Algebra für Informationssystemtechniker

Prof. Dr. Ulrike Baumann

Fachrichtung Mathematik

Institut für Algebra

www.math.tu-dresden.de/∼baumann

Ulrike.Baumann@tu-dresden.de

13.12.2017

5. Vorlesung

Restklassenringe (1)

- natürliche Zahlen
- Teiler und Primzahlen
- EUKLIDischer Algorithmus
  zur Berechnung von ggT(a, b)
- Erweiterter EUKLIDischer Algorithmus
- EULERsche φ-Funktion

Axiome von Peano

1. Zu jeder natürlichen Zahl n gibt es genau eine natürliche Zahl n^+, genannt der Nachfolger von n.

2. Aus $m^+ = n^+$ folgt $m = n$, d.h. jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.

3. Es gibt eine natürliche Zahl 0, die nicht Nachfolger einer natürlichen Zahl ist (d.h. es gibt keine natürliche Zahl n mit $n^+ = 0$).

4. (Induktionsaxiom)

   Ist S eine Menge von natürlichen Zahlen, die die Zahl 0 enthält und für jedes $n \in S$ auch $n^+ \in S$ erfüllt, dann ist S die Menge aller natürlichen Zahlen.

Standardmodell der natürlichen Zahlen

- Sei S eine Menge.
  $S^+ := S \cup \{S\}$ nennt man Nachfolger von S.

- $\mathbb{N} := \{0, 1, 2, 3, \dots\}$, wobei

  $0 := \emptyset$
  $1 := \emptyset^+ = \{\emptyset\}$
  $2 := \emptyset^{++} = \{\emptyset, \{\emptyset\}\}$
  $\vdots$

- Jede nichtleere Menge natürlicher Zahlen hat ein kleinstes Element (d.h. die natürlichen Zahlen sind wohlgeordnet).

Teiler und Primzahlen

- Seien $a, b \in \mathbb{N}$.
  a heißt Teiler von b in $\mathbb{N}$, wenn es ein $k \in \mathbb{N}$ mit $a \cdot k = b$ gibt.
- Eine natürliche Zahl p heißt Primzahl, wenn sie größer als 1 ist und nur durch 1 und sich selbst teilbar ist.
- Jede natürliche Zahl $n > 1$ ist durch eine Primzahl teilbar.
- Es gibt unendlich viele Primzahlen.
- Teilt eine Primzahl ein Produkt natürlicher Zahlen,
  dann teilt sie einen der Faktoren.

Fundamentalsatz der Arithmetik

- Jede natürliche Zahl $n > 1$ kann auf genau eine Weise als ein Produkt

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

geschrieben werden, wobei k eine natürliche Zahl ist, $p_1 < p_2 < \cdots < p_k$ Primzahlen sind und $\alpha_1, \alpha_2, \ldots, \alpha_k$ positive natürliche Zahlen sind.

Diese Darstellung heißt die kanonische Primfaktorenzerlegung von n.

- Die Anzahl der Teiler einer natürlichen Zahl $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ ist $\prod_{i=1}^{k} (\alpha_i + 1)$.

- Je zwei natürliche Zahlen a, b (mit $(a, b) \neq (0, 0)$) besitzen einen größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ und ein kleinstes gemeinsames Vielfaches $\mathrm{kgV}(a, b)$.
Gilt $\mathrm{ggT}(a, b) = 1$, dann nennt man a, b teilerfremd.

Euklidischer Algorithmus

- **Euklidischer Algorithmus** zur Berechnung von $\mathrm{ggT}(a, b)$ mit $a, b \in \mathbb{N} \setminus \{0\}$:

$$\begin{array}{rcrcll}
a & = & q_1 b & + & r_1 & \text{mit} \quad 0 \leq r_1 < b \\
b & = & q_2 r_1 & + & r_2 & \text{mit} \quad 0 \leq r_2 < r_1 \\
r_1 & = & q_3 r_2 & + & r_3 & \text{mit} \quad 0 \leq r_3 < r_2 \\
 & \vdots & & & & \\
r_{n-2} & = & q_n r_{n-1} & + & r_n & \text{mit} \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} & = & q_{n+1} r_n & & &
\end{array}$$

$$\Rightarrow \quad \mathrm{ggT}(a, b) = r_n \quad (\text{denn } r_n \mid a,\ r_n \mid b,\ t \mid a \wedge t \mid b \Rightarrow t \mid r_n)$$

- Zwei natürliche Zahlen a und b sind genau dann teilerfremd, wenn es ganze Zahlen α und β mit

$$\alpha \cdot a + \beta \cdot b = 1$$

gibt. Die Zahlen α und β können mit Hilfe des erweiteren Euklidischen Algorithmus berechnet werden.

Erweiterter EUKLIDischer Algorithmus

Erweiterer Euklidischer Algorithmus zur Darstellung von $\mathrm{ggT}(a, b)$ als Linearkombination $\alpha \cdot a + \beta \cdot b$:

	a	b				
a	1	0	$\mid$	$\cdot 1$		
b	0	1	$\mid$	$\cdot(-q_1)$	$\mid$	$\cdot 1$
r_1	1	$-q_1$			$\mid$	$\cdot(-q_2)$
r_2	$-q_2$	$1 + q_1 q_2$				
$\vdots$	$\vdots$	$\vdots$				
r_n	α	β				

$$\Rightarrow \quad \mathrm{ggT}(a, b) = \alpha \cdot a + \beta \cdot b$$

EULERsche φ-Funktion

- Sei $n \in \mathbb{N} \setminus \{0\}$. Die Anzahl der zu n teilerfremden Zahlen in $\{0, 1, \ldots, n-1\}$ wird mit $\varphi(n)$ bezeichnet. Man nennt die Funktion $n \mapsto \varphi(n)$ die EULERsche φ-Funktion.

- Hat die natürliche Zahl n die Darstellung $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, dann gilt:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$