Euklidischer Algorithmus

Euklidisches Algorithmus – Division mit Rest

Wie berechnet man ggT(693, 286)?

a) über Primfaktorzerlegung: 693 =
286 = $\Big\}$ ggT(693, 286) =

b) über Teilermengen: T(693) = { }
T(286) = { } $\Big\}$ ggT(693, 286) =

oder (NEU! – 3. Verfahren!). Dazu brauchen wir:

<u>Def. und Satz.</u> Seien $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Dann existiert genau ein Zahlenpaar $q, r \in \mathbb{Z}$ mit $a = q \cdot b + r$ und $0 \leq r < b$, d.h. kurz

$$\boxed{\forall a \in \mathbb{Z}, b \in \mathbb{N}\ \exists_1\, q, r \in \mathbb{Z}: \quad a = q \cdot b + r \ \wedge\ 0 \leq r < b}$$

Diese Darstellung heißt **Division mit Rest** und r heißt **Rest.** (In C/Java etc: $r = a \% b$)

$\boxed{\text{Ü}}$ a) $a = 15, b = 6$: $q = 2; r = 3$ $\quad 15 = 2 \cdot 6 + 3$

b) $a = -15, b = 6$: $q = -3; r = 3$ $\quad -15 = -3 \cdot 6 + 3$

Euklidischer Algorithmus – Sätze zum ggT

Wichtige Eigenschaften des ggT:

<u>Satz</u>. Seien $a, b \in \mathbb{Z}$:

1) $ggT(a,a) = a$ weil $T(a) \cap T(a) = T(a)$
2) $ggT(a,1) = 1$ weil $T(1) = \{1\}$ und $T(a) \cap T(1) = \{1\}$
3) $ggT(a,0) = a$ weil $T(0) = \mathbb{N}$ und $T(a) \cap T(0) = \{a\}$
4) $ggT(a,b) = ggT(b,a)$ weil $T(a) \cap T(b) = T(b) \cap T(a)$
5) $ggT(a,b) = ggT(a-b, b)$

Beweis.

$$\left.\begin{array}{l} ggT(a;b) \mid a \\ ggT(a;b) \mid b \end{array}\right\} \, ggT(a;b) \mid a-b$$

$\Rightarrow ggT(a;b) \in T(a-b) \cap T(b)$

sei $g \in T(a-b) \cap T(b)$ und $g > ggT(a;b)$

$\Rightarrow g \mid a-b \;\wedge\; g \mid b \Rightarrow g \mid (a-b)+b \Leftrightarrow g \mid a$

$\Rightarrow g \mid a \;\wedge\; g \mid b \;\wedge\; g > ggT(a;b)$ ↯ $\Rightarrow ggT(a;b) = ggT(a-b;b)$

Euklidischer Algorithmus – Eukl. Alg.

Jetzt kommt der eukl. Alg. (3. Verfahren und schnellstes!):

$$
\begin{aligned}
ggT(693,286) &= ggT(693-286;286) = ggT(407;286) \\
&= ggT(407-286,286) = ggT(121;286) \\
&= ggT(286;121) = ggT(165;121) \\
&= ggT(44;121) = ggT(77;44) \\
&= ggT(44;33) = ggT(33;11) = ggT(22;11) \\
&= ggT(11;11) = 11
\end{aligned}
$$

Division mit Rest (iteriert):

$$
\begin{aligned}
693 &= 2 \cdot 286 + 121 \\
286 &= 2 \cdot 121 + 44 \\
121 &= 2 \cdot 44 + 33 \\
44 &= 1 \cdot 33 + \boxed{11} \\
33 &= 3 \cdot 11 + 0
\end{aligned}
$$

ggT

letzter Rest ≠ 0

Tabellenform

a	b	r
693	286	121
286	121	44
121	44	33
44	33	$\boxed{11}$ ggT
33	11	0

Allgemein: $r_1 = a,\ r_2 = b$ rekursiv

$$
\left.
\begin{aligned}
r_1 &= q_1 r_2 + r_3 \\
r_2 &= q_2 r_3 + r_4 \\
&\dots
\end{aligned}
\right\}
\quad r_n = q_n r_{n+1} + r_{n+2} \quad (n \geq 1)
$$