Lineare Algebra I
5. Tutorium
Die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. Kollross
Dr. Le Roux
Dipl.-Math. Susanne Kürsten

WS 2010/2011
19. November 2010

Aufgaben

In diesem Tutrorium soll es um die Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ und den Umgang mit ihnen gehen.
Um in einer ersten Schreibweise angeben zu können, was $\mathbb{Z}/n\mathbb{Z}$ ist, benötigt man die folgende Definition von Resten.
Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ für die

$$a = q \cdot n + r \text{ und } 0 \leq r < n$$

gilt. Die Zahl r heißt dann Rest von a bei der Dividion durch n oder auch Rest von a modulo n.

Aufgabe G1 (Beispiele und Nullteiler)
Wir betrachten die Menge $\mathbb{Z}/n\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Dabei sei n eine natürliche Zahl. Für zwei Elemente $\overline{a}$ und $\overline{b}$ aus $\mathbb{Z}/n\mathbb{Z}$ wird wie folgt eine Multiplikation und eine Addition definiert:

$$\begin{aligned} \overline{a} +_n \overline{b} &:= \overline{r}, && \text{wobei } r \text{ der Rest von } a+b \text{ bei der Division durch } n \text{ ist,} \\ \overline{a} \cdot_n \overline{b} &:= \overline{r}, && \text{wobei } r \text{ der Rest von } a \cdot b \text{ bei der Division durch } n \text{ ist.} \end{aligned}$$

(a) Stellen Sie die Additions und Multiplikationstabellen für $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ auf.

(b) Welche Elemente der Mengen aus Aufgabenteil (a) haben Inverse bezüglich der Multiplikation, geben Sie diese Inversen Elemente an.
In Aufgabe G2 wird gezeigt, dass $\left(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n, \overline{0}, \overline{1}\right)$ für alle natürlichen Zahlen $n \geq 2$ ein Ring mit Eins ist. Wenn Sie dies vorraussetzen, welche der Ringe aus Aufgabenteil (a) sind dann Körper und warum?

(c) Welche der Ringe aus Aufgabenteil (a) haben Nullteiler? Geben Sie alle Nullteiler an.

(d) Für welche natürlichen Zahlen n besitzt $\mathbb{Z}/n\mathbb{Z}$ Nullteiler? Kann in diesem Fall $\mathbb{Z}/n\mathbb{Z}$ ein Körper sein?

Lösung:

(a) In $\mathbb{Z}/4\mathbb{Z}$ gilt:

$+_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

In $\mathbb{Z}/5\mathbb{Z}$ gilt:

$+_5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot_5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

In $\mathbb{Z}/6\mathbb{Z}$ gilt:

$+_6$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot_6$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(b) Die Inversen kann man an den Multiplikationstabellen ablesen:

In $\mathbb{Z}/4\mathbb{Z}$ ist $\overline{1}^{-1} = \overline{1}$ und $\overline{3}^{-1} = \overline{3}$. Die Elemente $\overline{0}$ und $\overline{2}$ haben keine Inversen.

In $\mathbb{Z}/5\mathbb{Z}$ ist $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$ und $\overline{4}^{-1} = \overline{4}$. Das Element $\overline{0}$ hat kein Inverses.

In $\mathbb{Z}/6\mathbb{Z}$ ist $\overline{1}^{-1} = \overline{1}$ und $\overline{5}^{-1} = \overline{5}$. Die Elemente $\overline{0}$, $\overline{2}$, $\overline{3}$ und $\overline{4}$ haben keine Inversen.

Bemerkung: Einige dieser Aussagen gelten immer. So hat die Null in einem Ring nie ein Inverses Element, die Eins ist immer zu sich selbst invers und wenn $a^{-1} = b$ gilt, dann ist auch $b^{-1} = a$.

Damit ein Ring mit Eins ein Körper ist, muss die Multiplikation kommutativ sein und jedes Element außer der Null muss ein Inverses besitzen.

