§7: MODULARE ARITHMETIK

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 $a \equiv b \bmod m$ und nennen m Modul.

Bsp.: a) $7 \equiv 22 \bmod 5$, da $5 \mid 7-22$.

b) $8 \not\equiv 22 \bmod 5$, da $5 \nmid 8-22$.

7.3 Satz (Zusammenhang Kongruenz - Division mit Rest)

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

Beweis:

„⇒" Sei $a \equiv b \bmod m$

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 $0 \leq r_1, r_2 < m$.

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

Wegen $m \mid a-b$ ist $r_1 - r_2 = 0$, d.h. $r_1 = r_2$.

„⇐" Sei umgekehrt

$$a = q_1 m + r$$
$$b = q_2 m + r$$

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

7.4. Interpretation als Äquivalenzrelation

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

a) Reflexivität:

$a \equiv a \bmod m$, da $m \mid 0$.

c) Transitivität:

Sei $a \equiv b \bmod m$ und $b \equiv c \bmod m$.

$\Rightarrow \quad m \mid (a-b)$ und $m \mid (b-c)$

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

und somit $a \equiv c \bmod m$.

b) Symmetrie:

Sei $a \equiv b \bmod m \Rightarrow m \mid (a-b) \Rightarrow m \mid (b-a) \Rightarrow b \equiv a \bmod m$.

Die Äquivalenzklassen

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

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 modulo m.

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

7.5. Lemma (Addition von Elementen zweier Restklassen)

Seien $[a]$ und $[b]$ zwei Restklassen (modulo 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

$$a' - a = pm$$
$$b' - b = qm$$

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

d.h. $a'+b' \in [a+b]$. □

Dieses Lemma motiviert:

7.6. Def.: Seien $[a], [b]$ zwei Restklassen. Wir definieren die (modulare) Addition von $[a]$ und $[b]$ durch

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

7.7. 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. $[3]+[5] = [8] = [2]$.

7.8. Satz (Eigenschaften der modularen Addition)

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

a) Kommutativgesetz:

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

b) Assoziativgesetz:

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

c) [0] ist neutrales Element der Addition:

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

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) $([a]+[b])+[c] = [a+b]+[c]$
$= [a+b+c]$
$= [a]+[b+c]$
$= [a]+([b]+[c])$.

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

d) Das inverse Element zu $[a]$ ist $[m-a]$, denn:
$[a]+[m-a] = [a+m-a] = [m] = [0]$. □.

7.9. Lemma (Multiplikation von Elementen zweier Restklassen)

Seien $[a]$ und $[b]$ zwei Restklassen (mod. 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

$a' - a = pm$
$b' - b = qm$

$\Rightarrow a' \cdot b' = (pm+a)(qm+b)$
$= pqm^2 + pmb + qma + ab$
$= (pqm + pb + qa)m + ab$

$\Rightarrow a'b' \equiv ab \bmod m$, d.h. $a'b' \in [ab]$ □.

Dieses Lemma motiviert:

7.10. Def.: Seien $[a], [b]$ zwei Restklassen. Wir definieren die (modulare) Multiplikation von $[a]$ und $[b]$ durch

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

7.11 Beispiel: Multiplikationstafel in $\mathbb{Z}_6$:

·	[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:

a) Es kommen i.A. nicht alle Elemente in jeder Zeile / Spalte vor: Manche fehlen, andere kommen mehrfach vor.

b) Aus $[a]\cdot[b] = [0]$ folgt i.A. nicht: $[a] = [0]$ oder $[b] = [0]$.

7.12. Satz (Eigenschaften der modularen Multiplikation)

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

a) Kommutativgesetz:
$$[a]\cdot[b] = [b]\cdot[a] \qquad \forall\, [a],[b] \in \mathbb{Z}_m$$

b) Assoziativgesetz:
$$([a]\cdot[b])\cdot[c] = [a]\cdot([b]\cdot[c]) \qquad \forall\, [a],[b],[c] \in \mathbb{Z}_m.$$

c) [1] ist neutrales Element der Multiplikation:
$$[1]\cdot[a] = [a] \qquad \forall\, [a] \in \mathbb{Z}_m$$

Beweis: Ähnlich elementar wie Beweis von Satz 7.8. □

Bem.: Offensichtlich findet man nicht zu jedem Element $[a] \in \mathbb{Z}_m \setminus \{[0]\}$ ein inverses Element $[b]$ bzgl. der Multiplikation (d.h. $[a] \cdot [b] = [1]$): Beispiel 7.11 zeigt, dass $[2], [3], [4]$ kein Inverses haben.

7.13 Satz (Multiplikative inverse Elemente in $\mathbb{Z}_m$)

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

Beweis:

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

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

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

Um zu zeigen, dass $ggT(a, m) = 1$, 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. Beutelspacher / Zschiegner: Diskrete Math. für Einsteiger, 2002 (Satz 5.3.4) $\square$