§ 3 Teilbarkeitslehre

In diesem Kapitel möchten wir wichtige Eigenschaften der natürlichen (bzw. ganzen-) Zahlen untersuchen.

Def. 3.1

Eine Zahl $b \in \mathbb{Z}$ (oder $\mathbb{N}$) teilt eine ganze Zahl $a \in \mathbb{Z}$, wenn ein $c \in \mathbb{Z}$ existiert mit $a = b \cdot c$.
Wir schreiben hierfür auch $b \mid a$ und sagt, dass b ein Teiler von a ist.
Ein $b \in \mathbb{Z}$ heißt gemeinsamer Teiler von $a_1, a_2 \in \mathbb{Z}$, falls c_1 & c_2 existieren mit $a_1 = c_1 \cdot b$ und $a_2 = c_2 \cdot b$.

Beispiel 3.2

Die Teiler von 12 sind $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

Lemma 3.3.

(i) $a \mid a \quad (a \in \mathbb{Z}, a \neq 0)$

(ii) $a \mid 0 \quad (a \in \mathbb{Z}, a \neq 0)$

(iii) $1 \mid a \quad (a \in \mathbb{Z})$

(iv) $b \mid a, \; c \mid b \Rightarrow c \mid a \quad (a, b, c \in \mathbb{Z}, \; b, c \neq 0)$

(v) $b \mid a \Rightarrow b \cdot c \mid a \cdot c \quad (a, b, c \in \mathbb{Z}, \; b, c \neq 0)$

(vi) $b \cdot c \mid a \cdot c \Rightarrow b \mid a \quad (a, b, c \in \mathbb{Z}, \; b, c \neq 0)$

(vii) $b_1 \mid a_1 \wedge b_2 \mid a_2 \Rightarrow b_1 \cdot b_2 \mid a_1 \cdot a_2 \; (a_i, b_i \in \mathbb{Z}, b_i \neq 0, i = 1,2)$

(viii) $b \mid a_1 \wedge b \mid a_2 \Rightarrow b \mid (c_1 \cdot a_1 + c_2 \cdot a_2) \; (a_i, c_i \in \mathbb{Z}, b \neq 0)$

(ix) $b \mid a \Rightarrow b \mid a \cdot c \; (a, b, c \in \mathbb{Z}, b \neq 0)$

(x) $b \mid a \wedge a \mid b \Rightarrow a = \pm \; (a, b \in \mathbb{Z}, a, b \neq 0)$

Beweis: 09.05.18

(i) $a = a \cdot 1 \Rightarrow a | a$

(ii) $0 = a \cdot 0 \Rightarrow a | 0$

(iii) $a = 1 \cdot a \Rightarrow 1 | a$

(iv) n.V. gilt: $c | b$ und $b | a \Rightarrow \exists m, n \in \mathbb{Z}: b = c \cdot m \;\&\; a = b \cdot n$

$\Rightarrow a = c \cdot m \cdot n = c \cdot (m \cdot n) \Rightarrow c | a$

(v) Aus $b | a$ folgt: $\exists m \in \mathbb{Z}$ mit $a = b \cdot m$.

Multiplizieren dieser Gleichung mit $c \in \mathbb{Z}^*$ erhält man

$a \cdot c = (b \cdot m) \cdot c \Rightarrow b \cdot c \,|\, a \cdot c$

(vi) $bc | ac \Rightarrow \exists m \in \mathbb{Z}^*$ mit $ac = (b \cdot c) \cdot m$

Bilden der Differenz liefert:

$0 = ac - b \cdot c \cdot m = (a - b \cdot m) \cdot c$.

