WS 2010/11

Zentralübung zur Vorlesung Diskrete Strukturen

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2010WS/ds/uebung/

1. Dezember 2010

ZÜ VI

Übersicht:

1. Übungsbetrieb: Klausur am 11.12.10
   Anmeldung, Ablauf, Code

2. Thema: Quiz: Rechnen modulo n

3. Vorbereitung auf TA's Blatt 7:

   Abstrakte Ringe (VA1 + VA2)
   Euklidscher Algorithmus (VA3)

1. Übungsbetrieb

1.1 Anmeldung

Die Anmeldung über TUMonline ist nur noch
in der laufenden Woche möglich.

Bei Nichtanmeldung: Bitte im Hörsaal bei der Aufsicht melden!

1.2 Ablauf

Es nicht erlaubt, Unterlagen zu benutzen,
außer
einem persönlich handbeschriebenen DIN A4 Blatt (beidseitig)

Fragen während der Klausur sind erlaubt,
aber
Anworten werden, falls notwendig,
nur als Hörsaalansage gegeben.

1.3 Code

Auf dem Deckblatt der Klausurangabe finden Sie 8 Kästchen in die Sie einen Code mit 8 Ziffern schreiben können

Mit diesem Code können Ihre Ergebnisse schnell und Datenschutzrechtlich sicher veröffentlicht werden.

Bitte notieren Sie Ihren Code als Gedächtnisstütze!!!

2. Thema:

2.1 Quiz: Rechnen modulo n

Wir rechnen in Z_8 in 3 Minuten, schriftlich!

Wieviel ist:

$$\begin{array}{|llll|}
1 \cdot 1 = ___| & 2 \cdot 2 = ___| & 3 \cdot 3 = ___| & (-3) = ___ \\
1 - 2 = ___| & 2 \cdot (-5) = ___| & 3^{-1} = ___| & (-3) \cdot 3 = ___ \\
(1-2)^3 = ___| & 2 \cdot (1-5) = ___| & 5^{-1} = ___| & (-7) \cdot 7 = ___ \\
\hline
\end{array}$$

?

Zusatzfrage: Besitzt 6 ein Inverses 6^{-1} ?

Lösung:

Wir rechnen in Z_8.

$$\begin{array}{llll} 1 \cdot 1 = \underline{1}\,| & 2 \cdot 2 = \underline{4}\,| & 3 \cdot 3 = \underline{1}\,| & (-3) = \underline{5} \\ 1 - 2 = \underline{7}\,| & 2 \cdot (-5) = \underline{6}\,| & 3^{-1} = \underline{3}\,| & (-3) \cdot 3 = \underline{7} \\ (1-2)^3 = \underline{7}\,| & 2 \cdot (1-5) = \underline{0}\,| & 5^{-1} = \underline{5}\,| & (-7) \cdot 7 = \underline{7} \end{array} \Bigg|$$

!

Es gibt kein Inverses von 6, denn 6 ist ein Nullteiler.

3. Vorbereitung auf TA's Blatt 7

3.1 VA 1, Abstrakte Ringe, elementare Eigenschaften

1. Man zeige:
   In einem beliebigen Ring $\langle R, \oplus, \odot, 0, 1\rangle$ gelten die folgenden Gleichungen.

$$a \odot 0 \;=\; 0 \odot a \;=\; 0\,, \qquad\qquad a \odot b \;=\; (-a) \odot (-b)\,.$$

Bemerkung 1: Das Inverse eines Elements x bezüglich der Operation $\oplus$ wird mit $-x$ bezeichnet.

Bemerkung 2: Da a und b beliebige Elemente aus R sind, schreiben wir die Gleichungen ohne Allquantoren.
Natürlich darf man auch $\forall a, b$ ergänzen.

Beweis:

1. Gleichung(en): $a \odot 0 \;=\; 0 \odot a \;=\; 0\,.$

- Es gilt

$$a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \oplus (a \odot 0)\,.$$

Daraus folgt mit additiver Kürzungsregel $a \odot 0 = 0.$

Da die Kommutativität der Multiplikation nicht vorausgesetzt wurde, müssen wir $0 \odot a = 0$ gesondert beweisen.

Dies folgert man aber analog wie vorhin.

2. Gleichung: $a \odot b = (-a) \odot (-b)$.

- Es gilt

$$0 = a \odot 0 = a \odot (b \oplus (-b)) = a \odot b \oplus a \odot (-b)\,.$$

Daraus folgt $-(a \odot b) = a \odot (-b)$.

Analog folgt $-(a \odot b) = (-a) \odot b$.

