Erweiterter Euklidischer Algorithmus (EEA)

Algorithmus Erweiterter Euklidischer Algorithmus (EEA)

EINGABE: a_0, a_1 mit $N(a_0) \geq N(a_1)$

1. Setze $i := 1$, $x_0 := 1$, $y_0 := 0$, $x_1 := 0$ und $y_1 := 1$.
2. While $(a_i \neq 0)$
   1. Berechne mittels euklidischer Division a_{i+1}, q_{i+1} mit
      $$a_{i-1} = q_{i+1}a_i + a_{i+1} \text{ und } N(a_{i+1}) < N(a_i) \text{ oder } a_{i+1} = 0.$$
   2. Setze $x_{i+1} := x_{i-1} - q_{i+1}x_i$.
   3. Setze $y_{i+1} := y_{i-1} - q_{i+1}y_i$.
   4. Setze $i := i + 1$.

AUSGABE: $a_{i-1} = \mathrm{ggT}(a_0, a_1) = x_{i-1}a + y_{i-1}b$

Korrektheit von EEA

Satz Korrektheit von EEA

Bei Eingabe $a_0, a_1 \in R$ berechnet EEA $\mathrm{ggT}(a_0, a_1)$, x, y mit

$$x \cdot a_0 + y \cdot a_1 = \mathrm{ggT}(a_0, a_1).$$

Beweis:

- Der Algorithmus terminiert mit $a_k = 0$ und $a_{k-1} = \mathrm{ggT}(a_0, a_1)$.
- Wir beweisen per Induktion die Invariante
$$a_i = x_i \cdot a_0 + y_i \cdot a_1 \text{ für } 0 \leq i < k.$$
- IA für $i = 0$ und $i = 1$:
$$a_0 = x_0 a_0 + y_0 a_1 = 1 \cdot a_0 + 0 \cdot a_1 \text{ und } a_1 = 0 \cdot a_0 + 1 \cdot a_1.$$
- IS für $i \to i + 1$:
$$\begin{aligned} a_{i+1} &= a_{i-1} - q_{i+1} a_i \overset{\text{IV}}{=} (x_{i-1} a_0 + y_{i-1} a_1) - q_{i+1}(x_i a_0 + y_i a_1) \\ &= (x_{i-1} - q_{i+1} x_i) a_0 + (y_{i-1} - q_{i+1} y_i) a_1 = x_{i+1} a_0 + y_{i+1} a_1 \end{aligned}$$
- Bei Terminierung gilt also
$$a_{k-1} = \mathrm{ggT}(a_0, a_1) = x_{k-1} a_0 + y_{k-1} a_1.$$

Bsp. EEA

Bsp: Wir berechnen wieder $\mathrm{ggT}(93, 42)$.

i	a_i	q_i	x_i	y_i
0	93	–	1	0
1	42	–	0	1
2	9	2	1	-2
3	6	4	-4	9
4	3	1	5	-11
5	0	2		

Damit gilt $\mathrm{ggT}(93, 42) = 3 = 5 \cdot 93 - 11 \cdot 42$.

kleinstes gemeinsames Vielfaches (kgV)

Definition kgV

Sei R ein faktorieller Ring und $a, b \in R$. Dann ist das *kleinste gemeinsame Vielfache* ($\mathrm{kgV}(a, b)$) von a und b definiert als ein

$c \in R$ mit $a|c$, $b|c$ und für jedes d, das von a und b geteilt wird, gilt $c|d$.

Satz Existenz kgV

Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Dann existiert $\mathrm{kgV}(a, b)$ und ist eindeutig bis auf Assoziiertheit.

Beweis:

- **Eindeutigkeit:** Analog zu $\mathrm{ggT}(a, b)$.
- **Existenz:** Analog zu $\mathrm{ggT}(a, b)$ betrachte die Primzerlegung
$$a = u \prod_{p \in P} p^{n_p} \text{ und } b = v \prod_{p \in P} p^{m_p} \text{ für } u, v \in R^*.$$
- Es gilt $\mathrm{kgV}(a, b) = \prod_{p \in P} p^{\max\{n_p, m_p\}}$, denn jedes gemeinsame Vielfache von a, b ist von der Form $\prod_{p \in P} p^{k_p}$, $k_p \geq \max\{n_p, m_p\}$.

Zusammenhang ggT und kgV

Satz ggT und kgV

Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Dann gilt

$$\mathrm{kgV}(a,b) = \frac{ab}{\mathrm{ggT}(a,b)} \quad \text{(bis auf Assoziiertheit).}$$

Beweis:

- Schreibe wieder $a = u \prod_{p \in P} p^{n_p}$ und $b = v \prod_{p \in P} p^{m_p}$. Dann gilt

$$\begin{aligned} ab = uv \prod_{p \in P} p^{n_p + m_p} &= uv \prod_{p \in P} p^{\min\{n_p, m_p\} + \max\{n_p, m_p\}} \\ &= uv \cdot \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b). \end{aligned}$$

Kongruenzrechnung

Definition Kongruenz

Seien $a, b \in \mathbb{N}$ und $n \in \mathbb{N}$. Wir bezeichen a als *kongruent* zu b falls $n \mid (a - b)$. Wir schreiben $a \equiv b \bmod n$.

Anmerkungen:

- Es gilt $a \equiv b \bmod n$ gdw $a = b + k \cdot n$ für ein $k \in \mathbb{Z}$.
- Sei $a = qn + r$ und $b = q'n + r$. Dann gilt
$$a - b = (q - q')n \text{ und damit } a \equiv b \bmod n.$$
- D.h. $a \equiv b$ gdw a, b lassen bei Division durch n denselben Rest.

Bsp:

- Es gilt $2 \equiv 7 \equiv 12 \bmod 5$.
- a ist gerade gdw $a = 0 \bmod 2$.

Repräsentanten-Unabhängigkeit

Satz Repräsentanten-Unabhängigkeit

Seien $a \equiv b \bmod n$ und $c \equiv d \bmod n$. Dann gilt

$$a + c \equiv b + d \text{ und } ac \equiv bd \bmod n.$$

Beweis:

- Es gilt $a = b + kn$ und $c = d + \ell n$ für $k, \ell \in \mathbb{Z}$. Damit ist
$$a + c = b + d + (k + \ell)n \ .$$
- D.h. $a + c \equiv b + d$.
- Analog gilt für die Multiplikation
$$ac = (b + kn)(d + \ell n) = bd + (kd + b\ell + k\ell n)n.$$
- Es folgt $ac \equiv bd \bmod n$.

Korollar

Für $a \equiv b \bmod n$ gilt $a^m \equiv b^m \bmod n$ für alle $m \in \mathbb{N}_0$.

Bsp. Repräsentanten-Unabhängigkeit

Bsp:

- Die letzte Dezimalstelle von 3^{100} ist
$$3^{100} \equiv 9^{50} \equiv (-1)^{50} \equiv 1 \bmod 10.$$
- Sei $a = \sum_i a_i 10^i$ mit $a_i \in \{0, \ldots, 9\}$ die Dezimaldarstellung von a.
- Es gilt $a \equiv \sum_i a_i (1)^i = \sum_i a_i \bmod 3$.
- D.h. $3 \mid a$ gdw die Quersumme von a durch 3 teilbar ist.
- Analog gilt $a \equiv \sum_i a_i (-1)^i \bmod 11$. D.h. $11 \mid a$ gdw die alternierende Quersumme von a durch 11 teilbar ist.