§ 2 Der euklidische Algorithmus in $\mathbb{Z}$

(2.12) Der euklidische Algorithmus (EA)

Seien $a, b \in \mathbb{N}$. Die Folgen $(r_k)_{k\geq 0}$, $(q_k)_{k\geq 1}$ seien rekursiv definiert durch:
$r_0 := a$, $r_1 := b$. Für $k \in \mathbb{N}_0$ sei q_{k+1} der Quotient und r_{k+2} der Rest bei Division von r_k durch r_{k+1} , falls $r_{k+1} \neq 0$, d.h.

$$(\star) \quad r_k \;=\; q_{k+1} \cdot r_{k+1} + r_{k+2} \quad \text{mit} \quad 0 \leq r_{k+2} < r_{k+1}$$

Dann gibt es eine Zahl $n \in \mathbb{N}$ mit $r_n \neq 0$ und $r_{n+1} = 0$, wobei gilt

$$r_n \;=\; \text{ggT}(a, b)$$

<u>Bew:</u> Wir führen wiederholte Division mit Rest aus. Dies ist solange möglich, wie die Zahl, durch die geteilt ist, von 0 verschieden ist.

$$\begin{aligned}
r_0 &= a \;,\quad r_1 \;=\; b \\
r_0 &= q_1 \cdot r_1 + r_2 \quad \text{mit} \quad 0 \leq r_2 < r_1 \\
r_1 &= q_2 \cdot r_2 + r_3 \quad \text{mit} \quad 0 \leq r_3 < r_2 \\
r_2 &= q_3 \cdot r_3 + r_4 \quad \text{mit} \quad 0 \leq r_4 < r_3 \\
&\;\vdots \\
r_k &= q_{k+1} \cdot r_{k+1} + r_{k+2} \quad \text{mit} \quad 0 \leq r_{k+2} < r_{k+1} \\
&\;\vdots
\end{aligned}$$

Annahme: $r_k > 0 \quad \forall\, k \geq 2$. Dann folgt $b = r_1 > r_2 > r_3 > r_4 > \ldots > r_k > \ldots > 0$,

d.h. es gibt unendlich viele natürliche Zahlen $< b$. **Widerspruch!**

Folglich gibt es ein $n \in \mathbb{N}$ mit $r_{n+1} = 0$ und $r_n \neq 0$. Zu zeigen bleibt, daß r_n wirklich der ggT von a und b ist. Dazu schreiben wir noch einmal das Divisionsschema auf:

$$\begin{aligned}
r_0 &= a \;,\quad r_1 \;=\; b \\
r_0 &= q_1 \cdot r_1 + r_2 \quad \text{mit} \quad 0 < r_2 < r_1 \\
r_1 &= q_2 \cdot r_2 + r_3 \quad \text{mit} \quad 0 < r_3 < r_2 \\
r_2 &= q_3 \cdot r_3 + r_4 \quad \text{mit} \quad 0 < r_4 < r_3 \\
&\;\vdots \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n \quad \text{mit} \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n \cdot r_n + \underbrace{r_{n+1}}_{=0}
\end{aligned}$$

Aus der letzten Gleichung folgt $r_n \,|\, r_{n-1}$, so daß nach (2.9c) gilt: $r_n = \text{ggT}(r_n, r_{n-1})$. Mit (2.10) und den obigen Gleichungen ergibt sich

$$\underline{\underline{\text{ggT}(a,b)}} = \text{ggT}(r_0,r_1) = \text{ggT}(r_1,r_2) = \text{ggT}(r_2,r_3) = \ldots = \text{ggT}(r_{n-1},r_n) = \underline{\underline{r_n}}$$

•

(2.13) BEM: Der ggT von $a, b \in \mathbb{Z}$ läßt sich im Falle $a \neq 0$ und $b \neq 0$ nach (2.9b) berechnen durch $\text{ggT}(a,b) = \text{ggT}(|a|,|b|)$, da dann $|a|,|b| \in \mathbb{N}$ gilt. Ansonsten ist $\text{ggT}(a,0) = |a|$ nach (2.9d), insbesondere ist $\text{ggT}(0,0) = 0$.