Damit erhalten wir

$$(-a) \odot (-b) = -(a \odot (-b)) = -(-(a \odot b)) = a \odot b\,.$$

2. Geben Sie zwei nichtkommutative Ringe an.

Lösung:

Man nehme die Ringe der $n \times n$-Matrizen für verschiedene $n \geq 2$.

Für die Matrixmultiplikation mit $n = 2$ gilt beispielsweise

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Was erhält man bei Rechnung modulo 2?

3.2 VA 2, Abstrakte Ringe, weitere Eigenschaften

Beweisen Sie:

1. Es gibt bis auf Isomorphie genau einen Ring $R = \langle S, \oplus, \odot, 0, 1\rangle$ mit drei Elementen, d. h. $S = \{0, 1, a\}$.

   Insbesondere also muss R isomorph sein zum Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1\rangle$.

Erinnerung: Sei $R = \langle S, \oplus, \odot, 0, 1\rangle$ ein Ring. Nach Vorlesung ist $\langle S, \oplus, 0\rangle$ eine abelsche Gruppe mit neutralem Element 0 und $\langle S, \odot, 1\rangle$ ist ein Monoid mit neutralem Element 1. Außerdem gelten die beidseitigen Distributivgesetze. Für Ringe mit mehr als einem Element gilt stets $1 \neq 0$. Der Ring ist kommutativ, falls die Multiplikation kommutativ ist.

Beweis:

Eine Gruppe mit 3 Elementen ist notwendigerweise zyklisch,
denn die Ordnung eines Elements ungleich dem Neutralen kann,
nach dem Satz von Lagrange, nicht 2 sein,
weil dann 2 Teiler der Gruppenordnung 3 sein müsste.

Jedes Element ungleich dem neutralen Element erzeugt die Gruppe. Die Verknüpfungstafel für $\oplus$ lautet deshalb wie folgt.

$\oplus$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

Dass diese Verknüpfungstafel eine Gruppe definiert, ergibt sich aus der Isomorphie zu $\langle \mathbb{Z}_3, +_3 \rangle$.

Auch die Verknüpfungstafel für die Multiplikation ergibt sich zwingend wegen

$$a \odot a = (1 \oplus 1) \odot (1 \oplus 1) = 1 \oplus 1 \oplus 1 \oplus 1 = 1$$

wie folgt:

$\odot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Dass alle Ringaxiome erfüllt sind, zeigt man wiederum mithilfe der Isomorphie auf den Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$.

Es folgt, dass R ein Ring ist.

Die Eindeutigkeit von R ist eine Konsequenz der Herleitung, denn die Verknüpfungstafeln hatten sichzwingend ergeben.

2. Der Ring $R = \langle S, \oplus, \odot, 0, 1 \rangle$ mit drei Elementen ist ein Körper.

Beweis:

R ist genau dann ein Körper, wenn $\langle S\setminus\{0\}, \odot, 1\rangle$ eine kommutative Gruppe ist.

Zum Beweis genügt der Hinweis auf die Isomorphie mit $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1\rangle$, weil $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1\rangle$ bekanntlich ein Körper ist, wenn n eine Primzahl ist.

Wir geben aber auch einen direkten Beweis an, wie folgt.

Direkter Beweis:

Wir streichen aus der Verknüpfungstafel die Zeile bzw. Spalte der Multiplikation mit 0 und erhalten.

$\odot$	1	a
1	1	a
a	a	1

Offenbar definiert die Multiplikation eine Gruppe.
Sie ist isomorph zu $\langle \mathbb{Z}_2, +_2 \rangle$.

Definition:
Es heiße $y \in S \setminus \{0\}$ *co*-Nullteiler von $x \in S \setminus \{0\}$, falls $x \odot y = 0$.

Beispiel: In $\mathbb{Z}_8$ sind $2, 4, 6$ *co*-Nullteiler von 4.

3. Sei t_x die Anzahl der *co*-Nullteiler eines Ringelementes $x \in S \setminus \{0\}$ eines endlichen, kommutativen Ringes $\langle S, \oplus, \odot, 0, 1 \rangle$.

   Dann ist $t_x + 1$ ein Teiler der Anzahl $n = |S|$ aller Ringelemente.

Beweis:

Sei $N_x = \{y \in S \setminus \{0\} \; ; \; x \odot y = 0\}$.
Wir zeigen, dass $N_x \cup \{0\}$ eine additive Untergruppe von $\langle S, \oplus \rangle$ bildet.