In allen drei Ringen aus Aufgabenteil (a) ist die Multiplikation kommutativ. Dies sieht man an der Symmetrie der Multiplikationstabellen.

In $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ haben nicht alle von Null verschiedenen Elemente ein Inverses. In $\mathbb{Z}/5\mathbb{Z}$ haben alle von Null verschiedenen Elemente ein Inverses.

Also ist $\mathbb{Z}/5\mathbb{Z}$ ein Körper, während $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ keine Körper sind.

(c) Die Ringe $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/6\mathbb{Z}$ haben Nullteiler. In $\mathbb{Z}/4\mathbb{Z}$ ist der einzige Nullteiler $\overline{2}$. In $\mathbb{Z}/6\mathbb{Z}$ sind die Nullteiler $\overline{2}$, $\overline{3}$ und $\overline{4}$.

(d) $\mathbb{Z}/n\mathbb{Z}$ hat genau dann Nullteiler, wenn n keine Primzahl ist.

Beweis: Es gilt für jedes Element $\overline{a} \in \mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}$: $\overline{a}$ ist Nullteiler $\Leftrightarrow$ Es existiert ein $\overline{b} \in \mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}$ mit $\overline{a} \cdot \overline{b} = 0$.

Außerdem gilt für $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}$:

$\overline{a} \cdot \overline{b} = 0 \Leftrightarrow a \cdot b$ lässt bei der Division durch n den Rest Null $\Leftrightarrow a \cdot b$ ist ein Vielfaches von n.

Wenn n keine Primzahl ist, also einen Teiler t hat, der nicht gleich Eins oder n ist, so erfüllt $a = t, b = \frac{n}{t}$ die letzte Bedingung und wegen der obigen Äquivalenzen hat dann $\mathbb{Z}/n\mathbb{Z}$ Nullteiler.

Ist n eine Primzahl, die $a \cdot b$ teilt, dann muss n entweder a oder b teilen (dies gilt wegen der Eindeutigkeit der Primzahlzerlegung in den natürlichen Zahlen und sollte bekannt sein). Das ist aber nicht möglich, da $a, b \in \{1, \ldots, n-1\}$ sind. D.h. wegen der obigen Äquivalenzen hat $\mathbb{Z}/n\mathbb{Z}$ in diesem Fall keine Nullteiler.

w.z.b.w.

Aus der Vorlesung ist bekannt, dass ein Körper keine Nullteiler besitzt. Wenn n keine Primzahl ist, kann also $\mathbb{Z}/n\mathbb{Z}$ kein Körper sein.

Aufgabe G2 (Restklassen und die Ringeigenschaft von $\mathbb{Z}/n\mathbb{Z}$)
Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$.
Man sagt a ist kongruent zu b modulo n und schreibt $a \equiv b \pmod{n}$, wenn a und b bei der Division durch n denselben Rest lassen.

(a) Zeige, dass die Relation $\equiv_n \subseteq \mathbb{Z} \times \mathbb{Z}$, die gegeben ist durch $(a, b) \in \equiv_n \Leftrightarrow a \equiv b \pmod{n}$ eine Äquivalenzrelation (siehe Tutoriumsblatt 1) ist.

(b) Zeige, dass die Äquivalenzklasse $\overline{a}$ dieser Relation, welche das Element a enthält die Gestalt

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\} =: a + n\mathbb{Z}$$

hat. Wie viele verschiedene solcher Äquivalenzklassen gibt es? Wann gilt $\overline{a} = \overline{b}$?

