Form der Äquivalenzklassen

Anmerkung:

- Es gilt $a = a \pm m = a \pm 2m = \ldots = a + km \bmod m$ für alle $k \in \mathbb{Z}$.
- Wir schreiben auch $\{x \in \mathbb{Z} \mid x = a + mk, k \in \mathbb{Z}\} = a + m\mathbb{Z}$.
- Es gibt m verschiedene Äquivalenzklassen modulo m:

$$0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}.$$

- Sei $a = \lfloor \frac{a}{m} \rfloor m + r$ mit $r \in \mathbb{Z}_m$. Es gilt $r = a \bmod m$.
- Wir repräsentieren $a + m\mathbb{Z}$ durch eindeutiges $r \in \mathbb{Z}_m$.

Anwendung: modularer Arithmetik

- Pseudozufallszahlen mittels Linearem Kongruenzgenerator.
- Beginne mit zufälligem Startwert $x_0 \in \mathbb{Z}_m$.
- Berechne iterativ für festes $a, b \in \mathbb{Z}_m$: $x_i = ax_{i-1} + b \bmod m$.
- $x_1, x_2, x_3, \ldots$ definieren eine Pseudozufallsfolge.

Teilbarkeit durch 3

Satz Teilbarkeit durch 3

Sei $n \in \mathbb{N}$. Dann gilt $3|n$ gwd 3 die Quersumme von n teilt.

Beweis:

- Sei $n_k \ldots n_1 n_0$ die Dezimaldarstellung von n, d.h. $n = \sum_{i=0}^{k} n_i 10^i$.
- Modulo 3 gilt
$$n = \sum_{i=0}^{k} n_i 10^i = \sum_{i=0}^{k} n_i (10 \bmod 3)^i = \sum_{i=0}^{k} n_i \bmod 3.$$
- D.h. $n = 0 \bmod 3$ genau dann wenn $\sum_{i=0}^{k} n_i = 0 \bmod 3$.
- Damit gilt $3|n$ genau dann wenn 3 die Quersumme $\sum_{i=0}^{k} n_i$ teilt.

Teilbarkeit von Linearkombinationen

Lemma Linearkombination

Seien $a, b, d \in \mathbb{N}$. Falls d sowohl a als auch b teilt, dann teilt d ebenfalls $ax + by$ für alle $x, y \in \mathbb{Z}$.

Beweis:

- Es gilt nach Voraussetzung $a = dk_a$ und $b = dk_b$ für $k_a, k_b \in \mathbb{Z}$.
- Daraus folgt $ax + by = dk_a x + dk_b y = d(k_a x + k_b y)$.
- Damit teilt d die ganzzahlige Linearkombination $ax + by$.

Lemma von Bézout

Lemma von Bézout

Seien $a, b \in \mathbb{Z}$. Dann gilt $\mathrm{ggT}(a, b) = \min\{ax + by \in \mathbb{N} \mid x, y \in \mathbb{Z}\}$.

Beweis:

- Sei $S = \{ax + by \in \mathbb{Z} \mid x, y \in \mathbb{Z}\}$ und $s \in S \cap \mathbb{N}$ minimal.
- Wir zeigen zunächst, dass $\mathrm{ggT}(a, b) \leq s$.
- Lemma Linearkombination: $\mathrm{ggT}(a, b) | s$ und damit $\mathrm{ggT}(a, b) \leq s$.
- Bleibt zu zeigen, dass ebenfalls $\mathrm{ggT}(a, b) \geq s$ gilt.
- Sei $q = \lfloor \frac{a}{s} \rfloor$. Dann gilt

$$a \bmod s = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy).$$

- D.h. $a \bmod s \in S$ und $a \bmod s < s$.
- Aufgrund der Minimalität von s muss $a \bmod s = 0$ gelten.
- Damit folgt $s|a$. Analog kann $s|b$ gezeigt werden.
- D.h. s ist ein gemeinsamer Teiler von a, b und $s \leq \mathrm{ggT}(a, b)$.

Korollar für den größten gemeinsamen Teiler

Korollar ggT-Korollar

Seien $a, b \in \mathbb{Z}$. Falls d sowohl a als auch b teilt, dann teilt d ebenfalls $\mathrm{ggT}(a, b)$.

