SS 2011

Zentralübung
Diskrete Strukturen
(zur Vorlesung Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2011SS/ds/uebung/

6. September 2011

ZÜ III

Übersicht:

1. Übungsbetrieb: Neuerungen

2. Thema: Quiz: Rechnen modulo n

3. Vorbereitung auf TA's Blatt 4:

   Abstrakte Ringe (VA1)
   Euklidscher Algorithmus (VA2)
   Partialbrüche (VA3)
   Division in $\mathbb{Z}_5[x]$ (VA 4)
   Restklassenringe (VA 5)
   Fouriertransformation: Komplexe Zahlen (VA 6)
   Erweiterter Euklidscher Algorithmus (VA 7)

1. Übungsbetrieb: Neuerungen

Freier Arbeitsraum für DS Teilnehmer
jeden Freitag, 12.30 - 16 Uhr, Seminarraum 03.11.018.

In zwangloser Folge werden Tutoren anwesend sein, mit denen man Fragen und Probleme diskutieren kann.

2. Thema: Quiz: Rechnen modulo n

Wir rechnen in Z_8 in 3 Minuten, schriftlich!

Wieviel ist:

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

?

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

Lösung:

2.1 VA 1, Abstrakte Ringe

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 sich zwingend 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!

2.2 VA 2, Euklidscher Algorithmus

Mit $R = \mathbb{Z}_3[x]$ bezeichnen wir den Ring aller Polynome über einer Variablen x mit Koeffizienten aus dem Körper $\langle \mathbb{Z}_3, +_3, \cdot_3 \rangle$ der ganzen Zahlen modulo 3.
Seien $a(x), b(x) \in R$ gegeben durch

$$\begin{aligned} a(x) &= x^6 + 2x^4 + 2x^3 + x^2 + 1\,, \\ b(x) &= x^3 + x^2 + 1\,. \end{aligned}$$

1. Bestimmen Sie Polynome $r_2(x), r_3(x), q_1(x), q_2(x) \in R$ mit $\text{grad}(r_3(x)) < \text{grad}(r_2(x)) < \text{grad}(b(x))$, so dass die folgenden Gleichungen gelten.

$$\begin{aligned} r_2(x) &= a(x) - q_1(x) \cdot b(x)\,, \\ r_3(x) &= b(x) - q_2(x) \cdot r_2(x)\,. \end{aligned}$$

Lösung:

$q_1(x)$ erhält man durch Division von $a(x)$ durch $b(x)$ mit Rest $r_2(x)$.
Ausführung der Division:

$$
\begin{array}{rcl}
\overbrace{x^6+2x^4+2x^3+x^2+1}^{a(x)} & (\text{div}) & \overbrace{x^3+x^2+1}^{b(x)} = x^3 \\
-\ (x^6+x^5+x^3) & & \\
\hline
-x^5+2x^4+x^3+x^2+1 & & -x^2 \\
-\ (-x^5-x^4-x^2) & & \\
\hline
x^3+2x^2+1 & & +1 \\
-\ (x^3+x^2+1) & & q_1(x) = x^3+2x^2+1 \\
\hline
x^2 = r_2(x) & &
\end{array}
$$

Entsprechend erhält man $q_2(x)$
durch Division von $b(x)$ durch $r_2(x)$ mit Rest $r_3(x)$.

$$
\begin{aligned}
a(x) &= x^6 + 2x^4 + 2x^3 + x^2 + 1\,, \\
b(x) &= x^3 + x^2 + 1\,, \\
q_1(x) &= x^3 + 2x^2 + 1\,, \\
r_2(x) &= x^2\,, \\
q_2(x) &= x + 1\,, \\
r_3(x) &= 1\,.
\end{aligned}
$$

2. Bestimmen Sie ein Polynom $t(x) \in R$ möglichst hohen Grades, das ein gemeinsamer Teiler von $a(x)$ und $b(x)$ ist.

Lösung:

Gesucht ist also der größte gemeinsame Teiler von $a(x)$ und $b(x)$.

