

7.1 Bedeutung in der Informatik

Rechnen mit Kongruenzen ist u. A. wichtig für

- Suche von Datensätzen in großen Dateien (Hashing)
- Prüfziffern (ISBN, Barcodes)
- Kryptographie
- Generierung von Pseudozufallszahlen

7.2. Def.: Zwei ganze Zahlen a, b heißen kongruent modulo m , wenn $m \in \mathbb{N}$ ein Teiler von $a-b$ ist:

$$m \mid a-b$$

Wir schreiben $a \equiv b \pmod{m}$ und nennen m Modul.

7.3. Beispiele

a) $7 \equiv 22 \pmod{5}$, da $5 \mid 7-22$

b) $8 \not\equiv 22 \pmod{5}$, da $5 \nmid 8-22$

7.4. Satz (Zusammenhang Kongruenz - Division mit Rest)

Es gilt $a \equiv b \pmod{m}$ genau dann, wenn a und b bei Division durch m den selben Rest besitzen.

Beweis:

" \Rightarrow ": Sei $a \equiv b \pmod{m}$.

Seien ferner $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ mit

$$a = q_1 m + r_1$$

$$b = q_2 m + r_2$$

und $0 \leq r_1, r_2 < m$. (ex. nach 6.2).

$$\Rightarrow a - b = (q_1 - q_2)m + (r_1 - r_2)$$

Wegen $a \equiv b \pmod{m}$ gilt $m \mid a - b$

$$\Rightarrow r_1 - r_2 = 0 \quad \text{d.h.} \quad r_1 = r_2$$

" \Leftarrow " Seien umgekehrt

$$a = q_1 m + r$$

$$b = q_2 m + r$$

$$\Rightarrow a - b = (q_1 - q_2)m, \quad \text{d.h.} \quad m \mid a - b. \quad \square$$

7.5. Interpretation als Äquivalenzrelation

Kongruenz modulo m definiert eine Äquivalenzrelation (vgl. § 4) auf \mathbb{Z} , denn es gilt:

a) Reflexivität:

$$a \equiv a \pmod{m}, \quad \text{da} \quad m \mid 0$$

b) Symmetrie:

$$\begin{aligned} \text{Sei } a \equiv b \pmod{m} &\rightarrow m \mid a - b \\ &\Rightarrow m \mid b - a \quad \Rightarrow b \equiv a \pmod{m}. \end{aligned}$$

c) Transitivität:

Seien $a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$

$$\Rightarrow m \mid a - b \quad \text{und} \quad m \mid b - c$$

Mit 6.5.(c) folgt $m \mid (a - b) + (b - c)$, d.h. $m \mid a - c$

und somit $a \equiv c \pmod{m}$. □

7.6. Def.: Die Äquivalenzklassen

$$[b] := \{ a \in \mathbb{Z} \mid a \equiv b \pmod{m} \}$$

mit $b \in \{0, 1, \dots, m-1\}$ heißen Restklassen von \mathbb{Z} modulo m .

Wir schreiben

$$\mathbb{Z}_m := \{ [0], [1], \dots, [m-1] \}$$

für die Menge aller Restklassen von \mathbb{Z} modulo m .

Können wir in der m -elementigen Menge \mathbb{Z}_m ähnlich rechnen wie in \mathbb{Z} ?

7.7. Lemma (Addition von Elementen zweier Restklassen)

Seien $[a], [b] \in \mathbb{Z}_m$ und seien $a' \in [a]$ und $b' \in [b]$ beliebig. Dann ist $a' + b' \in [a+b]$.

Beweis:

Für $a' \in [a]$ und $b' \in [b]$ ex. $p, q \in \mathbb{Z}$ mit

$$a' - a = pm$$

$$b' - b = qm$$

$$\Rightarrow a' + b' = (pm + a) + (qm + b) = (p+q)m + (a+b)$$

$$\Rightarrow a' + b' \in [a+b]$$

□

Dieses Lemma motiviert

7.8. Def.: Seien $[a], [b] \in \mathbb{Z}_m$. Wir definieren die
(modulare) Addition von $[a]$ und $[b]$ durch

$$[a] + [b] := [a+b]$$

7.9. Beispiel: Additionstafel in \mathbb{Z}_6

+	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

denn es gilt z.B. $[3] + [5] = [8] = [2]$.