Da $c \neq 0$ folgt aus der Nullteilerfreiheit in $\mathbb{Z}$,

dass $a - bm = 0 \Rightarrow a = b \cdot m \Rightarrow b | a$

(vii) n.V. $\exists m_1, m_2 \in \mathbb{Z}^*$ mit $a_1 = b_1 \cdot m_1 \;\&\; a_2 = b_2 \cdot m_2$

$\Rightarrow a_1 a_2 = (b_1 m_1)(b_2 m_2) = (b_1 b_2)(m_1 m_2)$

$\Rightarrow b_1 \cdot b_2 \,|\, a_1 a_2$

(viii) Teilt b zwei Zahlen a_1, a_2, so existiert $m_1, m_2 \in \mathbb{Z}^*$

mit $a_1 = b \cdot m_1 \;\&\; a_2 = b \cdot m_2$

Seien nun $c_1, c_2 \in \mathbb{Z}^*$ beliebig, dann ist

$c_1 \cdot a_1 + c_2 \cdot a_2 = c_1 \cdot (b \cdot m_1) + c_2 (b \cdot m_2)$

$= b(c_1 \cdot m_1 + c_2 \cdot m_2)$

$\Rightarrow b \,|\, (c_1 \cdot a_1 + c_2 \cdot a_2)$

(ix) Aus $b | a$ folgt: $\exists m \in \mathbb{Z}^*$ mit $a = b \cdot m$

Multiplizieren der Gleichung mit $c \in \mathbb{Z}^*$ liefert:

$a \cdot c = c \cdot b \cdot m = b \cdot (m \cdot c) \Rightarrow b \,|\, a \cdot c$

(x) Sind $a,b \in \mathbb{Z}^*$ mit $a | b$ & $b | a$ dann ex. $m,n \in \mathbb{Z}^*$ mit $a = b \cdot m$ und $b = a \cdot n$

$a = (an) \cdot m \iff a(1 - m \cdot n) = 0$

Da $a \neq 0$ folgt aus der Nullteilerfreiheit, dass $1 = m \cdot n \Rightarrow m = n = \pm 1$ Mit der nächsten Bemerkung folgt nun $a = \pm b$

Bemerkung 3.4

Ist $b \in \mathbb{N}^*$ ein Teiler von $a \in \mathbb{N}$ mit $a \neq b$, dann gilt $b < a$. Andernfalls wäre $b > a$, was $\underset{b|a}{a = bc} \geq b \cdot 1 = b > a$ impliziert.

$\ulcorner m | 1$ A: $m \neq 1 \Rightarrow m < 1$ also $m = 0$ ↯ zu $m \cdot n = 1 \lrcorner$

Definition 3.5

Seien $a,b \in \mathbb{Z}$ (nicht beide gleiche 0).

Der größte gemeinsame Teiler von a und b ist die größte ganze Zahl, die a und b teilt. Wir schreiben $ggT(a,b)$ für diese Zahl.

Ist $ggT(a,b) = 1$ so heißen a und b teilerfremd

Falls $a \neq 0$ so ist $ggT(a,0) := a$

Falls $a = b = 0$ ist $ggT(a,b)$ nicht definiert

Beispiel 3.6

$ggT(16, 12) = 4$

$ggT(120, 225) = 15 \quad \begin{pmatrix} 120 = 2^3 \cdot 3 \cdot 5 \\ 225 = 3^2 \cdot 5^2 \end{pmatrix}$

Für größere Zahlen ist der Euklidische Algorithmus eine effiziente Methode, um den ggT zu bestimmen.

Der Euklidische Algorithmus basiert auf der Division mit Rest.

Satz 3.7 (Division mit Rest)

Seien $a, b \in \mathbb{Z}$ mit $b > 0$. Dann existieren eindeutig bestimmte ganze Zahlen q, r mit

$a = b \cdot q + r$ und $0 \leq r < b$

Man nennt q den Quotienten & r den Rest (der bei der Division mit Rest von a durch b entsteht.

