Äquivalenzrelationen und modulo-Rechnung

(Äquivalenz-)Relationen

Eine (binäre/zweistellige) **Relation** zwischen zwei Mengen A und B ist eine Teilmenge des kartesischen Produkts $R \subset A \times B$. Im Fall $A = B$ spricht man von einer Relation auf A.

Stehen $a \in A$ und $b \in B$ in Relation zueinander, so ist $(a, b) \in R$.

Eine Relation auf A heißt **Äquivalenzrelation**, wenn sie für alle $a, b, c \in A$ folgenden Eigenschaften besitzt:

- Reflexitivät: $(a, a) \in R$
- Symmetrie: $(a, b) \in R \Rightarrow (b, a) \in R$
- Transitivität: $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$

Ist R eine Äquivalenzrelation auf A, so ist für jedes Element $a \in A$ die zugehörige **Äquivalenzklasse**:

$$[a] := \{b \in A : (a, b) \in R\}$$

- $[a]$ besteht aus genau den Elementen, die in Relation zu a stehen.
- a heißt Vertreter der Äquivalenzklasse $[a]$.
- Sind $[a]$ und $[b]$ zwei Äquivalenzklassen, so ist entweder $[a] = [b]$ oder $[a] \cap [b] = \emptyset$.

Division mit Rest

Jede ganze Zahl a kann mit Rest durch eine ganze Zahl b geteilt werden, d.h. es gibt eindeutige ganze Zahlen m und r, sodass

$$a = m \cdot b + r$$

mit $0 \leq r < |b|$. r heißt Rest der Division.

- Ist $r = 0$, so teilt b die Zahl a. Man schreibt $b \mid a$, andernfalls $b \nmid a$.
- Es gilt $b \mid (a - r)$.

Der größte gemeinsame Teiler

Der größte gemeinsame Teiler zweier Zahlen $a, b \in \mathbb{Z}$, geschrieben: $\mathrm{ggT}(a, b)$, ist die größte natürliche Zahl, die a und b teilt.

- Berechnung: Euklidischen Algorithmus.
- a und b heißen teilerfremd, wenn $\mathrm{ggT}(a, b) = 1$.
- Satz von Bézout: Es gibt zwei Zahlen $s, t \in \mathbb{Z}$, sodass
$$s \cdot a + t \cdot b = \mathrm{ggT}(a, b).$$
Berechnung: Erweiterter Euklid. Algorithmus.

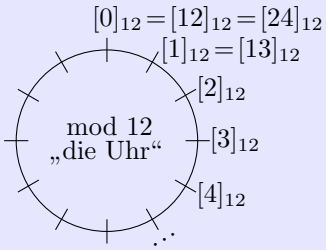
Modulo-Rechnung

Äquivalenz „modulo m“ ist eine Äquivalenzrelation. Die Äquivalenzklassen sind diejenigen Zahlen, welche bei Division durch m den selben Rest haben.

$a \equiv b \mod m$ heißt: $m \mid (a - b)$.

Die Äquivalenzklassen haben also die Gestalt

$$[a]_m = \{b \in \mathbb{Z} : a \equiv b \mod m\}.$$



Rechenregeln:

- $[a]_m + [b]_m = [a + b]_m$.
- $[a]_m \cdot [b]_m = [a \cdot b]_m$.

Für gegebene $a, b \in \mathbb{Z}$, kann die Gleichung

$$a \cdot x \equiv b \mod m$$

mithilfe des erweiterten Euklidischen Algorithmus gelöst werden.

(Erweiterter) Euklidischer Algorithmus

Euklidischer Algorithmus

Gegeben: $a, b \in \mathbb{Z}$.
Wiederholtes Ausführen der Division mit Rest liefert den $\mathrm{ggT}(a, b)$ als letzten Rest $\neq 0$ (hier: r_k).

$$\begin{aligned}
a &= m_1 \cdot b + r_1 \\
b &= m_2 \cdot r_1 + r_2 \\
r_1 &= m_3 \cdot r_2 + r_3 \\
&\vdots \\
r_{k-2} &= m_k \cdot r_{k-1} + r_k \\
r_{k-1} &= m_{k+1} \cdot r_k + 0
\end{aligned}$$

Erweiterter Euklid. Alg.

Gegeben: $a, b \in \mathbb{Z}$.
„Rückwärtsausführen“ des Euklidischen Algorithmus liefert $s, t \in \mathbb{Z}$ für $\mathrm{ggT}(a, b) = s \cdot a + t \cdot b$.

Löse die vorletzte Gleichung nach r_k $(= \mathrm{ggT}(a, b))$ auf und ersetze von unten nach oben die Reste $r_{k-1}, r_{k-2}, \ldots, r_2, r_1$.

Aufgaben

Äquivalenzrelationen

Aufgabe 1. Welche der folgenden Relationen R ist auf der jeweils angegebenen Menge eine Äquivelanzrelation? Bestimmen Sie ggf. alle Äquivalenzklassen.

a) $\mathbb{R}$, mit $(a,b) \in R \Leftrightarrow a+b$ ist gerade.
b) $\mathbb{R}$, mit $(a,b) \in R \Leftrightarrow a \cdot b > 0$.
c) $\mathbb{R} \setminus \{0\}$, mit $(a,b) \in R \Leftrightarrow a|b$.
d) $\mathbb{R}$, mit $(a,b) \in R \Leftrightarrow a \cdot b$ ist gerade.

Der größte gemeinsame Teiler

Aufgabe 2. Berechnen Sie den größten gemeinsamen Teiler der folgenden Zahlen

a) 123 und 46 b) 7468 und 2464 c) 55 und 34

Aufgabe 3. Beweisen Sie, dass für alle $a, b, c \in \mathbb{Z}$ gilt:

$$\mathrm{ggT}(\mathrm{ggT}(a,b),c) = \mathrm{ggT}(a,\mathrm{ggT}(b,c)).$$

Modulo-Rechnung

Aufgabe 4. Berechnen Sie und geben Sie den kleinsten nichtnegativen Vertreter der jeweiligen Äquivalenzklasse an.

a) $[7]_{12} + [13]_{12}$.
b) $[1]_{12} - [5]_{12}$
c) $[11]_{12} \cdot [24]_{12}$
d) $[-6]_{12} \cdot [17]_{12}$

Aufgabe 5. Es seien $A, B \in \{1, \ldots, 9\}$ und es sei $C = ABABAB$ (die Zahl mit den Ziffern A,B,A,...). Beweisen Sie mithilfe von Modulo-Rechnung, dass C durch 7 teilbar ist.

Aufgabe 6. Finden Sie das multiplikative Inverse zu 15 modulo 17, d.h. lösen Sie die Gleichung

$$15x \equiv 1 \mod 17.$$

Aufgabe 7. Lösen Sie die Gleichung $15x \equiv 6 \mod 21$.

Aufgabe 8. Es sei p eine Primzahl. Beweisen Sie für $a, b \in \mathbb{Z}$:

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Hinweis: Binomischer Lehrsatz.

(Erweiterter) Euklidischer Algorithmus

Aufgabe 9. Finden Sie ganze Zahlen s und t, sodass

$$123 \cdot s + 46 \cdot t = \mathrm{ggT}(123, 46).$$

Wie lauten die Zahlen $\overline{s}$ und $\overline{t}$, sodass

$$123 \cdot \overline{s} + 46 \cdot \overline{t} = 7?$$