7.10. Satz (Eigenschaften der modularen Addition)

Die Addition in \mathbb{Z}_m hat folgende Eigenschaften

a) Kommutativgesetz:

$$[a] + [b] = [b] + [a] \quad \forall [a], [b] \in \mathbb{Z}_m$$

b) Assoziativgesetz:

$$([a] + [b]) + [c] = [a] + ([b] + [c]) \quad \forall [a], [b], [c] \in \mathbb{Z}_m$$

c) $[0]$ ist neutrales Element der Addition:

$$[a] + [0] = [a] \quad \forall a \in \mathbb{Z}_m$$

d) Inverses Element:

Zu jedem $[a] \in \mathbb{Z}_m$ ex. $[b] \in \mathbb{Z}_m$ mit

$$[a] + [b] = [0].$$

Beweis:

a) $[a] + [b] = [a+b] = [b+a] = [b] + [a]$

b)
$$\begin{aligned} ([a] + [b]) + [c] &= [a+b] + [c] \\ &= [a+b+c] \\ &= [a] + [b+c] \\ &= [a] + ([b] + [c]) \end{aligned}$$

c) $[a] + [0] = [a+0] = [a]$

d) Das inverse Element zu $[a]$ ist $[m-a]$, denn

$$[a] + [m-a] = [a+m-a] = [m] = [0]. \quad \square$$

Lässt sich auf ähnliche Weise auch eine Multiplikation einführen?

7.11. Lemma (Multiplikation von Elementen zweier Restklassen)

Seien $[a], [b] \in \mathbb{Z}_m$ und seien $a' \in [a], b' \in [b]$ beliebig. Dann ist $a' \cdot b' \in [a \cdot b]$.

Beweis:

Für $a' \in [a]$ und $b' \in [b]$ ex. $p, q \in \mathbb{Z}$ mit

$$a' - a = pm$$

$$b' - b = qm$$

$$\begin{aligned} \Rightarrow a' \cdot b' &= (pm + a) \cdot (qm + b) \\ &= pqm^2 + pmb + qma + ab \\ &= (pqm + pb + qa)m + ab \end{aligned}$$

$$\Rightarrow a' b' \equiv ab \pmod{m}, \text{ d.h. } a' b' \in [ab]. \quad \square$$

Dieses Lemma motiviert:

7.12. Def.: Seien $[a], [b] \in \mathbb{Z}_m$. Dann ist die

(modulare) Multiplikation von $[a]$ und $[b]$ durch

$$[a] \cdot [b] := [a \cdot b].$$

7.13. Beispiel: Multiplikationstafel in \mathbb{Z}_6

\cdot	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

denn es gilt z.B. $[2] \cdot [5] = [10] = [4]$

Beachte:

- Es kommen in A nicht alle Elemente in jeder Zeile / Spalte vor: Manche fehlen, andere treten mehrmals auf.
- Aus $[a] \cdot [b] = [0]$ folgt in A nicht $[a] = [0]$ oder $[b] = [0]$.

7.14. Satz (Eigenschaften der modularen Multiplikation)

Die Multiplikation in \mathbb{Z}_m hat folgende Eigenschaften:

a) Kommutativgesetz:

$$[a] \cdot [b] = [b] \cdot [a] \quad \forall [a], [b] \in \mathbb{Z}_m.$$

b) Assoziativgesetz:

$$([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c]) \quad \forall [a], [b], [c] \in \mathbb{Z}_m$$

c) $[1]$ ist neutrales Element der Multiplikation:

$$[1] \cdot [a] = [a] \quad \forall [a] \in \mathbb{Z}_m.$$

Beweis: ähnlich elementar wie Beweis von Satz 7.10. \square

7.15. Bemerkung

Offensichtlich findet man nicht zu jedem Element $[a] \in \mathbb{Z}_m - \{[0]\}$ ein inverses Element $[b]$ bzgl. der Multiplikation (d.h. $[a] \cdot [b] = [1]$):

Beispiel 7.13 zeigt, dass $[2], [3], [4]$ kein Inverses haben.

Kann man dies genauer verstehen?

7.

7.16. Satz (Multiplikative inverse Elemente in \mathbb{Z}_m)

$[a] \in \mathbb{Z}_m \setminus \{[0]\}$ hat genau dann ein inverses Element bzgl. der Multiplikation, wenn a und m teilerfremd sind (d.h. $\text{ggT}(a, m) = 1$).

Beweis:

" \Rightarrow " Sei $[b]$ ein multiplikatives Inverses zu $[a] \in \mathbb{Z}_m \setminus \{[0]\}$.

$\Rightarrow [1] = [a][b] = [a \cdot b]$

$\Rightarrow \exists q \in \mathbb{Z} : ab - 1 = qm \quad (*)$

Um zu zeigen, dass $\text{ggT}(a, m) = 1$, zeigen wir, dass für jeden Teiler c von a und m gilt: $c \mid 1$.

Für $c \mid a$ und $c \mid m$ folgt mit Satz 6.5.(c):

$c \mid ab - qm$

Wegen (*) bedeutet dies $c \mid 1$.

" \Leftarrow " siehe z.B. Bentelspacher / Zschneiguer:

Discrete Mathematik für Einsteiger, 2002 (Satz 5.3.4)

7.17.

□

Folgerung:

Falls p eine Primzahl ist, so ist p teilerfremd zu jedem $a \in \{1, 2, \dots, p-1\}$.

Somit hat jedes Element in $\mathbb{Z}_p \setminus \{[0]\} = \{[1], \dots, [p-1]\}$ ein multiplikatives Inverses.