Der erweiterte euklidische Algorithmus (EEA)

Nach (2.8) gibt es zu $a, b \in \mathbb{Z}$ immer Zahlen $x, y \in \mathbb{Z}$ mit $\text{ggT}(a,b) = xa + yb$. Wir wollen nun den EA so erweitern, daß wir neben $\text{ggT}(a,b)$ auch diese Koeffizienten x und y berechnen können. Die Bezeichnungen seien wie in (2.12) gewählt: $r_0 := a$, $r_1 := b$

$$\begin{array}{rcll}
r_0 & = & q_1 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 & = & q_2 r_2 + r_3 & 0 < r_3 < r_2 \\
 & \vdots & & \\
r_k & = & q_{k+1} r_{k+1} + r_{k+2} & 0 < r_{k+2} < r_{k+1} \quad (0 \le k < n-2) \\
 & \vdots & & \\
r_{n-2} & = & q_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} & = & q_n r_n & (r_{n+1} = 0) \\
\hline
r_n & = & \text{ggT}(a,b) &
\end{array}$$

Wir schreiben jetzt diese Gleichungen in Matrizen–Form um:

$$\begin{array}{lccccccc}
(1) & \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} & = & \begin{pmatrix} q_1 r_1 + r_2 \\ r_1 \end{pmatrix} & = & \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \\
(2) & \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} & = & \begin{pmatrix} q_2 r_2 + r_3 \\ r_2 \end{pmatrix} & = & \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \\
 & \vdots & & & & \\
(k) & \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} & = & \begin{pmatrix} q_k r_k + r_{k+1} \\ r_k \end{pmatrix} & = & \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} \\
 & \vdots & & & & \\
(n-1) & \begin{pmatrix} q_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} & = & \begin{pmatrix} q_{n-1} r_{n-1} + r_n \\ r_{n-1} \end{pmatrix} & = & \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} \\
(n) & \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix} & = & \begin{pmatrix} q_n r_n + r_{n+1} \\ r_n \end{pmatrix} & = & \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}
\end{array}$$

Sukzessives Einsetzen ergibt:

$$\begin{pmatrix} a \\ b \end{pmatrix} \overset{(1)}{=} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \overset{(2)}{=} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} \overset{(3)}{=} \dots$$

$$\overset{(n-1)}{=} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} q_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$$

$$\overset{(n)}{=} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix}$$

$$= \underbrace{\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} g \\ 0 \end{pmatrix}$$

Die Matrix A hat ganzzahlige Elemente und ist als Produkt invertierbarer Matrizen selbst wieder invertierbar:

$$\det \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} = -1 \quad (\forall\, x \in \mathbb{Z}) \quad \Longrightarrow \quad \det(A) = (-1)^n .$$

$$A \cdot \begin{pmatrix} g \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \quad \Longrightarrow \quad \begin{pmatrix} g \\ 0 \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$$

Das Inverse von A berechnen wir über die adjungierte Matrix: es ist $A^{-1} = \det(A)^{-1} \cdot A^{\mathrm{ad}}$. Ist $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$, so ist $A^{\mathrm{ad}} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$. Folglich

$$A^{-1} = \det(A)^{-1} \cdot \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = (-1)^n \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} (-1)^n\delta & (-1)^{n+1}\beta \\ (-1)^{n+1}\gamma & (-1)^n\alpha \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$$

und

$$A^{-1} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} (-1)^n\delta a + (-1)^{n+1}\beta b \\ \star \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix}$$

Also: $g = \underbrace{((-1)^n\delta)}_{=:x} \cdot a + \underbrace{((-1)^{n+1}\beta)}_{=:y} \cdot b$ mit $x := (-1)^n A[2,2]$, $y := (-1)^{n+1} A[1,2] \in \mathbb{Z}$.

