Ganzzahlige Division mit Rest

Für $a, b \in \mathbb{N}$ mit $a \geq b$ gibt es stets eine „Zerlegung“ von a der Form

$$a = q \cdot b + r \text{ mit } 0 \leq r \leq b - 1 \ .$$

Hierbei gilt

$$q = \left\lfloor \frac{a}{b} \right\rfloor$$

(salopp formuliert: b passt q-mal in a rein) und

$$r = a - q \cdot b$$

ist der ganzzahlige Rest.

Zum Beispiel gilt für $a = 99$ und $b = 15$:

$$99 = 6 \cdot 15 + 9 \ .$$

Somit: $q = 6$ und $r = 9$.

Schema des Euklidischen Algorithmus

Berechnung des $\mathrm{ggT}(a_0, a_1)$ durch iterierte ganzzahlige Division mit Rest

a_0	$=$	$q_1 \cdot a_1 + a_2$	a_2	$=$	$-q_1 a_1 + a_0$
a_1	$=$	$q_2 \cdot a_2 + a_3$	a_3	$=$	$-q_2 a_2 + a_1$
	$\dots$			$\dots$	
a_i	$=$	$q_{i+1} \cdot a_{i+1} + a_{i+2}$	a_{i+2}	$=$	$-q_{i+1} \cdot q_{i+1} a_{i+1} + a_i$
	$\dots$			$\dots$	
a_{k-1}	$=$	$-q_{k-2} \cdot a_{k-2} + a_{k-3}$			
a_{k-2}	$=$	$q_{k-1} \cdot a_{k-1} + a_k$	a_k	$=$	$-q_{k-1} \cdot a_{k-1} + a_{k-2}$
a_{k-1}	$=$	$q_k \cdot a_k$			

Es gilt dann

$$\mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_1, a_2) = \cdots = \mathrm{ggT}(a_{k-2}, a_{k-1}) = \mathrm{ggT}(a_{k-1}, a_k) = a_k$$

und $a_k = x_i \cdot a_{i+1} + y_i \cdot a_i$ für geeignete $x_i, y_i \in \mathbb{Z}$.

ggT als ganzzahlige Linearkombination

Aus dem Schema des Euklidischen Algorithmus ergibt sich folgende rekursive Berechnung der $x_i, y_i \in \mathbb{Z}$ (zu Herleitung s. unten):

$$x_{k-2} = -q_{k-1} \quad \text{und} \quad y_{k-2} = 1$$

$$x_i = y_{i+1} - x_{i+1} \cdot q_{i+1} \quad \text{und} \quad y_i = x_{i+1}$$

berechnet werden. Insbesondere gilt:

$$\text{ggT}(a_0, a_1) = a_k = x_0 \cdot a_1 + y_0 \cdot a_0 \ .$$

Induktive Herleitung der Rekursionsformel: Aus

$$a_{i+2} = -q_{i+1}a_{i+1} + a_i \text{ und } a_k = x_{i+1}a_{i+2} + y_{i+1}a_{i+1}$$

ergibt sich

$$\begin{aligned} a_k &= x_{i+1}(-q_{i+1}a_{i+1} + a_i) + y_{i+1}a_{i+1} \\ &= \underbrace{(y_{i+1} - q_{i+1}x_{i+1})}_{=:x_i} a_{i+1} + \underbrace{x_{i+1}}_{=:y_i} a_i \ . \end{aligned}$$

Beispiellauf zum erweiterten Euklidischen Algorithmus

Zur Berechnung von ggT$(392, 252)$ erhalten wir mit $a_0 = 392$, $a_1 = 252$ unter Anwendung von

$$x_{k-2} = -q_{k-1} \text{ und } y_{k-2} = 1$$

und

$$x_i = y_{i+1} - x_{i+1}q_{i+1} \text{ und } y_i = x_{i+1}$$

die folgende Rechnung:

i	a_i	a_{i+1}	$q_{i+1} = \lfloor a_i/a_{i+1} \rfloor$	x_i	y_i
0	392	252	1	-3	2
1	252	140	1	2	-1
2	140	112	1	-1	1
3	112	28	4		

Test:

$$28 = \text{ggT}(392, 252) = 2 \cdot 392 - 3 \cdot 252 = 784 - 756$$