- Es gilt offensichtlich $0 \in N_x \cup \{0\}$.
- Abgeschlossenheit: Seien $y, z \in N_x \cup \{0\}$.
  Dann gilt $x \odot (y \oplus z) = x \odot y \; \oplus \; x \odot z = 0$, d. h.
  $y \oplus z \in N_x \cup \{0\}$.
- Inverse sind enthalten: Sei $y \in N_x \cup \{0\}$.
  Dann gilt $x \odot (-y) = -x \odot y = 0$, d. h. $-y \in N_x \cup \{0\}$.

Da $N_x \cup \{0\}$ eine additive Untergruppe von $\langle S, \oplus \rangle$ ist,
gilt nach dem Satz von Lagrange,
dass $t_x + 1 = |N_x \cup \{0\}|$ ein Teiler von $|S|$ ist,
w.z.b.w.

Bemerkung:

Die Konsequenz der Aussage in dieser Teilaufgabe ist, dass
jeder endliche kommutative Ring,
dessen Anzahl von Elementen eine Primzahl ist,
notwendigerweise auch ein Körper ist!

3.3 VA 3, Euklidscher Algorithmus

In gewissen kommutativen Ringen $R = \langle S, +, \cdot, 0, 1 \rangle$ stellt sich der erweiterte Euklidsche Algorithmus zur Berechnung des größten gemeinsamen Teilers $ggT(a, b)$ zweier Elemente $a \in S$ und $b \in S$ dar als eine iterierte Transformation (Matrixmultiplikation) Q_i angewandt auf Δ_{i-1} wie folgt mit $r_0 = a$ und $r_1 = b$.

$$\Delta_0 = \begin{pmatrix} a \\ b \end{pmatrix},$$

$$\Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_i \Delta_{i-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix},$$

für alle $i := 1, 2, \ldots, n \in \mathbb{N}$.

Dabei werden die Quotienten q_i so gewählt (geschätzt), dass die Δ_i mit wachsendem i in einem gewissen Sinn stets echt kleiner werden.

Eine Berechnung wird beendet, wenn die Folge der Δ_i maximale Länge besitzt, d. h. wenn kein Quotient existiert, der die Bildung eines noch kleineren Restes erlaubt.

Zur Bemessung der Größe von Elementen eines Ringes dient beispielweise im Ring der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ die Betragsfunktion. In Polynomringen wird der Grad eines Polynoms verwendet.

Wir betrachten im Folgenden den Ring $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ der ganzen Zahlen.

1. Zeigen Sie für alle entsprechenden i

$$ggT(a, b) = ggT(r_i, r_{i+1}) \,.$$

Beweis:

Gemeinsame Teiler zweier Ringelemente r_{i-1}, r_i übertragen sich auf deren Linearkombination $sr_{i-1} + tr_i$ wie folgt:

Falls x Teiler von r_{i-1} und von r_i, i. Z. $x|r_{i-1} \wedge x|r_i$,
dann gilt für gewisse Faktoren $h, k \in R$

$$sr_{i-1} + tr_i = sxh + txk = (sh + tk)x\,,$$

mithin $x|(sr_{i-1} + tr_i)$.

Die Matrixmultiplikation liefert eine Linearkombination wie folgt.

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i-1} - q_i r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}\,.$$

Da die Matrix invertierbar ist mit

$$Q^{-1} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix},$$

haben die Komponentenpaare der Δ_i für alle i die gleichen Teiler.
w.z.b.w.

1. Berechnen Sie mit dem Euklidschen Algorithmus den $ggT(10800, 122)$.

Berechnung:

Wir rechnen im Ring der ganzen Zahlen.

Im Euklidschen Algorithmus für den Ring ganzer Zahlen zur Berechnung des $ggT(a, b)$ werden die Quotienten q_i durch ganzzahlige Division bestimmt.

$$q_i = r_{i-1} \operatorname{div} r_i \, .$$

Abweichend davon könnte man aber auch grob schätzen.

Für die Linearkombination $r_{i+1} = r_{i-1} - q_i r_i$ folgt dann

$$r_{i+1} = r_{i-1} \bmod r_i \, .$$

Die Berechnung wird beendet, wenn $r_{n+1} = 0$ eintritt für irgendein $n \in \mathbb{N}$.

Berechnung (Fortsetzung):

$$
\begin{aligned}
r_0 &= 10800\,, \\
r_1 &= 122\,, \\
r_2 &= 10800 \bmod 122 = 64\,, \\
r_3 &= 122 \bmod 64 = 58\,, \\
r_4 &= 64 \bmod 58 = 6\,, \\
r_5 &= 58 \bmod 6 = 4\,, \\
r_6 &= 6 \bmod 4 = 2\,, \\
r_7 &= 4 \bmod 2 = 0\,.
\end{aligned}
$$

Ergebnis: $ggT(10800, 122) = r_6 = 2.$