Zusammenfassend erhalten wir:

(2.14) Der erweiterte euklidische Algorithmus (EEA)

Mit der Bezeichnungsweise von (2.12) gilt:

Die (2×2)–Matrix $A := \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$ ist invertierbar,

und es ist $A^{-1} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix}$ mit $g = \mathrm{ggT}(a,b)$. Insbesondere ist

$$g = ((-1)^n A[2,2]) \cdot a + (-1)^{n+1} A[1,2]) \cdot b$$

(2.15) BEM: **a)** In einer Darstellung $\mathrm{ggT}(a,b) = xa + yb$ $(x, y \in \mathbb{Z})$ sind die Koeffizienten nicht eindeutig bestimmt, es gibt sogar unendlich viele Möglichkeiten:
$\mathrm{ggT}(2,3) = 1 = (-1)\cdot 2 + 1\cdot 3 = 2\cdot 2 + (-1)\cdot 3 = 5\cdot 2 + (-3)\cdot 3 = (-4)\cdot 2 + 3\cdot 3.$

b) Sei $g = \mathrm{ggT}(a,b)$ und gelte $g = x_0 a + y_0 b$ mit $x_0, y_0 \in \mathbb{Z}$. Dann folgt

$$g = \left(x_0 + t\cdot\frac{b}{g}\right)a + \left(y_0 - t\cdot\frac{a}{g}\right)b \qquad (\forall\, t \in \mathbb{Z})$$

und dies sind alle möglichen Darstellungen von g.

c) Der EEA berechnet den ggT g von $a, b \in \mathbb{N}$ und Zahlen $x, y \in \mathbb{Z}$ mit $g = xa + yb$. Seien jetzt $a, b \in \mathbb{Z} \setminus \{0\}$. Nach (2.9b) gilt dann

$$g = \mathrm{ggT}(a,b) = \mathrm{ggT}(|a|,|b|)\,.$$

Mit dem EEA (2.14) lassen sich $x', y' \in \mathbb{Z}$ berechnen mit

$$g = x'\cdot|a| + y'\cdot|b|\,.$$

Um nun g als Linearkombination von a und b darzustellen, benutzen wir die Vorzeichenfunktion, die für $x \in \mathbb{R}$ definiert ist durch

$$\mathrm{sign}\,(x) := \begin{cases} 1 & \text{für } x > 0 \\ 0 & \text{für } x = 0 \\ -1 & \text{für } x < 0 \end{cases}$$

Insbesondere gilt $|x| = \mathrm{sign}\,(x)\cdot x$. Es folgt

$$g = (\underbrace{x'\cdot\mathrm{sign}\,(a)}_{=x\in\mathbb{Z}})\cdot a + (\underbrace{y'\cdot\mathrm{sign}\,(b)}_{=y\in\mathbb{Z}})\cdot b$$

Für $b = 0$ ist $|a| = \mathrm{ggT}(a,0) = \mathrm{sign}\,(a)\cdot a + 1\cdot b$. •

(2.16) DEF: $a_1, a_2, \ldots, a_n$ $(n \geq 2)$ seien ganze Zahlen. Eine ganze Zahl g heißt **ggT** von $a_1, a_2, \ldots, a_n$ (in Zeichen: $g = \mathrm{ggT}(a_1, a_2, \ldots, a_n)$), wenn gilt:

i) $g \geq 0$

ii) $g | a_i$ für alle $i = 1, 2, \ldots, n$

iii) Für ein beliebiges $t \in \mathbb{Z}$ mit $t | a_i$ für alle $i = 1, 2, \ldots, n$ folgt $t | g$,.

(2.17) SATZ: Für $a, b, c \in \mathbb{Z}$ gilt $\mathrm{ggT}(a,b,c) = \mathrm{ggT}(\mathrm{ggT}(a,b),c)\,.$

(2.18) BEM: Für ganze Zahlen $a_1, a_2, \ldots, a_n$ $(n \geq 3)$ gilt:

a) $\mathrm{ggT}(a_1, a_2, \ldots, a_n) = \mathrm{ggT}(\mathrm{ggT}(a_1, a_2, \ldots, a_{n-1}), a_n)$

b) $\mathrm{ggT}(a_1, a_2, \ldots, a_n)$ existiert und ist eindeutig bestimmt.