

Bsp. Euklidischer Algorithmus

Bsp: Berechne $\text{ggT}(93, 42)$ mittels EUKLID.

$$93 - 2 \cdot 42 = 9$$

$$42 - 4 \cdot 9 = 6$$

$$9 - 1 \cdot 6 = 3$$

$$6 - 2 \cdot 3 = 0$$

- D.h. $\text{ggT}(93, 42) = 3$.
- Durch Rücksubstitution erhalten wir die Bézout-Koeffizienten x, y mit $x \cdot 93 + y \cdot 42 = 3$.

$$3 = 9 - 1 \cdot 6$$

$$= 9 - 1 \cdot (42 - 4 \cdot 9) = -42 + 5 \cdot 9$$

$$= -42 + 5 \cdot (93 - 2 \cdot 42) = 5 \cdot 93 - 11 \cdot 42.$$

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 q_i, a_{i+1} mit

$$a_{i-1} = q_i a_i + a_{i+1} \text{ und } N(a_{i+1}) < N(a_i) \text{ oder } a_{i+1} = 0.$$

② Setze $x_{i+1} := x_{i-1} - q_i x_i$.

③ Setze $y_{i+1} := y_{i-1} - q_i y_i$.

④ Setze $i := i + 1$.

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

Korrektheit von EEA

Satz Korrektheit von EEA

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

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

Beweis:

- Der Algorithmus terminiert mit $a_k = 0$ und $a_{k-1} = \text{ggT}(a_0, a_1)$.
- Wir beweisen per Induktion die Invariante

$$a_i = x_i \cdot a_0 + y_i \cdot a_1 \text{ für } 0 \leq i < k.$$

- Bei Terminierung gilt also

$$a_{k-1} = \text{ggT}(a_0, a_1) = x_{k-1} a_0 + y_{k-1} a_1.$$

- 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 $i \rightarrow i + 1$:

$$\begin{aligned} a_{i+1} &= a_{i-1} - q_i a_i \stackrel{\text{IV}}{=} (x_{i-1} a_0 + y_{i-1} a_1) - q_i (x_i a_0 + y_i a_1) \\ &= (x_{i-1} - q_i x_i) a_0 + (y_{i-1} - q_i y_i) a_1 = x_{i+1} a_0 + y_{i+1} a_1 \end{aligned}$$

Bsp. EEA

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

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

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

kleinstes gemeinsames Vielfaches (kgV)

Definition kgV

Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Dann ist das *kleinste gemeinsame Vielfache* ($\text{kgV}(a, b)$) 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 $\text{kgV}(a, b)$ und ist eindeutig bis auf Assoziiertheit.

Beweis:

- **Eindeutigkeit:** Analog zu $\text{ggT}(a, b)$.
- **Existenz:** Analog zu $\text{ggT}(a, b)$ 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 $\text{kgV}(a, b) = \prod_{p \in P} p^{\max\{n_p, m_p\}}$, 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

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

Beweis:

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

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

Kongruenzrechnung

Definition Kongruenz modulo n

Seien $a, b \in \mathbb{N}$ und $n \in \mathbb{N}$. Wir sagen a ist *kongruent* zu b modulo n , falls $n \mid (a - b)$. Wir schreiben $a \equiv b \pmod{n}$.

Anmerkungen:

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

Bsp:

- Es gilt $2 \equiv 7 \equiv (-3) \pmod{5}$.
- a ist gerade gdw $a \equiv 0 \pmod{2}$.

Repräsentanten-Unabhängigkeit

Satz Repräsentanten-Unabhängigkeit

Seien $a \equiv b \pmod{n}$ und $c \equiv d \pmod{n}$. Dann gilt

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

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. $a + c \equiv b + d \pmod{n}$.
- Analog gilt für die Multiplikation

$$ac = (b + kn)(d + \ell n) = bd + (kd + b\ell + k\ell n)n.$$

- Es folgt $ac \equiv bd \pmod{n}$.

Korollar

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

Bsp. Repräsentanten-Unabhängigkeit

Bsp:

- Die letzte Dezimalstelle von 3^{100} ist

$$3^{100} = 9^{50} \equiv (-1)^{50} \equiv 1 \pmod{10}.$$

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

Binomische Formel mod p

Lemma Binomische Formel mod p

Seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$. Dann gilt

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Beweis:

- Nach Binomischer Formel gilt

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

- Wir wollen zeigen, dass $p \mid \binom{p}{i}$ für $1 \leq i < p$. Daraus folgt

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

- Es gilt $\binom{p}{i} \cdot i! = \frac{p!}{(p-i)!} = \prod_{j=0}^{i-1} (p-j)$.
- Wegen $i \geq 1$ teilt p die rechte Seite der Gleichung.
- Da p die rechte Seite teilt, muss p auch die linke Seite teilen.
- Wegen $i < p$ und p prim gilt aber $p \nmid i!$. Damit folgt $p \mid \binom{p}{i}$.

Anmerkung: Die Abbildung $f : \mathbb{Z} \rightarrow \mathbb{Z}, x \mapsto x^p \pmod{p}$ ist linear, d.h.

$$f(a + b) \equiv f(a) + f(b) \pmod{p}. \text{ (} f \text{ heißt Frobenius.)}$$