Diese Äquivalenzklassen heißen auch Restklassen modulo n. Sie bilden, wie bereits aus dem ersten Tutorium bekannt ist eine Partition von $\mathbb{Z}$. Betrachtet man die Restklasse $\overline{a}$, so wird a als Repräsentant von $\overline{a}$ bezeichnet.
Man kann nun $\mathbb{Z}/n\mathbb{Z}$ als die Menge der Restklassen modulo n mit den Operationen

$$+_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad (a + n\mathbb{Z}, b + n\mathbb{Z}) \mapsto a + b + n\mathbb{Z} \text{ und}$$
$$\cdot_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad (a + n\mathbb{Z}, b + n\mathbb{Z}) \mapsto a \cdot b + n\mathbb{Z}$$

definieren. (Dabei bezeichnen $a + b$ und $a \cdot b$ die normale Addition bzw. Multiplikation in den ganzen Zahlen.)

(c) Zeigen Sie, dass diese Operationen wohldefiniert sind.
Wohldefiniert bedeutet hier: Das Ergebnis der Multiplikation und Addition in $\mathbb{Z}/n\mathbb{Z}$ hängt nicht von der Wahl der Repräsentanten ab.

(d) Zeigen Sie, dass diese Definition mit der aus Aufgabe G1 übereinstimmt.

(e) Für welche natürlichen Zahlen n stimmt in $\mathbb{Z}/n\mathbb{Z}$ das Nullelement mit dem Einselement überein?

(f) Zeigen Sie, dass $(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n, 0+n\mathbb{Z}, 1+n\mathbb{Z})$ für jede natürliche Zahl $n \geq 2$ ein kommutativer Ring mit Eins ist.

Lösung:

(a) Man muss zeigen, dass $\equiv_n$ reflexiv, symmetrisch und transitiv ist. Seien dazu $a, b, c \in \mathbb{Z}$ beliebig.
a lässt bei der Division durch n denselben Rest wie a, es gilt also $a \equiv a \pmod{n}$ und $a \equiv_n a$. Somit ist $\equiv_n$ reflexiv.
Wenn $a \equiv_n b$ gilt dann folgt $a \equiv b \pmod{n}$, also haben a und b denselben Rest bei der Division durch n und es gilt nach Definition auch $b \equiv a \pmod{n}$ und damit $b \equiv_n a$. Insgesamt ist also $\equiv_n$ symmetrisch.
Wenn $a \equiv_n b$ und $b \equiv_n c$ gilt, bedeutet das $a \equiv b \pmod{n}$ und $b \equiv c \pmod{n}$. D.h. sowohl a und b als auch b und c lassen bei der Division durch n denselben Rest. Also haben alle drei Zahlen a, b und c denselben Rest bei der Division durch n. Insbesondere gilt also auch $a \equiv c \pmod{n}$ und $a \equiv_n c$. D.h. die Relation $\equiv_n$ ist transitiv.

w.z.b.w.

(b) Durch die Definition von Äquivalenzklassen und einfache Umformungen erhält man

$$\begin{aligned}
\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv_n b\} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} \\
&= \{b \in \mathbb{Z} \mid a \text{ und } b \text{ lassen denselben Rest bei der Division durch } n\} \\
&= \{b \in \mathbb{Z} \mid \exists\, q_1, q_2, r \in \mathbb{Z} \text{ mit } a = q_1 \cdot n + r, b = q_2 \cdot n + r \text{ und } 0 \leq r < n\} \\
&\subseteq \{b \in \mathbb{Z} \mid \exists\, q_1, q_2 \in \mathbb{Z} \text{ mit } b - a = (q_2 - q_1) \cdot n\} \subseteq \{b \in \mathbb{Z} \mid \exists\, k \in \mathbb{Z} \text{ mit } b = a + k \cdot n\} \\
&= \{a + kn \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}\,.
\end{aligned}$$

Andererseits: Wenn $a = q_1 \cdot n + r$ mit $q_1, r \in \mathbb{Z}, 0 \leq r < n$ und $b \in a + n\mathbb{Z}$ gilt, dann gibt es ein $k \in \mathbb{Z}$ mit $b = a + k \cdot n = (q_1 + k) \cdot n + r$. Somit haben a und b denselben Rest r bei der Division durch n, also ist $a \equiv_n b$, d.h. $b \in \overline{a}$.
In Mengenschreibweise bedeutet das $a + n\mathbb{Z} \subseteq \overline{a}$. Insgesamt folgt also die Gleichheit der beiden Mengen.

w.z.b.w.