Das gesuchte Polynom ist $t(x) = r_3(x) = 1$.

Begründung:
$b(x)$ ist nicht durch $r_2(x)$ ohne Rest teilbar.
Aber $r_2(x)$ ist ohne Rest durch $r_3(x) = 1$ teilbar.

2.3 VA 3, Partialbruchzerlegung

Bestimmen Sie Polynome $a(x),\ b(x) \in \mathbb{Q}[x]$, so dass gilt

$$\frac{x^2+x}{(x^2+1)(x^2+2)} = \frac{a(x)}{x^2+1} + \frac{b(x)}{x^2+2}\,.$$

Lösung:

Bringt man die Brüche der rechten Gleichungsseite auf einen gemeinsamen Nenner, so erhält man durch Vergleich der Zähler die Gleichung

$$a(x)(x^2+2)+b(x)(x^2+1)=x^2+x\,.$$

Zur Lösung der Gleichung wählen wir den Ansatz

$$a(x)=a_1x+a_0 \quad \text{und} \quad b(x)=b_1x+b_0$$

und erhalten

$$\begin{aligned} & a(x)(x^2+2)+b(x)(x^2+1) \\ &= a_1x^3+a_0x^2+2a_1x+2a_0+b_1x^3+b_0x^2+b_1x+b_0 \\ &= (a_1+b_1)x^3+(a_0+b_0)x^2+(2a_1+b_1)x+(2a_0+b_0)\,. \end{aligned}$$

Durch Koeffizientenvergleich gewinnt man

$$\begin{aligned} a_1 + b_1 &= 0\,, \\ a_0 + b_0 &= 1\,, \\ 2a_1 + b_1 &= 1\,, \\ 2a_0 + b_0 &= 0\,. \end{aligned}$$

Die Lösung ist

$$a_1 = 1,\ a_0 = -1,\ b_1 = -1,\ b_0 = 2\,.$$

2.4 VA 4, Division in $\mathbb{Z}_5[x]$

Gegeben seien die Polynome $a(x) = x^4 + x^3 + 3$ und $b(x) = 3x^2 + 4$ aus dem Polynomring $\mathbb{Z}_5[x]$ über dem Körper $\mathbb{Z}_5$.

1. Wie viele Elemente enthält die Menge $R_{\text{grad}(b)}$ aller Polynome $r(x) \in \mathbb{Z}_5[x]$ mit $\text{grad}(r) < \text{grad}(b)$?
2. Bestimmen Sie Polynome $q(x), r(x) \in \mathbb{Z}_5[x]$, so dass gilt $a(x) = q(x) \cdot b(x) + r(x)$ mit $\text{grad}(r) < 2$.

Wie viele Elemente enthält die Menge $R_{\mathrm{grad}(b)}$ aller Polynome $r(x) \in \mathbb{Z}_5[x]$ mit $\mathrm{grad}(r) < \mathrm{grad}(b)$?

Lösung:

$|R_b| = 25$.

Polynome höchstens vom Grad 1 sind durch 2 Koeffizienten bestimmt. Für jeden Koeffizienten gibt es 5 Belegungsmöglichkeiten.

Bestimmen Sie Polynome $q(x), r(x) \in \mathbb{Z}_5[x]$, so dass gilt
$a(x) = q(x) \cdot b(x) + r(x)$ mit $\text{grad}(r) < 2$.

Lösung:

Division:

$$
\begin{array}{rrcll}
 & \overbrace{x^4 + x^3 + 3}^{a(x)} & (\text{div}) & \overbrace{3x^2 + 4}^{b(x)} & = \quad 2x^2 \\
- & (x^4 + 3x^2) & & & \\
\hline
 & x^3 + 2x^2 + 3 & & & +2x \\
- & (x^3 + 3x) & & & \\
\hline
 & 2x^2 + 2x + 3 & & & +4 \\
- & (2x^2 + 1) & & q(x) = & 2x^2 + 2x + 4 \\
\hline
 & 2x + 2 \quad = r(x) & & &
\end{array}
$$

2.5 VA 5, Restklassenringe

Wir betrachten den Ring $R = \mathbb{Z}_3[x]$.

