23.12.19

Donnerstag, 21. Dezember 2023 10:05

Zahlentheorie und ihre Anwendungen

Division mit Rest

Im $(\mathbb{Z},+,\cdot)$ rechnen wir im "üblichen" Sinn. Es gibt eine Division mit Rest, das heißt zu $m,n \in \mathbb{Z}$ gibt es $q,r \in \mathbb{Z}$, $0 \le r < n$ so dass $m = q \cdot n + r$.

Zum Beispiel für $m = 43$ und $n = 10$: $43 = 4 \cdot 10 + 3$

Falls $r = 0$ ist, schreiben wir $n \mid m$ und sagen n teilt m.

Dfn 148 Zu $n,m \in \mathbb{N}$ heißt $ggT(m,n) := \max\{x \in \mathbb{N} \mid x \mid n \wedge x \mid m\}$ der größte gemeinsame Teiler von n und m.

Lemma 149 $m = q \cdot n + r$, $q \neq 0$, $\Rightarrow ggT(n,m) = ggT(n,r)$

Beweis Es sei $d = ggT(n,m) \in \mathbb{N}$, also: $n = d \cdot k$ und $m = d \cdot l \Rightarrow r = m - qn = d \cdot l - dkq = d(l - qk) \Rightarrow d \mid r \Rightarrow d \mid r \wedge d \mid m$. Angenommen es gibt $d' > d$ mit $d' \mid r$ und $d' \mid n$. Dann: $r = l'd'$, $n = k'd' \Rightarrow$

$m = qk'd' + l'd' = (qk' + l')d' \Rightarrow d' \mid m$ in $\mathbb{Z}$

zu $d = ggT(n, m)$ □

Satz 150 (Bezout) Zu $m, n \in \mathbb{Z}$ gibt es $a, b \in \mathbb{Z}$ mit

$ggT(m, n) = a \cdot m + b \cdot n$.

Beweis OBdA $m, n > 0$ und $n \geq m$. Induktion nach $n \in \mathbb{N}$. Indvoraussetzung: Satz richtig für alle $n' < n$. Induktionsanfang: $n = 1 \Rightarrow m = 1 \Rightarrow$ $ggT(m, n) = 1 \cdot 1 + 1 \cdot 0$. Induktionsschritt: <u>1 Fall</u>

<u>$m = n$</u>: $ggT(m, n) = m = 1 \cdot m + 0 \cdot n$ ✓

<u>2 Fall $m < n$</u>: $n = qm + r \overset{\text{Lemma}}{\Rightarrow} ggT(m, n) =$

$ggT(m, r) \overset{IV}{=} am + br = am + b(n - qm)$

$\boxed{\begin{array}{l} r \in \{0, \ldots, m-1\} \\ r < m < n \end{array}}$ $= m(a - bq) + n \cdot b$ □

Bemerkung 151 Euklidisches Algorithmus. Wir berechnen den ggT von $n = 101$ und $m = 35$:

$101 = 2 \cdot 35 + 31$

$35 = 1 \cdot 31 + 4$

Also ist $ggT(101, 35) = 1 =$

$= 4 - 1 \cdot 3 = 4 - (31 - 7 \cdot 4)$

$$35 = 1 \cdot 31 + 4$$
$$31 = 7 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

$$= 4 - 1 \cdot 3 = 4 - (31 - 7 \cdot 4)$$
$$= 8 \cdot 4 - 31$$
$$= 8 \cdot (35 - 1 \cdot 31) - 31$$
$$= 8 \cdot 35 - 9 \cdot 31$$
$$= (-9)(101 - 2 \cdot 35) + 8 \cdot 35$$
$$= (-9) \cdot 101 + 26 \cdot 35$$