Beweis:

- Lemma Linearkombination: d teilt $ax + by$ für alle $x, y \in \mathbb{Z}$.
- Lemma von Bézout: $\mathrm{ggT}(a, b) = \min\{ax + by \in \mathbb{N} \mid x, y \in \mathbb{Z}\}$.
- Damit teilt d ebenfalls $\mathrm{ggT}(a, b)$.

Teilerfremde Zahlen

Satz zur Teilerfremdheit

Seien $a, b, p \in \mathbb{Z}$. Falls $\mathrm{ggT}(a, p) = 1$ und $\mathrm{ggT}(b, p) = 1$, dann gilt $\mathrm{ggT}(ab, p) = 1$.

- Nach Lemma von Bézout existieren Zahlen $x, y, x', y' \in \mathbb{Z}$ mit
$$ax + py = \mathrm{ggT}(a, p) = 1 \text{ und } bx' + py' = \mathrm{ggT}(b, p) = 1.$$
- Multiplikation der beiden Gleichungen liefert
$$axbx' + axpy' + pybx' + pypy' = ab(xx') + p(axy' + ybx' + ypy') = 1.$$
- Daraus folgt $\mathrm{ggT}(ab, p) = 1$.

ISBN-Code

Anwendung: ISBN-Code

- Format: Ländercode-Verlagsnummer-laufendeNr-Prüfziffer
- ISBN ist 10-stellig mit Ziffern $z_1, \ldots, z_{10}$.
- Prüfziffer $z_{10} = \sum_{i=1}^{9} iz_i \bmod 11$, d.h. $\sum_{i=1}^{10} iz_i = 0 \bmod 11$.

Satz Fehlererkennung des ISBN-Codes

Der ISBN-Code erkennt einen Fehler und einen Zahlendreher.

Beweis:

- **Fehler:** Sei $z'_j = z_j + e_j$ fehlerhaft mit Fehlerterm $e_j \in \mathbb{Z}_{10}$.
- Prüfung liefert $(\sum_{i=1}^{10} iz_i) + je_j \bmod 11$. Benötigen $je_j \neq 0 \bmod 11$.
- Da $\mathrm{ggT}(j, 11) = 1$ und $\mathrm{ggT}(e_j, 11) = 1$ gilt $\mathrm{ggT}(je_j, 11) = 1$.
- D.h. $je_j \neq 0 \bmod 11$.
- **Dreher** $z_j \leftrightarrow z_{j+1}$: Erhalten $(\sum_{i=1}^{10} iz_i) + z_j - z_{j+1} \bmod 11$.
- Für den Fehlerterm gilt $z_j - z_{j+1} \neq 0 \bmod 11$, sofern $z_j \neq z_{j+1}$.

Der Teilersatz

Satz Teilersatz

Seien $a, b \in \mathbb{Z}$ und p prim. Falls $p|ab$, dann gilt $p|a$ oder $p|b$.

Beweis:

- **Annahme:** p teilt weder a noch b.
- Dann gilt $\mathrm{ggT}(a, p) = 1$ und $\mathrm{ggT}(b, p) = 1$, da p prim ist.
- Daraus folgt $\mathrm{ggT}(ab, p) = 1$. (Widerspruch: Nach Voraussetzung gilt $p|ab$ und damit $\mathrm{ggT}(ab, p) = p$.)

Fundamentalsatz der Arithmetik

Satz Fundamentalsatz der Arithmetik

Jedes natürliche Zahl $n > 1$ lässt sich eindeutig als Produkt von Primzahlen darstellen, d.h. $n = \prod_{i=1}^{k} p_i^{e_i}$ für prime p_i.

Beweis:

- Existenz der Darstellung $\prod_{i=1}^{k} p_i^{e_i}$ per Induktion über n (Folie 12).
- Eindeutigkeit: Sei $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots q_r$.
- Teilersatz: $p_1 | \prod_{i=1}^{r} q_i$ und damit teilt p_1 ein q_i.
- Da q_i prim ist, gilt $p_1 = q_i$. Wir teilen beide Darstellungen durch p_1.
- Iterierung des Arguments liefert für jedes p_j ein passendes q_i.
- Damit sind beide Darstellungen identisch.