Man sieht leicht, dass es n Restklassen gibt. Eine mögliche Darstellung wäre $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \ldots, \overline{n-1}\}$.
Es ist $\overline{a} = \overline{b} \Leftrightarrow b \in \overline{a} \Leftrightarrow \exists\, k \in \mathbb{Z}$ mit $b = a + k \cdot n \Leftrightarrow \exists\, k \in \mathbb{Z}$ mit $b - a = k \cdot n \Leftrightarrow n$ teilt $b - a$.

(c) Seien $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ mit $a_1 + n\mathbb{Z} = a_2 + n\mathbb{Z}$ und $b_1 + n\mathbb{Z} = b_2 + n\mathbb{Z}$. Man muss nun zeigen, dass

$$a_1 + b_1 + n\mathbb{Z} = a_2 + b_2 + n\mathbb{Z} \text{ und } a_1 \cdot b_1 + n\mathbb{Z} = a_2 \cdot b_2 + n\mathbb{Z} \text{ gilt.}$$

Aus den Voraussetzungen für a_1, a_2, b_1 und b_2 zusammen mit den Äquivalenzen am Ende von Aufgabenteil (b) folgt die Existenz von zwei natürlichen Zahlen k_1 und k_2 mit $a_1 - a_2 = k_1 \cdot n$ und $b_1 - b_2 = k_2 \cdot n$. Daraus ergibt sich

$$\begin{aligned}
(a_1 + b_1) - (a_2 + b_2) &= (a_1 - a_2) + (b_1 - b_2) = (k_1 + k_2) \cdot n \text{ und} \\
(a_1 \cdot b_1) - (a_2 \cdot b_2) &= a_1 \cdot b_1 - a_1 \cdot b_2 + a_1 \cdot b_2 - a_2 \cdot b_2 = a_1 \cdot (b_1 - b_2) + (a_1 - a_2) \cdot b_2 = (a_1 \cdot k_2 + k_1 \cdot b_2) \cdot n.
\end{aligned}$$

Wegen $(k_1 + k_2), (a_1 \cdot k_2 + k_1 \cdot b_2) \in \mathbb{Z}$ und den Äquivalenzen am Ende von Aufgabenteil (b) folgen hieraus die Behauptungen $a_1 + b_1 + n\mathbb{Z} = a_2 + b_2 + n\mathbb{Z}$ und $a_1 \cdot b_1 + n\mathbb{Z} = a_2 \cdot b_2 + n\mathbb{Z}$.

w.z.b.w.

(d) Man wählt als Repräsentanten die natürlichen Zahlen von 0 bis $n-1$, dann erhält man die Darstellung in Aufgabe G1. Zusätzlich muss überprüft werden, ob die Definitionen von Addition und Subtraktion übereinstimmen. Seien $a, b \in \{0, \ldots, n-1\}$ und r der Rest von $a + b$ bei der Division durch n. Dann ist nach der Definition in Aufgabe G1 $\overline{a} +_n \overline{b} = \overline{r}$ und nach der in dieser Aufgabe ist $\overline{a} +_n \overline{b} = \overline{a + b} = a + b + n\mathbb{Z} = r + n\mathbb{Z} = \overline{r}$. Für die Multiplikation funktioniert das analog.
Die beiden Definitionen stimmen also überein.

(e) Nur für $n = 1$ gilt n teilt $1 - 0$. Somit ist $\overline{0} = \overline{1}$ in $\mathbb{Z}/n\mathbb{Z}$ genau dann, wenn $n = 1$ ist.

