

Mathematik IT 2 (Lineare Algebra)

für die Studiengänge Informatik, IMT und eBusiness im Sommersemester 2013

Euklidischer Algorithmus

Gegeben sind Zahlen $a, b \in \mathbb{Z}$ mit $b \neq 0$. Gesucht sind der größte gemeinsame Teiler $\text{ggT}(a, b)$ von a und b , sowie Zahlen $\alpha, \beta \in \mathbb{Z}$ mit $\text{ggT}(a, b) = \alpha \cdot a + \beta \cdot b$. Es gilt

$$\text{ggT}(a, b) = \begin{cases} b & , \text{ falls } a \bmod b = 0 \\ \text{ggT}(b, a \bmod b) & , \text{ sonst} \end{cases}$$

Die Berechnung erfolgt mit dem (erweiterten) Euklidischen Algorithmus:

$$\begin{array}{lll} \alpha_0 := 1 & , & \beta_0 := -q_0 & , & \text{wobei } a = q_0 \cdot b + r_0 \\ \alpha_1 := -q_1 & , & \beta_1 := 1 + q_0 \cdot q_1 & , & \text{wobei } b = q_1 \cdot r_0 + r_1 \\ \alpha_2 := \alpha_0 - \alpha_1 \cdot q_2 & , & \beta_2 := \beta_0 - \beta_1 \cdot q_2 & , & \text{wobei } r_0 = q_2 \cdot r_1 + r_2 \\ \vdots & & \vdots & & \vdots \\ \alpha_n := \alpha_{n-2} - \alpha_{n-1} \cdot q_n & , & \beta_n := \beta_{n-2} - \beta_{n-1} \cdot q_n & , & \text{wobei } r_{n-2} = q_n \cdot r_{n-1} + r_n \text{ und } n \geq 2 \end{array}$$

Setze $\alpha := \alpha_n$ und $\beta := \beta_n$ für das niedrigste n mit $r_{n+1} = 0$.

Beispiel:

Gesucht ist der ggT von $a = 126$ und $b = 22$. Mit den Notationen des o.g. Algorithmus berechnet man:

$$\begin{array}{llll} 126 = 5 \cdot 22 + 16 & \Rightarrow & \alpha_0 = 1 & , \quad \beta_0 = -5 \\ 22 = 1 \cdot 16 + 6 & \Rightarrow & \alpha_1 = -1 & , \quad \beta_1 = 1 + (-5) \cdot 1 = 6 \\ 16 = 2 \cdot 6 + 4 & \Rightarrow & \alpha_2 = 1 - (-1) \cdot 2 = 3 & , \quad \beta_2 = -5 - 6 \cdot 2 = -17 \\ 6 = 1 \cdot 4 + 2 & \Rightarrow & \alpha_3 = -1 - 3 \cdot 1 = -4 & , \quad \beta_3 = 6 - (-17) \cdot 1 = 23 \\ 4 = 2 \cdot 2 + 0 & \Rightarrow & \alpha = \alpha_3 = -4 & , \quad \beta = \beta_3 = 23 \end{array}$$

Es gilt also $\text{ggT}(126, 22) = 2 = -4 \cdot 126 + 23 \cdot 22$.

Bemerkungen:

- Die (einfache) Bestimmung des größten gemeinsamen Teilers von a und b wird Euklidischer Algorithmus genannt. Werden ergänzend die Koeffizienten α und β der Linearkombination $\text{ggT}(a, b) = \alpha \cdot a + \beta \cdot b$ mit bestimmt, dann spricht man in der Literatur oft auch vom erweiterten Euklidischen Algorithmus.
- In der oben angegebenen Darstellung des Euklidischen Algorithmus wird jeder Rest r_n als Linearkombination von a und b dargestellt, d.h. es gilt $r_n = \alpha_n \cdot a + \beta_n \cdot b$. Dieser Zusammenhang ist nicht auf den ersten Blick ersichtlich, wird aber deutlich, wenn man nach jedem Schritt die Koeffizienten durch Einsetzen direkt mitbestimmt. Für obiges Beispiel sieht das wie folgt aus:

$$\begin{array}{lll} 126 = 5 \cdot 22 + 16 & \Rightarrow & 16 = 126 - 5 \cdot 22 \\ 22 = 1 \cdot 16 + 6 & \Rightarrow & 6 = 22 - 1 \cdot 16 = 1 \cdot 22 - (1 \cdot 126 - 5 \cdot 16) = -1 \cdot 126 + 6 \cdot 22 \\ 16 = 2 \cdot 6 + 4 & \Rightarrow & 4 = 16 - 2 \cdot 6 = 1 \cdot 126 - 5 \cdot 16 - 2 \cdot (-1 \cdot 126 + 6 \cdot 22) = 3 \cdot 126 - 17 \cdot 22 \\ 6 = 1 \cdot 4 + 2 & \Rightarrow & 2 = 6 - 1 \cdot 4 = -1 \cdot 126 + 6 \cdot 22 - (3 \cdot 126 - 17 \cdot 22) = -4 \cdot 126 + 23 \cdot 22 \\ 4 = 2 \cdot 2 + 0 & \Rightarrow & \text{ggT}(126, 22) = 2 = -4 \cdot 126 + 23 \cdot 22 \end{array}$$

- Man kann alternativ auch erst den größten gemeinsamen Teiler von a und b berechnen, und dann anschließend „rückwärts“ die Koeffizienten α und β berechnen. Für obiges Beispiel sieht das wie folgt aus:

$$\begin{aligned}
126 &= 5 \cdot 22 + 16 &\Rightarrow 16 &= 126 - 5 \cdot 22 \\
22 &= 1 \cdot 16 + 6 &\Rightarrow 6 &= 22 - 1 \cdot 16 \\
16 &= 2 \cdot 6 + 4 &\Rightarrow 4 &= 16 - 2 \cdot 6 \\
6 &= 1 \cdot 4 + 2 &\Rightarrow 2 &= 6 - 1 \cdot 4 \\
4 &= 2 \cdot 2 + 0 &\Rightarrow \text{ggT}(126, 22) &= 2
\end{aligned}$$

Daraus folgt:

$$\begin{aligned}
\text{ggT}(126, 22) &= 2 = 6 - 1 \cdot 4 = 6 - (16 - 2 \cdot 6) \\
&= 3 \cdot 6 - 1 \cdot 16 = 3 \cdot (22 - 1 \cdot 16) - 1 \cdot 16 \\
&= 3 \cdot 22 - 4 \cdot 16 = 3 \cdot 22 - 4 \cdot (126 - 5 \cdot 22) \\
&= -4 \cdot 126 + 23 \cdot 22
\end{aligned}$$

Allgemein führt das auf den folgenden Algorithmus: Berechne

$$\begin{aligned}
a &= q_0 \cdot b + r_0 \\
b &= q_1 \cdot r_0 + r_1 \\
r_0 &= q_2 \cdot r_1 + r_2 \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} \cdot r_n + 0
\end{aligned}$$

Setze der Reihe nach

$$\begin{aligned}
s_{n+1} &:= 0 & , & & t_{n+1} &:= 1 \\
s_n &:= t_n & , & & t_n &:= s_n - q_{n-1} \cdot t_n \\
&\vdots & & & \vdots & \\
s_j &:= t_{j+1} & , & & t_j &:= s_{j+1} - q_j \cdot t_{j+1} \\
&\vdots & & & \vdots & \\
\alpha &:= s_0 := t_1 & , & & \beta &:= t_0 := s_1 - q_0 \cdot t_1
\end{aligned}$$

Für diese Variante des erweiterten Euklidischen Algorithmus gilt $\text{ggT}(a, b) = r_n = s_j \cdot r_{j-2} + t_j \cdot r_{j-1}$ für $j = 0, 1, \dots, n+1$, wobei $r_{-2} := a$ und $r_{-1} := b$.