Wenn $r = 0$, so ist b ein Teiler von a

Notation:

Ist $q = \frac{a}{b} \in \mathbb{Q}$. Dann bezeichnet:

$\lfloor \frac{a}{b} \rfloor$ die größte ganze Zahl kleiner gleich $\frac{a}{b}$

$\lceil \frac{a}{b} \rceil$ die kleinste ganze Zahl größer gleich $\frac{a}{b}$

Beweis von 3.7.

Sei $q = \lfloor \frac{a}{b} \rfloor$. Dann ist $q \leq \frac{a}{b} < q+1$

Demnach ist:

$q \cdot b \leq \frac{a}{b} \cdot b = a < (q+1) \cdot b = q \cdot b + b$

Mit $r := a - q \cdot b$ folgt $0 \leq r < b$ und $a = q \cdot b + r$

Ist $r = 0$ so ist b ein Teiler von a.

Es bleibt die Eindeutigkeit dieser Darstellung zu zeigen.

Angenommen

$(*)$ $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ mit $0 \leq r_1, r_2 < b$

OE: $r_2 < r_1$ (Ist $r_1 = r_2$ so ist auch $q_1 = q_2$)

$\Rightarrow 0 < r_1 - r_2 < b$. Insbesondere ist b kein Teiler von $(r_2 - r_1)$

Mit $(*)$ folgt allerdings, dass $(q_1 - q_2) b = -(r_2 - r_1)$.

$\Rightarrow$ b ist ein Teiler von $(r_2 - r_1)$ ↯ $\square$

Satz 3.8 (Euklidischer Algorithmus) — Euklid von Alexandria ca. 3. Jhd v. Chr.

Seien $a_1, a_2 \in \mathbb{Z}$ mit $a_2 \neq 0$. Dann terminiert die sukzessive Division mit Rest

$$a_1 = q_1 \cdot a_2 + a_3$$
$$a_2 = q_2 \cdot a_3 + a_4$$
$$a_j = q_j \cdot a_{j+1} + a_{j+2}$$
$$\vdots$$
$$a_{n-2} = q_{n-2} \cdot a_{n-1} + a_n$$
$$a_{n-1} = q_{n-1} \cdot a_n + 0$$

mit Rest 0 und $ggT(a_1, a_n) = a_n$

Rückwärts einsetzen der Gleichungen:

$$a_n = a_{n-2} - q_{n-2} \cdot a_{n-1}$$
$$a_{n-1} = \dots$$
$$\vdots$$
$$a_3 = a_1 - q_1 \cdot a_2$$

liefert eine Darstellung

$ggT(a_1, a_2) = u \cdot a_1 + v \cdot a_2 \quad u, v \in \mathbb{Z}$

Die Bestimmung des ggT, sowie der obigen Darstellung, nennt man den erweiterten Euklidischen Algorithmus

Beispiel 3.9

Wir wollen den ggT von 544 und 391 bestimmen, sowie die Darstellung des ggT aus dem erw. Eukl. Algorithmus:

$a_1 = 544$, $a_2 = 391$

$$544 = 1 \cdot 391 + 153$$
$$391 = 2 \cdot 153 + 85$$
$$153 = 1 \cdot 85 + 68$$
$$85 = 1 \cdot 68 + 17$$
$$68 = 4 \cdot 17 + 0$$

$\Rightarrow ggT(544, 391) = 17$

$$\begin{aligned} 17 &= 85 - 1 \cdot 68 \\ &= 85 - 1 \cdot (153 - 1 \cdot 85) = -1 \cdot 153 + 2 \cdot 85 \\ &= -1 \cdot 153 + 2(391 - 2 \cdot 153) = 2 \cdot 391 - 5 \cdot 153 \\ &= 2 \cdot 391 - 5(544 - 1 \cdot 391) \\ &= -5 \cdot 544 + 7 \cdot 391 \end{aligned}$$

Beweis von 3.8:

Wegen Satz 3.7 ist $|a_{j+1}| < |a_j|$ für $j \geq 2$ somit muss bei endlichen vielen Schritten $a_{n+1} = 0$ sein.

