Vorlesung “Mathematische Strukturen”

Sommersemester 2015

Prof. Barbara König
Übungsleitung: Dennis Nolte

Zahlen

Division mit Rest

Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen mit $a \neq 0$. Dann gibt es eindeutig bestimmte Zahlen $z, r \in \mathbb{Z}$ mit $0 \leq r < |a|$ und

$$z \cdot a + r = b$$

- z heißt Ergebnis der ganzzahligen Division von b durch a und man schreibt $z = b \operatorname{div} a$.
- r heißt Rest der ganzzahligen Division von b durch a und man schreibt $r = b \bmod a$.

Dabei ist $|a|$ der Absolutwert von a, beispielsweise ist $|-7| = 7$.
Im Folgenden wird a aber immer eine positive ganze Zahl sein.

Zahlen

Konkret (z.B. bei Verwendung eines Taschenrechners) lassen sich ($b \operatorname{div} a$) und ($b \bmod a$) folgendermaßen berechnen (für den Fall, dass $a > 0$):

$$b \operatorname{div} a = \left\lfloor \frac{b}{a} \right\rfloor \qquad b \bmod a = b - a \cdot \left\lfloor \frac{b}{a} \right\rfloor$$

Dabei steht $\lfloor q \rfloor$ mit $q \in \mathbb{R}$ für die Abrundung von q nach unten. D.h., $\lfloor q \rfloor$ ist die größte ganze Zahl, die kleiner gleich q ist.

Beispiele: $\lfloor 3 \rfloor = 3$, $\lfloor 5,17 \rfloor = 5$, $\lfloor \pi \rfloor = 3$, $\lfloor -1 \rfloor = -1$, $\lfloor -0,7 \rfloor = -1$

Zahlen

Ein Spezialfall der Division mit Rest ist die Teilbarkeit:

Teilbarkeit

Seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen. Man sagt, a teilt b, wenn es ein $z \in \mathbb{Z}$ gibt mit $a \cdot z = b$.
Wir schreiben auch $a \mid b$ und nennen a Teiler von b.

Bemerkung: Hier wird auch $a = 0$ erlaubt.

Die Relation $\mid$ (Teilbarkeit) ist eine partielle Ordnung, wenn man sie auf die natürlichen Zahlen einschränkt.

Zahlen

Gelten folgende Beziehungen?

$2 \mid 18$	(Ja, $z = 9$)
$-7 \mid 14$	(Ja, $z = -2$)
$3 \mid 10$	(Nein)
$0 \mid 0$	(Ja, z beliebig)
$0 \mid 7$	(Nein)
$7 \mid 0$	(Ja, $z = 0$)

Zahlen

Primzahl

Eine Zahl $p \in \mathbb{N}_0$ heißt Primzahl, wenn folgendes gilt:

- $p \neq 0$ und $p \neq 1$
- die einzigen Teiler von p in den natürlichen Zahlen sind 1 und p selbst.

Primzahlen: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$

Es gibt unendlich viele Primzahlen.

Zahlen

Eindeutigkeit der Primfaktorzerlegung

Sei $n \in \mathbb{N}_0$ mit $n \neq 0$ eine natürliche Zahl. Ein Produkt $p_1 \cdot \cdots \cdot p_m = n$ von Primzahlen heißt Primfaktorzerlegung von n.

Jede Zahl $n \neq 0$ besitzt eine solche Primfaktorzerlegung.
Wenn man zudem verlangt, dass die Primfaktoren in aufsteigender Reihenfolge angeordnet sind ($p_i \leq p_j$ für $i < j$), so ist die Primfaktorzerlegung einer Zahl eindeutig.

Bemerkungen:

- Die Primfaktorzerlegung von 1 ist das leere Produkt.
- Wenn wir auch die 1 als Primzahl einführen würden, so würden wir die die Eindeutigkeit der Primfaktorzerlegung verlieren. ($7 = 1 \cdot 7 = 1 \cdot 1 \cdot 7 = \ldots$).

Zahlen

Größter gemeinsamer Teiler

Seien $a, b \in \mathbb{N}_0$ (wobei mindestens eine der beiden Zahlen verschieden von 0 ist). Eine Zahl $d \in \mathbb{N}_0$ heißt größter gemeinsamer Teiler von a und b ($d = ggT(a, b)$), falls folgendes gilt:

- $d \mid a$ und $d \mid b$, d.h., d teilt sowohl a als auch b.
- für jede andere natürliche Zahl d', die a und b teilt, gilt: $d' \leq d$.

Zahlen

Kleinstes gemeinsames Vielfaches

Seien $a, b \in \mathbb{N}_0$. Eine Zahl $m \in \mathbb{N}_0$ mit $m \neq 0$ heißt kleinstes gemeinsames Vielfaches von a und b ($m = kgV(a,b)$), falls folgendes gilt:

- $a \mid m$ und $b \mid m$, d.h., sowohl a als auch b teilen m.
- für jede andere natürliche Zahl m', die von a und b geteilt wird, gilt: $m \leq m'$.

