Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Übungen zur Grundlagen der Mathematik im Wintersemester 2019/2020, Blatt 14
Fachbereich Mathematik, Stefan Geschke

A: Präsenzaufgaben am 27. Januar 2020

1. Sei $m \in \mathbb{N} \setminus \{1\}$ und $a \in \mathbb{Z} \setminus \{0\}$. Zeigen Sie, dass $[a]_m$ genau dann ein multiplikatives Inverses in $\mathbb{Z}_m$ besitzt, wenn a und m teilerfremd sind, also wenn $\mathrm{ggT}(a, m) = 1$ gilt.

   Lösung. Angenommen a und m haben einen gemeinsamen Teiler $n > 1$. Wir setzen $k = \frac{m}{n}$. Dann ist $a \cdot k$ ein gemeinsames Vielfaches von m und a. Damit gilt $[a]_m \cdot [k]_m = [a \cdot k]_m = [0]_m$. Wäre $[a]_m$ in $\mathbb{Z}_m$ invertierbar, so könnten wir die Gleichung $[a]_m \cdot [k]_m = [0]_m$ mit dem Inversen von $[a]_m$ multiplizieren und erhielten $[k]_m = [0]_m$, was aber nicht sein kann, da k kein Vielfaches von m ist.

   Ist umgekehrt $\mathrm{ggT}(a, m) = 1$, so existieren $x, y \in \mathbb{Z}$ mit $1 = ax + my$. Auf beiden Seiten der Gleichung bilden wir die Restklassen modulo m und erhalten $[1]_m = [a]_m \cdot [x]_m + [m]_m \cdot [y]_m$, also $[a]_m \cdot [x]_m = [1]_m$. Damit ist $[x]_m$ zu $[a]_m$ invers.

2. Stelle fest, ob $[7]_{60}$ in $\mathbb{Z}_{60}$ bezüglich der Multiplikation invertierbar ist. Falls ja, bestimme das Inverse.

   Lösung. Wir führen den euklischen Algorithmus mit 7 und 60 durch. Es gilt

   $$\begin{aligned} 60 &= 8 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

   Rückwärtseinsetzen liefert

   $$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (60 - 8 \cdot 7) - 7 = 2 \cdot 60 - 17 \cdot 7.$$

   Damit ist $[-17]_{60} = [43]_{60}$ das multiplikative Inverse von $[7]_{60}$ in $\mathbb{Z}/60\mathbb{Z}$.

3. Auf der Menge $Q = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ haben wir die Äquivalenzrelation $\sim$ durch

   $$(a, b) \sim (c, d) \quad \Leftrightarrow \quad ad = cb$$

   definiert. Auf dem Quotienten $\mathbb{Q} = Q/\sim$ hatten wir dann die Multplikation durch

   $$[(a, b)]_\sim \cdot [(c, d)]_\sim = [(ac, bd)]_\sim$$

   definiert. Zeigen sie, dass die Multiplikation auf $\mathbb{Q}$ wohldefiniert ist, d.h., unabhängig von der Wahl der Repräsentanten der Äquivalenzklassen.

   Lösung. Seien $a, a', c, c' \in \mathbb{Z}$ und $b, b', d, d' \in \mathbb{N}$ mit $(a, b) = (a', b')$ und $(c, d) \sim (c'd')$. Dann gilt $ab' = a'b$ und $cd' = c'd$.

   Es ist zu zeigen, dass $(ac, bd) \sim (a'c', b'd')$ gilt, also $acb'd' = a'b'cd$. Das folgt aber sofort aus den Gleichungen $ab' = a'b$ und $cd' = c'd$.