5. Teilbarkeit und Restklassen

5.1. Division mit Rest

Eine natürliche Zahl a lässt bei der Division durch eine natürliche Zahl $b \neq 0$ einen eindeutig bestimmten Rest r. Für diesen Rest gilt stets $0 \leq r < b$. Wir bezeichnen diesen Rest mit $a \bmod b$.

Bsp: $a = 7$, $b = 3$

$a \bmod b = 7 \bmod 3 = 1$

Denn $7 = 2 \cdot 3 + 1$.

Wie berechnet man $a \bmod b$?

(i) Falls $a < b$ ist, gilt $a \bmod b = a$.

(ii) Falls $a \geq b$ ist, gilt $a \bmod b = (a-b) \bmod b$.

Bsp: $7 \bmod 3 = (7-3) \bmod 3 = 4 \bmod 3$

$= (4-3) \bmod 3 = 1 \bmod 3 = 1$

Die Anzahl der benötigten Subtraktionen wird mit $a \operatorname{div} b$ bezeichnet.

Es gilt stets: $a = (a \operatorname{div} b) \cdot b + (a \bmod b)$

Bsp: $a = 12$, $b = 5$

$12 \bmod 5 = (12-5) \bmod 5 = (7-5) \bmod 5 = 2$

$12 \operatorname{div} 5 = 2$

Somit gilt: $12 = 2 \cdot 5 + 2$

5.2. Der größte gemeinsame Teiler

Ein $d \in \mathbb{N}$ heißt gemeinsamer Teiler von $a \in \mathbb{N}$ und $b \in \mathbb{N}$, wenn $d \mid a$ und $d \mid b$ gilt.

d ist größter gemeinsamer Teiler von a und b, wenn $d' \mid d$ für alle gemeinsamen Teiler von a und b gilt.

Bsp: $a = 12$, $b = 18$

$d = 2$ und $d' = 3$ sind gemeinsame Teiler von 12 und 18

3 kann nicht größter gemeinsamer Teiler sein, da 2 kein Teiler von 3 ist.

6 ist ein größter gemeinsamer Teiler von 12 und 18.

Merke: Der größte gemeinsame Teiler von $a \in \mathbb{N}$ und $b \in \mathbb{N}$ ist eindeutig bestimmt. Er wird mit $ggt(a,b)$ bezeichnet.

Wie berechnet man $ggt(a,b)$?

(i) Falls $b = 0$ ist, gilt $ggt(a,b) = a$.

(ii) Falls $b > 0$ ist, gilt $ggt(a,b) = ggt(b, a \bmod b)$

Bsp: $a = 12$, $b = 18$

$$ggt(12,18) = ggt(18, 12 \bmod 18) = ggt(18,12)$$
$$= ggt(12, 18 \bmod 12) = ggt(12,6)$$
$$= ggt(6, 12 \bmod 6) = ggt(6,0) = 6$$

Dieses Berechnungsverfahren heißt Euklidischer Algorithmus.

Neben dem Wert $ggt(a,b)$ erhält man damit auch $p \in \mathbb{Z}$ und $q \in \mathbb{Z}$ mit $ggt(a,b) = p \cdot a + q \cdot b$.

Man spricht dann auch vom Erweiterten Euklidischen Algorithmus.

Bsp: $a = 27$, $b = 17$

$ggt(27,17)$	$10 = 27 - 1 \cdot 17$	$1 = -7 \cdot 17 + 12(27 - 1 \cdot 17)$
$= ggt(17,10)$	$7 = 17 - 1 \cdot 10$	$1 = 5 \cdot 10 - 7 \cdot (17 - 1 \cdot 10)$
$= ggt(10,7)$	$3 = 10 - 1 \cdot 7$	$1 = -2 \cdot 7 + 5 \cdot (10 - 1 \cdot 7)$
$= ggt(7,3)$	$1 = 7 - 2 \cdot 3$	$1 = 1 \cdot 3 - 2(7 - 2 \cdot 3)$
$= ggt(3,1)$	$0 = 3 - 3 \cdot 1$	$1 = 1 \cdot 1 + 1 \cdot (3 - 3 \cdot 1)$
$= ggt(1,0) = 1$		$1 = 1 \cdot 1 + 1 \cdot 0$

Ergebnis: $ggt(27,17) = 1 = \underbrace{12}_{p} \cdot 27 - \underbrace{19}_{q} \cdot 17$

5.3. Primfaktorzerlegung

Ein $p \in \mathbb{N} \setminus \{0,1\}$ heißt Primzahl, wenn es kein $d \in \mathbb{N} \setminus \{1,p\}$ gibt mit $d \mid p$. Die ersten Glieder der Folge der Primzahlen lauten:

$2, 3, 5, 7, 11, 13, 17, \ldots$

Lemma: Sei p eine Primzahl, die das Produkt $a \cdot b$ von $a \in \mathbb{N}$ und $b \in \mathbb{N}$ teilt. Dann gilt $p \mid a$ oder $p \mid b$.