(f) Nach Aufgabenteil (e) sind in diesen Mengen Eins und Null verschieden.
Alle anderen Ringeigenschaften ergeben sich direkt aus den bekannten Ringeigenschaften der ganzen Zahlen.
Die Assoziativität der Multiplikation ergibt sich beispielsweise wie folgt. Für alle $a, b, c \in \mathbb{Z}$ gilt

$$\overline{a} \cdot_n (\overline{b} \cdot_n \overline{c}) = \overline{a} \cdot_n \overline{b \cdot c} = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c} = \overline{a \cdot b} \cdot_n \overline{c} = (\overline{a} \cdot_n \overline{b}) \cdot_n \overline{c}$$

Aufgabe G3 (Der größte gemeinsame Teiler und die Körpereigenschaft von $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p)
In der ganzen Aufgabe sei $n \geq 2$ eine natürliche Zahl.
Außerdem seien jetzt a und b natürliche Zahlen. Der größte gemeinsame Teiler von a und b wird mit Hilfe des euklidischen Algorithmus bestimmt. Bei diesem macht man im ersten Schritt eine Division mit Rest von a durch b. Der Rest sei r_1. Im nächsten Schritt macht man dasselbe mit b und r_1. Dies wird fortgeführt, bis ein Rest r_k Null ist. Dann gilt $\mathrm{ggT}(a, b) = r_{k-1}$.
Der allgemeine Verlauf des Euklidischen Algorithmus sieht also wie folgt aus.

$$\begin{aligned}
a &= q_1 \cdot b + r_1 \text{ mit } 0 \leq r_1 < b \\
b &= q_2 \cdot r_1 + r_2 \text{ mit } 0 \leq r_2 < r_1 \\
r_1 &= q_3 \cdot r_2 + r_3 \text{ mit } 0 \leq r_3 < r_2 \\
\vdots &\ \vdots\ \vdots \\
r_{k-4} &= q_{k-2} \cdot r_{k-3} + r_{k-2} \text{ mit } 0 \leq r_{k-2} < r_{k-3} \\
r_{k-3} &= q_{k-1} \cdot r_{k-2} + r_{k-1} \text{ mit } 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &= q_k \cdot r_{k-1} + 0
\end{aligned}$$

Dabei sind alle vorkommenden Zahlen natürliche Zahlen und man erhält $\mathrm{ggT}(a, b) = r_{k-1}$.

(a) Bestimmen sie mit Hilfe des Euklidischen Algorithmus $\mathrm{ggT}(99, 78)$ und $\mathrm{ggT}(34357, 17017)$.

(b) Zeigen Sie, dass der beschriebene Euklidische Algorithmus immer endet.

(c) Zeigen Sie, dass der beschriebene Euklidische Algorithmus tatsächlich den größten gemeinsamen Teiler der beiden gegebenen Zahlen bestimmt.

Es gilt der Satz: Für $a, b, d \in \mathbb{N}$ mit $d = \mathrm{ggT}(a, b)$ existieren immer ganze Zahlen x und y mit

$$d = ax + by\ .$$

Die Zahlen x und y können dabei aus dem Euklidischen Algorithmus durch Rückwärtseinsetzen bestimmt werden. Mit den obigen Bezeichnungen hat man

$$\begin{aligned}
d &= r_{k-1} = r_{k-3} - q_{k-1} r_{k-2} = x_1 r_{k-3} + y_1 r_{k-2} \text{ mit } x_1 := 1, y_1 := -q_{k-1} \\
d &= x_1 r_{k-3} + y_1 (r_{k-4} - q_{k-2} r_{k-3}) = x_2 r_{k-4} + y_2 r_{k-3} \text{ mit } x_2 := y_1, y_2 := x_1 - y_1 q_{k-2} \text{ usw.}
\end{aligned}$$

Es ergibt sich also eine Gleichungskette

$$d = x_1 r_{k-3} + y_1 r_{k-2} = x_2 r_{k-4} + y_2 r_{k-3} = \cdots = x_{k-2} b + y_{k-2} r_1 = x_{k-1} a + y_{k-1} b,$$

wobei alle vorkommenden Zahlen ganze Zahlen und x_{k-1}, y_{k-1} die gesuchten Zahlen sind.
Auf diese Weise zeigt man den obigen Satz und kann im konkreten Beispiel die Zahlen x und y bestimmen.

