Erweiterter euklidischer Algorithmus

Eingabe: a, b
Ausgabe: x, y, g mit $ax + by = g = \text{ggT}(a, b)$.

- $r_0 = |a|$
- $r_1 = |b|$
- $\begin{pmatrix} x_0 & x_1 \\ y_0 & y_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- **Solange** $r_i \neq 0$ $(i = 1, \ldots)$:
  - $q_i := \lfloor r_{i-1} / r_i \rfloor$
  - $r_{i+1} := r_{i-1} \mod r_i$
  - $\begin{pmatrix} x_{i+1} & x_i \\ y_{i+1} & y_i \end{pmatrix} := \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

Ergebnis: $x_{i-1}, y_{i-1}, r_{i-1}$

Beispiel

i	0	1	2	3	4	5	6
r_i	234	84	66	18	12	6	0
q_i		2	1	3	1	2	1
x_i	1	0	1	-1	4	-5	14
y_i	0	1	-2	3	-11	14	-39

Analyse I

- $r_{i-1}/r_i = q_i$ Rest r_{i+1}
- $r_{i+1} = r_{i-1} - q_i \cdot r_i$ mit $0 \leq r_{i+1} < r_i$
- $r_0 > r_1 > \ldots \geq 0 \rightsquigarrow$ Algorithmus terminiert nach höchstens r_0 Schritten (schlechte Abschätzung).
- Sei N Anzahl der Iterationen:
  $r_0 > r_1 > \ldots r_N = g > r_{N+1} = 0$.

Analyse II

$$\begin{pmatrix} r_i & r_{i+1} \end{pmatrix} = \begin{pmatrix} r_{i-1} & r_i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} = \begin{pmatrix} x_i & x_{i-1} \\ y_i & y_{i-1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$$

Behauptung. $g \mid a, b$.

Beweis.

$$\begin{aligned} \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} r_0 & r_1 \end{pmatrix} &= \begin{pmatrix} r_1 & r_2 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} r_2 & r_3 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \dots \\ &= \begin{pmatrix} r_N & 0 \end{pmatrix} \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

□

$$\begin{pmatrix} r_i & r_{i+1} \end{pmatrix} = \begin{pmatrix} r_{i-1} & r_i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} = \begin{pmatrix} x_i & x_{i-1} \\ y_i & y_{i-1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$$

Behauptung. Für jedes i gilt

$$a \cdot x_i + b \cdot y_i = r_i$$

Insbesondere $a \cdot x_N + b \cdot y_N = g$.

Beweis.
Genauer:

$$\begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} = \begin{pmatrix} r_i & r_{i+1} \end{pmatrix}$$

Induktionsanfang:

$$\begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} x_0 & x_1 \\ y_0 & y_1 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} r_0 & r_1 \end{pmatrix}$$

Analyse III

$$\begin{pmatrix} r_i & r_{i+1} \end{pmatrix} = \begin{pmatrix} r_{i-1} & r_i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} = \begin{pmatrix} x_i & x_{i-1} \\ y_i & y_{i-1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$$

Behauptung. Für jedes i gilt

$$a \cdot x_i + b \cdot y_i = r_i$$

Insbesondere $a \cdot x_N + b \cdot y_N = g$.

Beweis.
Induktionsschritt:

$$\begin{aligned} \begin{pmatrix} a & b \end{pmatrix} \cdot \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} &= \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} x_{i-1} & x_i \\ y_{i-1} & y_i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \\ &= \begin{pmatrix} r_{i-1} & r_i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \\ &= \begin{pmatrix} r_i & r_{i+1} \end{pmatrix} \end{aligned}$$

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

Beweis.
Wir wissen schon $g \mid a, b$. Zu zeigen: wenn $h \mid a, b$, dann $h \mid g$.
Aus $h \mid a, b$ folgt $h \mid a \cdot x_N + b \cdot y_N = g$. □