8.1 Der EUKLIDische Algorithmus

Der Euklidische Algorithmus liefert den größten gemeinsamen Teiler (ggT) zweier ganzer Zahlen,

$$\mathrm{ggT}(a,b) = \max\{d \in \mathbb{Z} \mid d|a, d|b\}$$

Wenn man der Einfachheit halber noch $\mathrm{ggT}(0,0) = 0$ setzt, hat man die Funktion

$$\mathrm{ggT} : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{N}$$

mit den folgenden Eigenschaften:

Hilfssatz 1 *Für beliebige $a, b, c, q \in \mathbb{Z}$ gilt:*
(i) $\mathrm{ggT}(a,b) = \mathrm{ggT}(b,a)$.
(ii) $\mathrm{ggT}(a,-b) = \mathrm{ggT}(a,b)$.
(iii) $\mathrm{ggT}(a,0) = |a|$.
(iv) $\mathrm{ggT}(a-qb,b) = \mathrm{ggT}(a,b)$.

Beweis. Trivial; für (iv) verwendet man die Äquivalenz $d|a,b \Longleftrightarrow d|a-qb,b$. ◇

Der Euklidische Algorithmus wird gewöhnlich als Folge von Divisionen mit Rest aufgeschrieben:

$$r_0 = |a|, r_1 = |b|, \ldots, r_{i-1} = q_i r_i + r_{i+1},$$

wobei q_i der ganzzahlige Quotient und r_{i+1} der eindeutig bestimmte Divisionsrest mit $0 \leq r_{i+1} < r_i$ ist. Ist dann $r_n \neq 0$ und $r_{n+1} = 0$, so ist $r_n = \mathrm{ggT}(a,b)$. Denn aus Hilfssatz 1 folgt

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_0,r_1) = \mathrm{ggT}(r_1,r_2) = \ldots = \mathrm{ggT}(r_n,0) = r_n.$$

Da außerdem

$$r_1 > r_2 > \ldots > r_i \geq 0 \quad \text{für alle } i,$$

wird die Abbruchbedingung $r_{n+1} = 0$ nach spätestens $n \leq |b|$ Iterationsschritten (also Divisionen) erreicht.

Eine kleine Erweiterung liefert sogar noch mehr. Es ist nämlich jedes r_i ganzzahlige Linearkombination der beiden vorhergehenden Divisionsreste, also auch von $|a|$ und $|b|$; für r_0 und r_1 ist das trivial, und allgemein folgt es durch Induktion: Sei schon $r_j = |a|x_j + |b|y_j$ für $0 \leq j \leq i$. Dann folgt

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= |a|x_{i-1} + |b|y_{i-1} - q_i|a|x_i - q_i|b|y_i \\ &= |a|(x_{i-1} - q_i x_i) + |b|(y_{i-1} - q_i y_i). \end{aligned}$$

Diese Überlegung liefert gleich eine explizite Konstruktion für die Koeffizienten mit; sie erfüllen nämlich die Rekursionsformeln

$$x_{i+1} = x_{i-1} - q_i x_i \quad \text{mit} \quad x_0 = 1, x_1 = 0,$$

$$y_{i+1} = y_{i-1} - q_i y_i \quad \text{mit} \quad y_0 = 0, y_1 = 1,$$

die bis auf die Startwerte mit der Formel für die r_i übereinstimmen:

$$r_{i+1} = r_{i-1} - q_i r_i \quad \text{mit} \quad r_0 = |a|, r_1 = |b|.$$

Der **erweiterte Euklidische Algorithmus** (auch Algorithmus von LAGRANGE genannt) ist die Zusammenfassung dieser drei Rekursionsformeln. Damit ist gezeigt (wenn man die Vorzeichen von x_n und y_n passend justiert):

Satz 1 *Der erweiterte Euklidische Algorithmus liefert in endlich vielen Schritten zu zwei ganzen Zahlen a und b den größten gemeinsamen Teiler d und ganzzahlige Koeffizienten x und y mit $ax + by = d$.*

Bemerkungen

1. Das kleinste gemeinsame Vielfache berechnet man nach der Formel

   $$\mathrm{kgV}(a, b) = \frac{ab}{\mathrm{ggT}(a, b)}$$

   ebenfalls effizient.

2. Der größte gemeinsame Teiler mehrerer Zahlen kann man nach der Formel

   $$\mathrm{ggT}(\ldots(\mathrm{ggT}(\mathrm{ggT}(a_1, a_2), a_3)\ldots, a_r)$$

   berechnen; hier sind noch kleine Optimierungen möglich. Analoges gilt für das kleinste gemeinsame Vielfache.