(d) Bestimmen Sie auf die gerade beschriebene Weise ganze Zahlen x und y mit $\mathrm{ggT}(99, 78) = 99x + 78y$.

(e) Bestimmen Sie ganze Zahlen x und y mit $\mathrm{ggT}(34357, 17017) = 34357x + 17017y$.

(f) Sei $(\mathbb{Z}/n\mathbb{Z})^\times$ die Menge der bezüglich der Multiplikation invertierbaren Elemente in $(\mathbb{Z}/n\mathbb{Z})$. Zeigen Sie

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \,|\, \mathrm{ggT}(a, n) = 1\}\ .$$

Tipp: Zeigen Sie als ersten Schritt, dass ein Element $\overline{a}$ von $\mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar ist, wenn es ganze Zahlen x und y gibt für die $ax + ny = 1$ gilt.

(g) Für welche n ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper?

Lösung:

(a) Im ersten Fall ergibt der euklidische Algorithmus

$$\begin{array}{rcrcrcr} 99 & = & 1 & \cdot & 78 & + & 21 \\ 78 & = & 3 & \cdot & 21 & + & 15 \\ 21 & = & 1 & \cdot & 15 & + & 6 \\ 15 & = & 2 & \cdot & 6 & + & 3 \\ 6 & = & 2 & \cdot & 3 & + & 0\,. \end{array}$$

Es gilt also $\mathrm{ggT}(99,78)=3$.

Für die zweite Aufgabe ergibt der Euklidische Algorithmus

$$\begin{array}{rcrcrcr} 34357 & = & 2 & \cdot & 17017 & + & 323 \\ 17017 & = & 52 & \cdot & 323 & + & 221 \\ 323 & = & 1 & \cdot & 221 & + & 102 \\ 221 & = & 2 & \cdot & 102 & + & 17 \\ 102 & = & 6 & \cdot & 17 & + & 0\,. \end{array}$$

Es ist also $\mathrm{ggT}(34357,17017)=17$.

(b) Wegen der Bedingung $0 \le r_{i+1} < r_i$ (für $i \in \mathbb{N}$) wird der berechnete Rest in jedem Schritt mindestens im Eins kleiner, aber nie kleiner als Null. D.h. nach spätestens r_1+1 Schritten muss der Rest Null sein und der Algorithmus bricht ab.

(c) An der ersten Zeile des euklidischen Algorithmus

$$a = q_1 \cdot b + r_1 \text{ mit } 0 \le r_1 < b$$

sieht man:

Haben a und b einen gemeinsamen Teiler t, so teilt t auch r_1 und

haben b und r_1 einen gemeinsamen Teiler t, so teilt t auch a.

Da dies für jeden Teiler gilt ergibt sich sofort $\mathrm{ggT}(a,b)=\mathrm{ggT}(b,r_1)$.

Auf analoge Weise ergibt sich mit Hilfe der zweiten Zeile des euklidischen Algorithmus $\mathrm{ggT}(b,r_1)=\mathrm{ggT}(r_1,r_2)$. Indem man dies Zeilenweise fortführt erhält man die Gleichungskette

$$\mathrm{ggT}(a,b)=\mathrm{ggT}(b,r_1)=\mathrm{ggT}(r_1,r_2)=\cdots=\mathrm{ggT}(r_{k-3},r_{k-2})=\mathrm{ggT}(r_{k-2},r_{k-1})\,.$$

An der letzten Zeile des euklidischen Algorithmus kann man ablesen, dass r_{k-1} eine Teiler von r_{k-2} ist. Das bedeutet es gilt $\mathrm{ggT}(r_{k-2},r_{k-1})=r_{k-1}$.