Beachten und nutzen Sie im Folgenden die Isomorphie zwischen $\langle \mathbb{Z}_3[x]/(g), +, \cdot \rangle$ und $\langle \mathbb{Z}_3[x]_{\text{grad}(g)}, +_g, \cdot_g \rangle$, die für alle $g \in R$ durch die Abbildung $[f]_g \rightarrow Rem_g(f)$ gegeben ist.

Wir schreiben gelegentlich $p \in \mathbb{Z}_3[x]/(g)$ für $p \in \mathbb{Z}_3[x]_{\text{grad}(g)}$.

Sei $g(x) = x^2 + 2x + 1$.

1. Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(g)$.
2. Bestimmen Sie die Spalten der Additions- und Multiplikations-Verknüpfungstafeln zum Element $[x+2]_g \in \mathbb{Z}_3[x]/(g)$.
3. Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft

$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$

4. Ist der Restklassenring $\mathbb{Z}_3[x]/(g)$ ein Körper? Begründung!

Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(g)$.

Lösung:

Wir stellen die Elemente des Rings $\mathbb{Z}_3[x]/(x^2+2x+1)$ durch die Reste in $\mathbb{Z}_3[x]_2$ dar.
Es gilt

$$\mathbb{Z}_3[x]_2 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}\,.$$

Bestimmen Sie die Spalten der
Additions- und Multiplikations-Verknüpfungstafeln
zum Element $[x+2]_g \in \mathbb{Z}_3[x]/(g)$.

Lösung:

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$

Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft

$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$

Lösung:

Es gilt $p(x) = x^2 + x$ und $r(x) = 1$.

Ist der Restklassenring $\mathbb{Z}_3[x]/(g)$ ein Körper? Begründung!

Lösung:

Der Restklassenring $\mathbb{Z}_3[x]/(x^2+2x+1)$ ist kein Körper, weil er nicht nullteilerfrei ist. Es gilt

$$(x+1)\cdot(x+1) = x^2+2x+1 \equiv_g 0\,.$$

2.6 VA 6, Fouriertransformation: Komplexe Zahlen

Wir betrachten den Körper $\mathbb{C}$ der komplexen Zahlen.
Es sei $i \in \mathbb{C}$ mit $i^2 = -1$.

Zeigen Sie, dass für jedes $n \in \mathbb{N}$ die komplexe Zahl $e^{\frac{2\pi i}{n}}$
eine multiplikative Untergruppe W_n von $\mathbb{C}$ erzeugt,
die isomorph ist zu $\mathbb{Z}_n$.

Stellen Sie W_n in der Gaußschen Zahlenebene dar
und machen Sie sich klar, was in Ihrer Darstellung
die Multiplikation in W_n bedeutet.

Lösung:

$\mathbb{C}$ ist zusammen mit der Multiplikation keine Gruppe.

Gleichwohl gibt es Teilmengen von $\mathbb{C}$, die zusammen mit der Multiplikation eine Gruppe bilden. Wir sprechen in diesem Fall von multiplikativen Untergruppen von $\mathbb{C}$.

Eine maximale multiplikative Untergruppe in $\mathbb{C}$ ist $\mathbb{C} \setminus \{0\}$.

Trivialerweise bildet auch $\{0\}$ zusammen mit der Multiplikation eine Untergruppe.

Eine multiplikative Untergruppe von $\mathbb{C}$,
die irgendein von 0 verschiedenes Element enthält,
kann die 0 nicht enthalten.

