

## 4 Kongruenz und Modulorechnung

In unserer Zeitrechnung haben wir uns daran gewöhnt, nur mit endlich vielen Zahlen zu rechnen. Es ist gerade 3 Uhr und in 50 Stunden muss ich abreisen. Wie spät ist es dann? Niemand addiert einfach 50 zur 3, denn die Uhrzeit „53 Uhr“ gibt es nicht. Auf einer herkömmlichen Zeigeruhr beginnt alle 12 Stunden die Zeitzählung neu. Daher ist für „50 Stunden später“ der Rest von 50 beim Teilen durch 12 interessant. Das sind 2, folglich ist es bei der Abreise 5 Uhr.



In der Grundschule befasst man sich ebenfalls mit der Division, da man sich aber auf natürliche Zahlen beschränkt, wird die Division mit Rest ausgeführt, wenn sie nicht restlos aufgeht.

Für manche Rechenregeln und mathematische Probleme ist es wesentlich, festzustellen, ob eine Division aufgeht oder nicht. Letztlich geht es dabei auch wieder um die Division mit Rest.

### 4.1 Definition der Kongruenz

Die Kongruenz zwischen zwei ganzen Zahlen ist in Bezug auf einen Teiler definiert. Der Teiler heißt in diesem Zusammenhang Modul.



#### Definition

Gegeben sei ein Modul  $m \in \mathbb{N}$ . Zwei ganze Zahlen  $a$  und  $b$  heißen kongruent modulo  $m$ , wenn die Division von  $a$  und  $b$  durch  $m$  den gleichen Rest  $r$  lässt.

Formal:

$$a \equiv b \pmod{m} \Leftrightarrow \exists t_a, t_b, r \in \mathbb{Z} : a = t_a m + r \text{ und } b = t_b m + r \text{ und } 0 \leq r < m$$



Beispiele:

$$12 \equiv 26 \pmod{7}, \text{ denn } 12 = 1 \cdot 7 + 5 \text{ und } 26 = 3 \cdot 7 + 5$$

12 und 26 lassen also beide den Rest 5 beim Teilen durch 7.

$$6 \equiv -2 \pmod{8}, \text{ denn } 6 = 0 \cdot 8 + 6 \text{ und } -2 = -1 \cdot 8 + 6$$

6 und  $-2$  lassen also beide den Rest 6 beim Teilen durch 8.

Aus der Definition der Kongruenz lässt sich eine direkt damit verbundene Eigenschaft herleiten. Sie wird manchmal auch zur Definition der Kongruenz von zwei Zahlen verwendet.

#### Satz 1

$$a \equiv b \pmod{m} \Leftrightarrow \exists t \in \mathbb{Z} : a - b = tm$$



#### Beweis

(da eine Äquivalenz zu beweisen ist, zerfällt der Beweis in zwei Unterbeweise)



„ $\Rightarrow$ “

$$a \equiv b \pmod{m}$$

$\Rightarrow a = t_a m + r$  und  $b = t_b m + r$  beide Gleichungen werden subtrahiert

$$\begin{aligned} \Rightarrow a - b &= t_a m + r - (t_b m + r) \quad \text{Klammern auflösen, ordnen} \\ \Rightarrow a - b &= t_a m - t_b m \quad m \text{ ausklammern, } t_a - t_b = t \in \mathbb{Z} \\ \Rightarrow a - b &= tm \quad \blacksquare \end{aligned}$$

„ $\Leftarrow$ “

Gegeben sind  $a, b \in \mathbb{Z}$  mit  $a - b = tm$  und  $t \in \mathbb{Z}$ . Die ganzzahlige Division von  $a$  und  $b$  durch  $m$  ergibt:

$$a = t_a m + r_a \quad \text{und} \quad b = t_b m + r_b \quad \text{mit } 0 \leq r_a, r_b < m \quad \text{Subtraktion}$$

$$\Rightarrow a - b = t_a m + r_a - (t_b m + r_b) \quad \text{Einsetzen der Voraussetzung}$$

$$\Rightarrow tm = t_a m + r_a - (t_b m + r_b) \quad \text{Ordnen}$$

$$\Rightarrow (t - t_a + t_b)m = r_a - r_b \quad \text{Das besagt, dass } r_a - r_b \text{ ein ganzzahliges}$$

Vielfaches von  $m$  ist. Aus  $0 \leq r_a < m$  und  $0 \leq r_b < m$  folgt

$-m < r_a - r_b < m$ . Das einzige ganzzahlige Vielfache von  $m$  in diesem Intervall ist  $0 \cdot m$ .

$$\Rightarrow r_a - r_b = 0 \Rightarrow r_a = r_b \quad \blacksquare$$

## 4.2 Rechengesetze für Kongruenzen

Für die Verwendung von Kongruenzen für Aussagen über Zahlen und deren Beweise ist es günstig, einige Rechenregeln für Kongruenzen zu kennen.

