§9 Teilbarkeit im Bereich der ganzen Zahlen

Wir beschäftigen uns in diesem Paragraphen mit den grundlegenden Begriffen aus der elementaren Zahlentheorie. Dazu gehören Teiler, Vielfaches, größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches. Zur Berechnung des größten gemeinsamen Teilers behandeln wir den euklidischen Algorithmus. Wesentliches Hilfsmittel dafür ist die Division mit Rest.

Auf der Menge $\mathbb{Z}$ der ganzen Zahlen gibt es zwei **Rechenoperationen** (Verknüpfungen), und zwar die **Addition** und die **Multiplikation**, die allerdings unterschiedliche Eigenschaften haben. In beiden Fällen gelten die Kommutativität, Assoziativität und Distributivität. Für die Addition gibt es ein Nullelement, nämlich die Zahl 0, und für die Multiplikation gibt es ein Einselement (die Zahl 1).

Zu jeder Zahl aus $\mathbb{Z}$ gibt es die negative Zahl, jedoch gibt es zu $z \in \mathbb{Z}$ i.a. kein Inverses bzgl. der Multiplikation, das wieder in $\mathbb{Z}$ liegt. Man sagt, daß die ganzen Zahlen einen **kommutativen Ring** bilden, im Gegensatz etwa zu den reellen Zahlen, die einen Körper bilden. Der Ring $\mathbb{Z}$ ist außerdem **nullteilerfrei** , d.h. es gilt

$$\forall\, a, b \in \mathbb{Z} : a \cdot b = 0 \iff (a = 0 \vee b = 0)$$

Wir stellen folgenden Unterschied bei den beiden Rechenoperationen $+$ und $\cdot$ fest:
Sind a und b beliebig vorgegebene ganze Zahlen, so hat von den beiden Gleichungen

$$(1)\quad a + x = b \qquad\qquad (2)\quad a \cdot x = b$$

die erste immer eine Lösung in $x_0 \in \mathbb{Z}$, nämlich $x_0 = b - a \in \mathbb{Z}$, die zweite dagegen i.a. keine Lösung in $\mathbb{Z}$, wie die folgenden Beispiele zeigen:

$2 \cdot x = 3$ ist nicht in $\mathbb{Z}$ lösbar, da links immer eine gerade und rechts eine ungerade Zahl steht. Oder: Betrachtet man dies als Gleichung in $\mathbb{Q}$, so wäre $x_0 = \frac{3}{2} \notin \mathbb{Z}$ die einzige Lösung.

$0 \cdot x = 1$ ist in $\mathbb{Z}$ nicht lösbar, da links 0 und rechts $1 \neq 0$ steht. Allgemeiner: Die Gleichung $0 \cdot x = b$ ist nur für $b = 0$ lösbar. In dem Falle hat sie dann aber jede ganze Zahl als Lösung.

$2 \cdot x = -8$ ist lösbar in $\mathbb{Z}$ mit $x_0 = -4 \in \mathbb{Z}$

Die Forderung, daß (2) immer lösbar sein soll, falls $a \neq 0$ ist,motiviert die Einführung der rationalen Zahlen, die dann einen **Körper** bilden. So weit werden wir nicht gehen, wir werden uns statt dessen mit den Fällen beschäftigen, in denen (2) lösbar ist. Dies führt auf den Teilbarkeitsbegriff.

(9.1) DEF: a und b seien ganze Zahlen. a heißt ein **Teiler** von b (in Zeichen $a \mid b$), wenn es ein $k \in \mathbb{Z}$ gibt mit der Eigenschaft $\boxed{a \cdot k = b}$. In dieser Situation sagt man auch, daß a die Zahl b **teilt** oder daß b ein (ganzzahliges) **Vielfaches** von a ist.

Beispiel: $2|4\ ,\ \ -3|9\ ,\ \ 2\not|3$ (teilt nicht) , $7|0\ ,\ \ 0|0\ ,\ \ 0\not|1$

Bei der Definition der Teilbarkeit wird die Division **nicht** benutzt.
Nur im Falle $a \neq 0$ bedeutet $a|\,b$, daß $\dfrac{b}{a}$ eine ganze Zahl ist.

(9.2) BEM: a) $a|\,b \iff \exists\, k \in \mathbb{Z} : a \cdot k = b \qquad a\not|\,b \iff \forall\, k \in \mathbb{Z} : a \cdot k \neq b$

b) Ist a ein Teiler von b und gilt $ak = b$, so ist auch k ein Teiler von b. k heißt ein zu a **komplementärer Teiler** von b. Er ist im Falle $a \neq 0$ eindeutig bestimmt:
$ak = b = ak' \implies a(k-k') = 0 \overset{a\neq 0}{\implies} k - k' = 0 \implies k = k'$.

c) $\forall\, a \in \mathbb{Z} :\ a|\,0 \quad (a \cdot 0 = 0)$

d) $\forall\, b \in \mathbb{Z} :\ 0|\,b \implies b = 0 \quad (b = 0 \cdot k = 0)$

e) $a|\,b \implies a|(-b)\ ,\ (-a)|\,b\ ,\ (-a)|(-b)$. Hieraus ergibt sich: $a|\,b \iff |a|\,||b|$.

Chr.Nelius:Mathematik für Informatiker I (WS 2000/01) *22.12.2000*

In dem folgenden Satz sind die wichtigsten Eigenschaften der Teilbarkeitsbeziehung zusammengefaßt, die sich einfach auf Grundlage der Definition beweisen lassen:

(9.3) SATZ: Für beliebige ganze Zahlen a, b, c, d gilt :

a) $1|a$ und $a|\,a$ (Reflexivität)

b) $a|\,b$ und $b \neq 0 \implies 1 \leq |a| \leq |b|$

c) $a|\,b$ und $b|\,a \implies |a| = |b|$

d) $a|b$ und $b|c \implies a|\,c$ (Transitivität)

e) $a|\,b$ und $c|\,d \implies ac\,|\,bd$

f) $a|\,b$ und $a|\,c \implies a|\,(xb + yc)\ \ \forall\, x, y \in \mathbb{Z}$.

(9.4) FOLG: a) Jede ganze Zahl $b \neq 0$ besitzt nur endlich viele Teiler.

b) 0 besitzt unendlich viele Teiler.

(9.5) LEMMA: Sei $n \in \mathbb{N}$. Gilt dann $mk = n$ mit $k, m \in \mathbb{N}$, so folgt $m \leq \lfloor\sqrt{n}\rfloor$ oder $k \leq \lfloor\sqrt{n}\rfloor$.