Erweiterter Euklidischer Algorithmus

Algorithmus ERWEITERTER EUKLIDISCHER ALG. (EEA)

EINGABE: $a, b \in \mathbb{N}$

1. If $(b = 0)$ then return $(a, 1, 0)$;
2. $(d, x, y) \leftarrow \text{EEA}(b, a \bmod b)$;
3. $(d, x, y) \leftarrow (d, y, x - \lfloor \frac{a}{b} \rfloor y)$;

AUSGABE: $d = \text{ggT}(a, b) = xa + yb$

Korrektheit:

- Schritt 1: Für $b = 0$ gilt $d = a = \text{ggT}(a, 0) = 1a + 0b$.
- Schritt 2: $d = \text{ggT}(a, b) = \text{ggT}(b, a \bmod b)$ folgt aus dem ggT-Satz.
- Schritt 3: Für die Koeffizienten gilt
$$d = \text{ggT}(b, a \bmod b) = xb + y(a - \lfloor \tfrac{a}{b} \rfloor b) = ya + (x - \lfloor \tfrac{a}{b} \rfloor y)b.$$
- D.h. $(x, y) \leftarrow (y, x - \lfloor \frac{a}{b} \rfloor y)$ erhält die Invariante $d = xa + yb$.

Laufzeit:

- $\mathcal{O}(\log^2(\max\{a, b\}))$ analog zu EUKLID(a, b)

Beispiel $\mathrm{ggT}(15, 11)$

Tabellarische Schreibweise:

a	b	$\lfloor \frac{a}{b} \rfloor$	x	y
15	11	1	3	-4
11	4	2	-1	3
4	3	1	1	-1
3	1	3	0	1
1	0	-	1	0

Schreibweise als Gleichungen:

$$\begin{aligned} 15 - 1 \cdot 11 &= 4 \\ 11 - 2 \cdot 4 &= 3 \\ 4 - 1 \cdot 3 &= 1 \\ 3 - 3 \cdot 1 &= 0 \end{aligned} \qquad \begin{aligned} 1 &= 11 + 3(15 - 1 \cdot 11) = 3 \cdot 15 - 4 \cdot 11 \\ 1 &= 4 - 1(11 - 2 \cdot 4) = -11 + 3 \cdot 4 \\ 1 &= 4 - 1 \cdot 3 \end{aligned}$$

Abelsche Gruppen

Definition Abelsche Gruppe

Eine abelsche Gruppe ist ein Tupel $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ$ mit den folgenden Eigenschaften

1. Abgeschlossenheit: $\circ : G \times G \to G, (a, b) \mapsto a \circ b$
2. Kommutativität: $a \circ b = b \circ a$ für alle $a, b \in G$
3. Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$
4. Neutrales Element: $\exists! e \in G : a \circ e = a$ für alle $a \in G$
5. Inverses Element: Schreibweisen
   - multiplikativ: $\forall a \in G \; \exists! a^{-1} \in G$ mit $a \circ a^{-1} = e$
   - additiv: $\forall a \in G \; \exists! (-a) \in G$ mit $a \circ (-a) = e$

Wir schreiben auch abkürzend G statt $(G, \circ)$, wenn $\circ$ bekannt ist.

Falls nicht anders bezeichnet, so schreiben wir G multiplikativ mit der Verknüpfung $\circ = \cdot$.

Beispiele für Gruppen

Bsp: Unendliche Gruppen

- $(\mathbb{Z}, +)$ ist eine additive Gruppe
  1. Addition ganzer Zahlen liefert eine ganze Zahl.
  2. $a + b = b + a$ für alle $a, b \in \mathbb{Z}$
  3. $(a + b) + c = a + (b + c)$ für alle $a, b, c \in \mathbb{Z}$
  4. Neutrales Element ist $0 \in \mathbb{Z}$.
  5. Inverses von $a \in Z$ ist $(-a) \in Z$, denn $a + (-a) = 0$.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine multiplikative Gruppe
  1. Produkt von Null verschiedener rationaler Zahlen ist nicht Null.
  2. Kommutativität: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d} \cdot \frac{a}{b}$ für $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$.
  3. Assoziativität gilt analog in $\mathbb{Q}$.
  4. Neutrales Element ist $1 \in \mathbb{Q} \setminus \{0\}$.
  5. Inverses von $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ ist $\frac{b}{a} \in \mathbb{Q} \setminus \{0\}$.
- $(\mathbb{Z}, \cdot)$ ist keine Gruppe, denn 2 besitzt kein Inverses.
- $(\mathbb{N}, +)$ ist keine Gruppe, denn 1 besitzt kein Inverses.

Wir betrachten nun Gruppen G mit endlicher Kardinalität $|G|$.

Die additive Gruppe $(\mathbb{Z}_m, +)$

Satz $(\mathbb{Z}_m, +)$ ist eine Gruppe

Sei $m \in \mathbb{N}$. Dann ist $\mathbb{Z}_m$ zusammen mit der Addition modulo m

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m,\ (a, b) \mapsto a + b \bmod m$$

eine additive Gruppe.