Kongruenzen darf man wie Gleichungen mit Rechnungen kombinieren. Dabei ist allerdings die Division nicht zulässig, man muss sich auf  $+$ ,  $-$  und  $\cdot$  beschränken.

### Satz 2

Sei  $m \in \mathbb{N}$  ein Modul und seien  $a, b, c, d \in \mathbb{Z}$

$$a \equiv b \pmod{m} \quad \text{und} \quad c \equiv d \pmod{m} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{m} \\ a - c \equiv b - d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases}$$

### Beweis

$$a \equiv b \pmod{m} \quad \text{und} \quad c \equiv d \pmod{m} \Rightarrow a - b = t_1 m \quad \text{und} \quad c - d = t_2 m \quad (*)$$

„für  $+$ “ Addition beider Gleichungen (\*)

$$\Rightarrow a - b + c - d = (t_1 + t_2)m \quad \text{Umordnen}$$

$$\Rightarrow a + c - (b + d) = (t_1 + t_2)m \quad \text{Da } t_1 + t_2 \in \mathbb{Z}, \text{ gilt nach Satz 1}$$

$$\Rightarrow a + c \equiv b + d \pmod{m}$$

„für  $-$ “ Subtraktion beider Gleichungen (\*)

$$\Rightarrow a - b - (c - d) = (t_1 - t_2)m \quad \text{Umordnen}$$

$$\Rightarrow a - c - (b - d) = (t_1 - t_2)m \quad \text{Da } t_1 - t_2 \in \mathbb{Z}, \text{ gilt nach Satz 1}$$

$$\Rightarrow a - c \equiv b - d \pmod{m}$$



„für ·“

$$a \equiv b \pmod{m} \text{ und } c \equiv d \pmod{m}$$

$$\Rightarrow a = t_a m + r_1 \text{ und } b = t_b m + r_1 \text{ und } c = t_c m + r_2 \text{ und } d = t_d m + r_2$$

$$\Rightarrow ac = (t_a m + r_1)(t_c m + r_2) \text{ und } bd = (t_b m + r_1)(t_d m + r_2) \text{ Ausmultipl.}$$

$$\Rightarrow ac = t_a t_c m^2 + t_a r_2 m + t_c r_1 m + r_1 r_2 \text{ und } bd = t_b t_d m^2 + t_b r_2 m + t_d r_1 m + r_1 r_2$$

In drei Summanden lässt sich jeweils  $m$  ausklammern. Der Teilungsrest modulo  $m$  wird demzufolge allein von  $r_1 r_2$  bestimmt. Der ist damit für  $ac$  und  $bd$  gleich. Also gilt:

$$ac \equiv bd \pmod{m} \blacksquare$$



Diese einfachen Rechenregeln haben eine praktische Anwendung bei der Berechnung von Potenzen. Ein einfaches Beispiel hierfür ist die Berechnung des Teilungsrestes von Zehnerpotenzen.

So ist z.B.  $10 \equiv 3 \pmod{7}$ . Folglich ist  $100 = 10^2 \equiv 3^2 = 9 \equiv 2 \pmod{7}$ .