Wegen $e^{\frac{2\pi i}{n}} \neq 0$ sind deshalb die

von $e^{\frac{2\pi i}{n}}$ erzeugten multiplikativen Untergruppen

gleichzeitig Untergruppen der multiplikativen Gruppe $\mathbb{C} \setminus \{0\}$.

Sei

$$W_n = \{(e^{\frac{2\pi i}{n}})^k \,;\, k \in \mathbb{Z}\} \subseteq \mathbb{C} \setminus \{0\}\,.$$

W_n ist die von $e^{\frac{2\pi i}{n}}$ erzeugte (zyklische) multiplikative Untergruppe von $\mathbb{C} \setminus \{0\}$.

Nun gilt

$$W_n = \{e^{\frac{2\pi i}{n}}, e^{\frac{2(2\pi i)}{n}}, \ldots, e^{\frac{k(2\pi i)}{n}}, \ldots, e^{\frac{n(2\pi i)}{n}} = 1\}\,.$$

Die Abbildung

$$\phi(e^{\frac{k(2\pi i)}{n}}) = k \bmod n$$

ist eine Isomorphie von W_n auf $\mathbb{Z}_n$ wegen

$$\begin{aligned}
\phi(x \cdot y) &= \phi(e^{\frac{k_x(2\pi i)}{n}} e^{\frac{k_y(2\pi i)}{n}}) \\
&= \phi(e^{\frac{(k_x+k_y)(2\pi i)}{n}}) \\
&= (k_x + k_y) \bmod n \\
&= \phi(x) +_n \phi(y)\,.
\end{aligned}$$

In der Gaußschen Zahlenebene liegen die Elemente von W_n auf einem Kreis von Punkten mit Abstand 1 zum Nullpunkt.

Die Multiplikation einer komplexen Zahl z mit $e^{\frac{k(2\pi i)}{n}}$

$$z \cdot e^{\frac{k(2\pi i)}{n}}$$

bedeutet dann eine Drehung des Vektors z um den Winkel $\frac{k(2\pi)}{n}$ im Gegenuhrzeigersinn (bei positivem k).

2.7 VA 7, Erweiterter Euklidscher Alg.

Bestimmen Sie mit dem erweiterten Euklidschen Algorithmus einen größten gemeinsamen Teiler der Polynome
$x^5 - 5x^4 + 4x^3 + 2x^2 - 12x + 10$ und $x^2 - 1$. Die Polynome werden im Ring $\mathbb{Q}[x]$ betrachtet.

Lösung:

Wir führen die Auswertung der Formeln von Hand aus mit Buchführung in einer Tabelle, zunächst ohne die Spalten für die Erweiterung des Euklidschen Algorithmus.

k	r_{k-1}	r_k	q_k
$k=1$	$(x^5-5x^4+4x^3+2x^2-12x+10)$	(x^2-1)	(x^3-5x^2+5x-3)
$k=2$	(x^2-1)	$(-7x+7)$	$(-\frac{1}{7}x-\frac{1}{7})$
$k=3$	$(-7x+7)$	0	

Einen größten gemeinsamen Teiler der Polynome lesen wir mit $r_2 = (-7x + 7)$ aus der Tabelle ab.
Durch Normierung erhalten wir den normierten ggT mit $x - 1$.

Die Erweiterung des euklidschen Algorithmus ist zwar für die Berechnung des ggT nicht notwendig, die Aufgabenstellung verlangt dies aber.

k	q_k	m_{k-1}	n_{k-1}	m_k	n_k
$k=1$	(x^3-5x^2+5x-3)	1	0	0	1
$k=2$	$(-\frac{1}{7}x-\frac{1}{7})$			1	$-(x^3-5x^2+5x-3)$

Wir erhalten mit $p := x^5 - 5x^4 + 4x^3 + 2x^2 - 12x + 10$ und $q := x^2 - 1$

$$ggT(p,q) = -7x + 7 = 1 \cdot p - (x^3 - 5x^2 + 5x - 3) \cdot q\,.$$