Insgesamt ergibt sich also $\mathrm{ggT}(a,b)=r_{k-1}$.

w.z.b.w.

(d) Aus der vorletzten Gleichung des euklidischen Algorithmus erhalten wir $3=15-2\cdot 6$.

Mit Hilfe der dritten Gleichung ergibt sich $3=15-2\cdot(21-1\cdot 15)=-2\cdot 21+3\cdot 15$.

Durch Einsetzen der zweiten Gleichung ergibt sich $3=-2\cdot 21+3\cdot(78-3\cdot 21)=3\cdot 78-11\cdot 21$. Und schließlich erhalten wir unter Verwendung der ersten Gleichung die Darstellung

$3=3\cdot 78-11\cdot(99-1\cdot 78)=-11\cdot 99+14\cdot 78$.

Dies ist die gesuchte Lösung mit $x=-11$ und $y=14$.

(e) Aus der vorletzten Gleichung des euklidischen Algorithmus erhalten wir $17=221-2\cdot 102$.

Mit Hilfe der dritten Gleichung ergibt sich $17=221-2\cdot(323-1\cdot 221)=-2\cdot 323+3\cdot 221$.

Durch Einsetzen der zweiten Gleichung ergibt sich $17=-2\cdot 323+3\cdot(17017-52\cdot 323)=3\cdot 17017-158\cdot 323$. Und schließlich erhalten wir unter Verwendung der ersten Gleichung die Darstellung

$17=3\cdot 17017-158\cdot(34357-2\cdot 17017)=-158\cdot 34357+319\cdot 17017$.

Dies ist die gesuchte Lösung mit $x=-158$ und $y=319$.

(f) Aus der Definition und den bisher hergeleiteten Eigenschaften von Restklassen folgt

$$\begin{aligned} \overline{a}\in\mathbb{Z}/n\mathbb{Z} \text{ ist invertierbar} &\iff \exists\,\overline{x}\in\mathbb{Z}/n\mathbb{Z} \text{ mit } \overline{a\cdot x}=\overline{a}\cdot_n\overline{b}=\overline{1} \iff \exists\,x,y\in\mathbb{Z} \text{ mit } ax-1=-y\cdot n \\ &\iff \exists\,x,y\in\mathbb{Z} \text{ mit } ax+ny=1 \end{aligned}$$

Wenn $\text{ggT}(a,n) = 1$ gilt, so existieren wegen dem in der Aufgabe beschriebenen Satz ganze Zahlen x und y mit $ax + yn = 1$ und wegen der gerade bewiesenen Äquivalenz ist $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ invertierbar.

Andererseits: Sei $\text{ggT}(a,n) = d > 1$. Angenommen $\overline{a}$ ist dennoch in $\mathbb{Z}/n\mathbb{Z}$ invertierbar. Dann existieren ganze Zahlen x und y mit $ax + ny = 1$. Die linke Seite dieser Gleichung ist durch d teilbar, die Rechte nicht, was ein Widerspruch ist. $\overline{a}$ ist also nicht invertierbar.

Insgesamt folgt $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann invertierbar, wenn $\text{ggT}(a,n) = 1$ gilt. Die behauptete Gleichheit von Mengen folgt daraus sofort.

w.z.b.w.

(g) Da nach Aufgabe G2 (f) $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring mit Eins ist, ist $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} - \{0\}$ gilt. Dies ist nach dem letzten Aufgabenteil genau dann der Fall, wenn jede Zahl in $\{1, \ldots, n-1\}$ zu n teilerfremd ist. Das gilt nach Definition genau dann, wenn n eine Primzahl ist.

Insgesamt ergibt sich: $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn p eine Primzahl ist.