente hat und der der von uns betrachtete Körper $GF[2^8]$ ist - $2^8 = 256$, was genau der möglichen Anzahl verschiedener Bytes gleicht. Ausschließlich in diesem Körper operieren die Teilfunktionen des AES-Verschlüsselungsalgorithmus.

  Das AES-Verschlüsselungsverfahren ist das aktuell am häufigsten eingesetzte symmetrische kryptographische Verfahren zur Verschlüsselung von Kommunikation in den vielfältigen Datennetzen der heutigen Zeit zur Sicherstellung von Vertraulichkeit der gesendeten / empfangenen Informationen.

5.6 Was ist mitzunehmen ?

Mitzunehmen sind

- Den ggT zweier ganzer Zahlen mittels des euklidischen Algorithmus bestimmen/berechnen können
- Den ggT als Vielfachsumme der zwei ihn bestimmenden ganzen Zahlen darstellen können - auf zwei verschiedene Arten
- In einer vorgegebenen Restgruppe $\mathbb{Z}_n$ addieren/subtrahieren und multiplizieren/dividieren können (modulare Arithmetik)
- Algebraischen Strukturen **Gruppe** und **Körper** kennen und vorgegebene Strukturen als **Gruppe** oder **Körper** nachweisen können.
- Polynomadditionen /-subtraktionen /-multiplikationen /-divisionen in einem Polynomring $(K[X], +, \cdot)$ durchführen können
- Den ggT von Polynomen bestimmen können

5.7 Verwendete Literatur

Hartmann, Mathematik für Informatiker, Kapitel 4.2, 4.3, 5

Teschl, Mathematik für Informatiker, Kapitel 4

Beutelspacher, Lineare Algebra, Kapitel 9

Ergänzung für Interessierte Kryptographischer Verfahren :

Johannes Buchmann, Einführung in die Kryptographie - Kapitel 6 (AES-Algorithmus)

Beutelspacher, Kryptologie, Kapitel 1 (zu Cäsar-Chiffrierung) , 5.3 (zu RSA)

5.8 Üben und Verstehen - Übungsaufgaben

Zum Üben und Verstehen - Übungsblatt 5 -

Aufgaben 1 - 4, 5(*), 6(*)