Beweis:

1. Sei $a + b = qm + r$ mit $r \in \mathbb{Z}_m$. Dann gilt $a + b = r$ in $\mathbb{Z}_m$.
2. Folgt aus Kommutativität der Addition in $\mathbb{Z}$.
3. Folgt aus Assoziativität der Addition in $\mathbb{Z}$.
4. Neutrales Element ist $0 \in \mathbb{Z}_m$, denn $a + 0 = a \bmod m$.
5. Inverses von a ist

$$(-a) = \begin{cases} m - a & \text{für } a \neq 0 \\ 0 & \text{sonst.} \end{cases}$$

Definition $\mathbb{Z}_n^*$

Definition Eulersche ϕ-Funktion

Sei $n \in \mathbb{N}$. Wir definieren $\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \mid \mathrm{ggT}(a, n) = 1\}$. Die *Eulersche phi-Funktion* bezeichnet die Kardinalität von $\mathbb{Z}_n^*$, d.h. $\phi(n) = |\mathbb{Z}_n^*|$.

Bsp:

- Sei p prim. Dann gilt $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ und $\phi(p) = p - 1$.
- Sei $n = pq$ mit p, q prim. Dann gilt
$$\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0, p, 2p, \ldots, (q-1)p, q, 2q, (p-1)q\}.$$
- Damit folgt $\phi(n) = |\mathbb{Z}_n^*| = n - 1 - (q-1) - (p-1) = (p-1)(q-1)$.

Die multiplikative Gruppe $\mathbb{Z}_n^*$

Satz $(\mathbb{Z}_n^*, \cdot)$ ist eine Gruppe

Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z}_n^*$ zusammen mit der Multiplikation modulo n

$$\cdot : \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*,\ (a, b) \mapsto a \cdot b \bmod n$$

eine multiplikative Gruppe.

Beweis:

- Abschluss: Seien $a, b \in \mathbb{Z}_n^*$, d.h. $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n) = 1$.
- Aus Satz zur Teilerfremdheit folgt damit $\mathrm{ggT}(ab, n) = 1$.
- $\mathrm{ggT}(ab, n) = \mathrm{ggT}(ab \bmod n, n) = 1$, d.h. $(ab \bmod n) \in \mathbb{Z}_n^*$.
- Kommutativität und Assoziativität folgen aus der Kommutativität und Assoziativität der Multiplikation über $\mathbb{Z}$.
- $1 \in \mathbb{Z}_n^*$ ist neutrales Element, denn $1 \cdot a = a \bmod n$ für alle $a \in \mathbb{Z}_n^*$.

Berechnung von Inversen in $\mathbb{Z}_n^*$

Fortsetzung Beweis: Inverse in $\mathbb{Z}_n^*$

- Lemma von Bézout: $\exists x, y \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(a, n) = ax + ny$.
- OBdA gilt $x \in \mathbb{Z}_n$, denn $1 = a(x + kn) + n(y - ak)$ für alle $k \in \mathbb{Z}$.
- Es gilt $ax = 1 - ny = 1 \bmod n$, d.h. $x = a^{-1} \in \mathbb{Z}_n$.
- Ferner gilt $x \in \mathbb{Z}_n^*$, da $xa + ny = 1 = \mathrm{ggT}(x, n)$ nach Lemma von Bézout.

Korollar Berechnung von Inversen

Sei $a \in \mathbb{Z}_n^*$. Dann kann $a^{-1} \in \mathbb{Z}_n^*$ in Zeit $\mathcal{O}(\log^2 n)$ berechnet werden.

- Berechne mit EEA Zahlen $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = ax + ny$.
- Setze $a^{-1} = x \bmod n$.

Eine nicht-abelsche Gruppe

Satz Die symmetrische Gruppe

Sei $\mathcal{G}_n$ die Menge aller Permutation auf $[n]$. Dann ist $(\mathcal{G}_n, \circ)$ mit $\pi \circ \pi' = \pi(\pi')$ als Hintereinanderausführung von Permutationen eine nicht-abelsche Gruppe.

Beweis:

1. Abgeschlossenheit: $\pi(\pi')$ ist eine Permutation.
2. Nicht-kommutativ, d.h. nicht-abelsch:
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
3. Assoziativität:
$\pi \circ (\pi' \circ \pi'') = \pi \circ (\pi'(\pi'')) = \pi(\pi'(\pi'')) = \pi(\pi') \circ \pi'' = (\pi \circ \pi') \circ \pi''$.
4. Neutrales Element ist die Identität $\pi_{id} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$
5. $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}, \pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}$.

Lösbarkeit von linearen Gleichungen

Satz Eindeutige Lösung

Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Dann besitzt die Gleichung $az = b$ für jedes $b \in \mathbb{Z}_n$ genau eine Lösung $z \in \mathbb{Z}_n$.

Beweis:

- **Existenz:** EEA liefert $x, y \in \mathbb{Z}$ mit $ax + ny = 1$.
- Dann gilt $a^{-1} = x \bmod n$ und damit $z = a^{-1}b \bmod n$.
- **Eindeutigkeit:** Seien z und z' Lösungen.
- Dann gilt $az - b = az' - b \bmod n$ bzw. $a(z - z') = 0 \bmod n$.
- Wegen $\mathrm{ggT}(a, n) = 1$ folgt $n|(z - z')$ und damit $z = z' \bmod n$.