Nun ist a_n ein Teiler von a_{n-1}, also ist (vgl. Lemma 3.3(viii)) a_n auch ein Teiler von $a_{n-2} = q_{n-2} \cdot a_{n-1} + a_n$.

Induktiv folgt nun, dass a_n ein Teiler von $a_n, \dots, a_1$ ist.

Insbesondere ist a_n also ein Teiler von a_1 und a_2.

Ist g ein Teiler von a_1 und a_2, dann ist g auch ein Teiler von $a_3 = a_1 - q \cdot a_2$. Induktiv folgt, dass g ein Teiler von $a_1, \dots, a_n$ ist.

Mit (3.3)(x) folgt also, dass a_n der größte gemeinsame Teiler von a_1 und a_2 ist

[Also jeder Teiler von a_1 und a_2 teilt a_n & a_n teilt a_1 und a_2 $\Rightarrow a_n = ggT(a_1, a_2)$] $\boxtimes$

Proposition 3.10

(a) $ggT(a,b) = ggT(b,a)$

(b) $\forall q \in \mathbb{Z}$ ist $ggT(a,b) = ggT(b, a - q \cdot b)$

(c) Ist $g = ggT(a,b)$, dann ist $ggT\left(\underbrace{\frac{a}{g}}_{\in \mathbb{Z}}, \underbrace{\frac{b}{g}}_{\in \mathbb{Z}}\right) = 1$

Beweis:

(a) klar!

(b) Ist genau das Argument im Beweis von 3.8 mit dem wir begründet haben, dass der Eukl. Algorithmus den ggT berechnet

(c) Sei $g := ggT(a,b)$, A: $e > 1$ ist ein gemeinsamer Teiler von $\frac{a}{g}$ und $\frac{b}{g}$ $\Rightarrow \exists x, y \in \mathbb{Z}$ mit:

$\frac{a}{g} = x \cdot e$ und $\frac{b}{g} = y \cdot e$

$\Rightarrow$ $g \cdot e$ ist ein Teiler von a und b.

Da $g = ggT(a,b)$ folgt $e = 1$ $\Rightarrow$ $ggT\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ $\boxed{\equiv}$

Vom additiven Standpunkt aus gesehen ist die „1" der Grundbaustein der natürlichen (bzw. ganzen) Zahlen. Jede natürliche Zahl kann durch aufaddieren der 1 gebildet werden.
Wir fragen uns, was die multiplikativen Grundbausteine der natürlichen Zahlen sind. Dies führt zum Begriff der Primzahl.

Definition 3.11
Eine natürliche Zahl $p \geq 2$ heißt Primzahl, wenn p keine nicht-trivialen Teiler hat, d.h. p hat nur 1 und p als Teiler.
Die Menge aller Primzahlen bezeichnen wir mit:
$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ ist Primzahl}\}$.

Lemma 3.12
Sei p eine Primzahl mit $p \mid a \cdot b$. Dann gilt $p \mid a$ oder $p \mid b$. [Bem. $6 \mid 8 \cdot 9$ aber $6 \nmid 8$ & $6 \nmid 9$]

Beweis:
A: $p \mid a \cdot b$ aber $p \nmid a$ z.Z $p \mid b$. Da p eine Primzahl ist, ist $ggT(p,a) = 1$ ($= p$ geht nicht, weil $p \nmid a$)
Mit dem Eukl. Algorithmus $\exists x, y \in \mathbb{Z}$ mit $1 = x \cdot p + y \cdot a$
Multiplizieren mit b liefert $b = x \cdot p \cdot b + y \cdot a \cdot b$.
Nach Voraussetzung ist p ein Teiler von $a \cdot b$, also
$c \cdot p = a \cdot b$ $\Rightarrow$ $b = x \cdot p \cdot b + y \cdot c \cdot p = p(x \cdot b + y \cdot c)$
$\Rightarrow$ p ist ein Teiler von b. $\boxed{\equiv}$