Zahlen

Wie bestimmt man den größten gemeinsamen Teiler?

Bestimmung von $d = ggT(a,b)$ – Methode 1

- Bestimme die Primfaktorzerlegungen von a und b
- Betrachte alle Primfaktoren p, die in beiden Zerlegungen vorkommen: angenommen p kommt in a k-mal und in b ℓ-mal vor. Dann kommt p in d genau $\min(k, \ell)$-mal vor.

Beispiel: $ggT(12, 30)$

- $12 = 2 \cdot 2 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$
- $ggT(12, 30) = 2 \cdot 3 = 6$.

Zahlen

Bestimmung von $d = ggT(a,b)$ – Methode 2 (Euklidischer Algorithmus)

- $ggT(0, a) = a$
- $ggT(a, b) = ggT(b, a)$
- $ggT(a, b) = ggT(a - b, b)$, falls $b \leq a$

Wende diese Regeln zur ggT-Berechnung so lange an, bis ein Ausdruck der Form $ggT(0, a)$ erreicht wird.

$$ggT(12, 30) = ggT(30, 12) = ggT(18, 12) = ggT(6, 12)$$
$$= ggT(12, 6) = ggT(6, 6) = ggT(0, 6) = 6$$

Zahlen

Bemerkung:

Die Methode 2 ist bei weitem effizienter, insbesondere, wenn man die dritte Regel durch

$$ggT(a, b) = ggT(a \bmod b, b) \quad \text{falls } b \leq a$$

ersetzt.

Zahlen

Der ggT und die ggT-Berechnung sind ein wichtiges Werkzeug für das Lösen bestimmter Gleichungen.

Lösen diophantischer Gleichungen

Gegeben seien $a, b, c \in \mathbb{N}_0$ (wobei mindestens eine der beiden Zahlen a, b verschieden von 0 ist). Wir suchen Lösungen $x, y \in \mathbb{Z}$ der Gleichung

$$a \cdot x + b \cdot y = c$$

Es gilt:

- Diese Gleichung hat genau dann eine Lösung, wenn $ggT(a, b) \mid c$.

Zahlen

Für Gleichungen der Form $a \cdot x + b \cdot y = ggT(a, b)$ kann man x, y dadurch bestimmen, dass man die ggT-Berechnung "rückwärts" nachvollzieht.

Beispiel: Lösen von $30 \cdot x + 12 \cdot y = 6$.

$$\begin{aligned} ggT(12, 30) &= ggT(12, 18) = ggT(6, 12) = ggT(6, 6) \\ &= ggT(6, 0) = ggT(0, 6) = 6 \end{aligned}$$

Dabei wurden die Zahlen folgendermaßen ermittelt:
$18 = 30 - 12$, $6 = 18 - 12$.

Damit kann man einsetzen:

$$6 = 18 - 12 = (30 - 12) - 12 = 30 \cdot 1 + 12 \cdot (-2)$$

Und damit hat man eine Lösung $x = 1$, $y = -2$.

Zahlen

Gleichungen der Form $a \cdot x + b \cdot y = c$ mit $c \neq ggT(a, b)$ (aber $ggT(a, b) \mid c$) kann man folgendermaßen lösen:

- Zunächst die Gleichung $a \cdot x' + b \cdot y' = ggT(a, b)$ lösen.
- Dann die Lösungen x', y' mit $c/ggT(a, b)$ multiplizieren, das ergibt die Lösungen x, y.

Beispiel: Lösen von $30 \cdot x + 12 \cdot y = 24$
$\leadsto$ Lösen von $30 \cdot x' + 12 \cdot y' = 6$ ergibt $x' = 1$, $y' = -2$.
$\leadsto$ mit $24/6 = 4$ multiplizieren ergibt $x = 4$, $y = -8$.

Zahlen

Teilerfremdheit

Zwei Zahlen $a, b \in \mathbb{N}_0$ heißen teilerfremd, falls $ggT(a, b) = 1$.

Eulersche φ-Funktion

Die Eulersche φ-Funktion $\varphi\colon \mathbb{N}_0 \to \mathbb{N}_0$ ist folgendermaßen definiert:

- $\varphi(n)$ mit $n \in \mathbb{N}_0$ ist die Anzahl der Zahlen zwischen 1 und n, die zu n teilerfremd sind.

$$\varphi(n) = |\{m \in \mathbb{N}_0 \mid 1 \leq m \leq n \text{ und } ggT(m, n) = 1\}|$$

Zahlen

Beispiele (Eulersche φ-Funktion):

n	$\varphi(n)$	n	$\varphi(n)$
0	0	7	6
1	1	8	4
2	1	9	6
3	2	10	4
4	2	11	10
5	4	12	4
6	2	13	12

Für eine Primzahl p gilt $\varphi(p) = p - 1$.

Außerdem gilt:

- $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, falls m, n teilerfremd sind.
- $\varphi(p^k) = p^k - p^{k-1}$, falls p eine Primzahl ist.