Satz zur Berechnung des ggTs

Satz ggT-Satz

Sei $a \in \mathbb{N}_0$, $b \in \mathbb{N}$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a \bmod b)$

- Wir zeigen zunächst $\mathrm{ggT}(a, b) | \mathrm{ggT}(b, a \bmod b)$.
- Sei $d = \mathrm{ggT}(a, b)$, d.h. d teilt sowohl a als auch b.
- Damit teilt d jede ganzzahlige Linearkombination von a und b.
- Es gilt $a \bmod b = a - qb$ mit $q = \lfloor \frac{a}{b} \rfloor$. Damit teilt d auch $a \bmod b$.
- ggT-Korollar: d teilt $\mathrm{ggT}(b, a \bmod b)$.

- Zeigen nun, dass $\mathrm{ggT}(b, a \bmod b) | \mathrm{ggT}(a, b)$.
- Sei $d = \mathrm{ggT}(b, a \bmod b)$, d.h. $d|b$ und $d|a \bmod b$.
- Schreibe $a = qb + (a \bmod b)$. Damit teilt d auch a.
- ggT-Korollar: d teilt $\mathrm{ggT}(a, b)$.

Euklidischer Algorithmus (300 v. Chr.)

Algorithmus EUKLID

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

1. If $(b = 0)$ then return a;
2. Else return EUKLID$(b, a \bmod b)$

AUSGABE: $\mathrm{ggT}(a, b)$

Korrektheit:

- Schritt 1: $\mathrm{ggT}(a, 0) = a$. Schritt 2: folgt aus ggT-Satz.

Laufzeit:

- Für die Laufzeitanalyse benötigen wir die Fibonaccizahlen

$$F_0 := 0,\ F_1 := 1,\ F_i := F_{i-1} + F_{i-2} \text{ für } i \geq 2.$$

Laufzeit von EUKLID

Satz Laufzeit von EUKLID

Seien $a, b \in \mathbb{N}$ mit $a > b$. Sei k die Anzahl der Rekursionen von EUKLID(a, b). Dann gilt $a \geq F_{k+2}$ und $b \geq F_{k+1}$.

Beweis: per Induktion über k

- **IV** für $k = 1$: $b \geq 1 = F_2$ und $a > b$. D.h. $a \geq 2 = F_3$.
- **IS** $k - 1 \to k$: EUKLID(a, b) ruft EUKLID$(b, a \bmod b)$ auf.
- EUKLID$(b, a \bmod b)$ benötigt $k - 1$ Rekursionen, d.h. nach IA gilt
$$b \geq F_{k+1} \text{ und } (a \bmod b) \geq F_k.$$
- $b + (a \bmod b) = b + (a - \lfloor \frac{a}{b} \rfloor b) \leq a$, da $\lfloor \frac{a}{b} \rfloor \geq 1$ wegen $a > b$.
- Damit erhalten wir $a \geq b + (a \bmod b) \geq F_{k+1} + F_k = F_{k+2}$.

Logarithmische Laufzeit von EUKLID

Satz Laufzeit von EUKLID

Seien $a, b \in \mathbb{N}$ mit $a \geq F_{k+1} > b$. Dann benötigt EUKLID(a, b) Laufzeit $\mathcal{O}(\log^3 a)$.

Beweis:

- Wegen $b < F_{k+1}$ benötigt EUKLID weniger als k Rekursionen.
- Am Ende von Dima I: Herleitung expliziter Formel für F_k.
- Es gilt $F_k = \Omega(\phi^k)$, wobei $\phi = \frac{1+\sqrt{5}}{2}$ der goldene Schnitt ist.
- Daraus folgt $\phi^k = \mathcal{O}(F_k)$ bzw. $k = \mathcal{O}(\log F_k) = \mathcal{O}(\log a)$.
- D.h. EUKLID(a, b) benötigt weniger als $k = \mathcal{O}(\log a)$ Aufrufe.
- Multiplikation und Division mit Operanden der Bitlänge $\mathcal{O}(\log a)$ benötigen Zeit $\mathcal{O}(\log^2 a)$. D.h. die Gesamtlaufzeit ist $\mathcal{O}(\log^3 a)$.

Anmerkungen:

- Die Operanden in EUKLID werden sukzessive kleiner.
- Eine exakte Analyse liefert eine Schranke von $\mathcal{O}(\log^2 a)$.