Beweis: Sei also p eine Primzahl mit $p \mid (a \cdot b)$.

1. Fall: $p \mid a$. Dann sind wir fertig.

2. Fall: p ist kein Teiler von a.

Dann muss, da p Primzahl ist, $\text{ggT}(p,a) = 1$ sein.

Aus dem EEA gewinnen wir $s \in \mathbb{Z}$ und $t \in \mathbb{Z}$ mit $1 = s \cdot p + t \cdot a$.

Damit erhalten wir:

$$\begin{aligned} b = b \cdot 1 &= b \cdot (s \cdot p + t \cdot a) \\ &= s \cdot p \cdot b + t \cdot (a \cdot b) \\ &= s \cdot p \cdot b + t \cdot (k \cdot p) \quad (\text{wegen } p \mid a \cdot b) \\ &= p \cdot (s \cdot b + t \cdot k) \end{aligned}$$

Also gilt $p \mid b$. ▨

Satz: Jede natürliche Zahl $n \geq 2$ lässt sich bis auf die Reihenfolge der Faktoren eindeutig als Produkt von Primzahlen darstellen.

[ohne Beweis]

Satz: Es gibt unendlich viele Primzahlen.

Beweis: Angenommen es gäbe nur endlich viele Primzahlen $p_1, p_2, p_3, \dots, p_n$. Betrachte die natürliche Zahl

$$k = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

k hat eine Zerlegung in Primfaktoren: $k = q_1 \cdot q_2 \cdot \dots \cdot q_e$

In dieser Zerlegung kann aber p_1 nicht vorkommen, da p_1 kein Teiler von k ist. Auch $p_2, p_3, \dots, p_n$ können nicht vorkommen. Dann ist keiner der Faktoren $q_1, q_2, \dots, q_e$ eine Primzahl – ein Widerspruch. ▨

5.4. Das Rechnen mit Restklassen

Zwei ganze Zahlen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ heißen kongruent modulo der natürlichen Zahl $n \in \mathbb{N}$, wenn es ein $k \in \mathbb{Z}$ gibt mit $n \cdot k = a - b$. Wir schreiben dann $a \equiv_n b$.

Bsp: a) $17 \equiv_5 7$

b) $-6 \equiv_{19} 32$

Rechenregeln

Für alle $a, b, c \in \mathbb{Z}$, alle $n \in \mathbb{N}$ und alle $m \in \mathbb{N} \setminus \{0\}$ gilt:

(i) $a \equiv_n b \Rightarrow (a+c) \equiv_n (b+c)$

(ii) $a \equiv_n b \Rightarrow (a \cdot c) \equiv_n (b \cdot c)$

(iii) $a \equiv_n b \Rightarrow a^m \equiv_n b^m$

Bsp: $a = 2$, $b = 7$, $n = 5$, $m = 3$

$2 \equiv_5 7 \Rightarrow 2^3 = 8 \equiv_5 343 = 7^3$

Satz: Für alle $n \in \mathbb{N}$ ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$.

[ohne Beweis]

Mit $\mathbb{Z}_n$ wird die Menge der Äquivalenzklassen, genannt Restklassen, von $\equiv_n$ bezeichnet.

Bsp: $n = 4$

$\mathbb{Z}_4 = \{ \{0, 4, -4, 8, -8, \dots\},$
$\{1, 5, -3, 9, -7, \dots\},$
$\{2, 6, -2, 10, -6, \dots\},$
$\{3, 7, -1, 11, -5, \dots\} \}$

Für Restklassen $\bar{a}, \bar{b} \in \mathbb{Z}_n$ definieren wir eine Addition und eine Multiplikation:

(i) $\bar{a} + \bar{b} = \overline{(a+b)}$

(ii) $\bar{a} \cdot \bar{b} = \overline{(a \cdot b)}$

Bsp: $n = 4$, $\bar{a} = \bar{2}$, $\bar{b} = \bar{3}$

$$\bar{2} + \bar{3} = \overline{(2+3)} = \bar{5} = \bar{1}$$

$$\bar{2} \cdot \bar{3} = \overline{(2 \cdot 3)} = \bar{6} = \bar{2}$$

Als Vertreter einer Restklasse $\bar{a} \in \mathbb{Z}_n$ wählt man üblicherweise die Zahl $b \in \bar{a}$ mit $0 \leq b < n$. Die Beschreibung der Addition und Multiplikation erfolgt durch Angabe von Verknüpfungstafeln für diese Vertreter.

Bsp: $n = 4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	(1)
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	(2)
3	0	3	2	1

lesen: $\bar{2} + \bar{3} = \bar{1}$

$\bar{2} \cdot \bar{3} = \bar{2}$