Für 1000 rechnen Sie dann ähnlich:

$$1000 = 100 \cdot 10 \equiv 2 \cdot 3 = 6 \pmod{7}$$

Und weiter:

$$10.000 = 100 \cdot 100 \equiv 2 \cdot 2 = 4 \pmod{7}$$

Das ist natürlich erheblich einfacher als die Division tatsächlich durchzuführen:  $10.000 = 1428 \cdot 7 + 4$

### 4.3 Kongruenz als Äquivalenzrelation

Für diesen Abschnitt holen wir zunächst ein wenig aus. Wir betrachten eine Menge  $M$  von Elementen. Für die Elemente dieser Menge ist eine Relation definiert, was für uns einfach nur bedeuten soll, dass zwei Elemente in gewisser Beziehung zueinander stehen oder eben nicht. In der Alltagswelt könnten die Elemente der Menge alle Menschen sein und die Relation eine Verwandtschaftsbeziehung, z.B. „ist Mutter von“. Bei einer Menge von Zahlen kennen wir z.B. die Kleinerrelation, bei der Menge der natürlichen Zahlen könnte es die Teilerrelation sein. Nun interessieren Mathematiker prinzipielle Struktureigenschaften dieser Relationen. Abgeleitet von den Eigenschaften der Gleichheitsrelation ist die Äquivalenzrelation eine solche Grundstruktur, die folgendermaßen definiert ist:



#### Definition

Gegeben sei eine Menge  $M$  und eine Relation  $\circ$  für die Elemente der Menge  $M$ . Die Relation  $\circ$  heißt dann Äquivalenzrelation, wenn folgende drei Eigenschaften erfüllt sind:

1. Reflexivität: Für alle Elemente  $a$  von  $M$  gilt:  $a \circ a$
2. Symmetrie: Für alle Elemente  $a, b$  von  $M$  gilt:  $a \circ b \Rightarrow b \circ a$
3. Transitivität: Für alle Elemente  $a, b, c$  von  $M$  gilt:  $a \circ b$  und  $b \circ c \Rightarrow a \circ c$



**Beispiele** für solche Äquivalenzrelationen sind:

Definiert man „ist Geschwister von“ im engeren Sinn, also dass beide Menschen dieselbe Mutter und denselben Vater haben, so ist „ist

Geschwister von“ eine Äquivalenzrelation auf der Menge der Menschen.

Definiert man für zwei Geraden „ist parallel zu“ also „haben überall den gleichen Abstand“, so ist „ist parallel zu“ eine Äquivalenzrelation auf der Menge der Geraden.

Mit diesem Hintergrundwissen stellt sich nun die Frage, ob „ist kongruent zu modulo  $m$ “ eine Äquivalenzrelation auf der Menge  $\mathbb{Z}$  der ganzen Zahlen ist.

### Satz 3



Die Kongruenzrelation ist für alle Modulo  $m$  auf der Menge  $\mathbb{Z}$  eine Äquivalenzrelation.

### Beweis



Die Kongruenzrelation ist letztlich deshalb eine Äquivalenzrelation, weil die grundlegende Eigenschaft „haben den gleichen Teilungsrest“ auf die Gleichheit zurückgreift, die eine Äquivalenzrelation ist.

Gehen wir die drei Eigenschaften einzeln durch.

1. Reflexivität: Jede Zahl hat zu sich selbst den gleichen Teilungsrest.
2. Symmetrie: Hat  $a$  den gleichen Teilungsrest wie  $b$ , so auch  $b$  wie  $a$ .
3. Transitivität: Hat  $a$  den gleichen Teilungsrest wie  $b$  und  $b$  den gleichen Teilungsrest wie  $c$ , so hat auch  $a$  den gleichen Teilungsrest wie  $c$ .

## 4.4 Restklassen

Nun wird die Menge, auf der die Äquivalenzrelation definiert ist, von ihr in Klassen aufgeteilt, d.h. wir können jedes Element der Menge genau einer Klasse zuordnen. Da wir uns mit der Kongruenzrelation beschäftigen, sprechen wir im folgenden nicht nur von Klassen, sondern von Restklassen.

### Definition



Jede Menge  $\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$  nennt man eine *Restklasse modulo  $m$* . Jedes Element  $x \in \bar{a}$  heißt *Repräsentant* der Restklasse  $\bar{a}$ . Die Menge aller Restklassen modulo  $m$  bezeichnet man mit  $R_m$ .

Wir zerlegen also  $\mathbb{Z}$  bei gegebenem  $m \in \mathbb{N}$  so in Restklassen, dass alle Zahlen, die beim Teilen durch  $m$  denselben Rest lassen, in einer Klasse zusammengefasst werden.

Zum Beispiel wird für das Modul  $m = 5$   $\mathbb{Z}$  in 5 Klassen zerlegt, wobei die Klasse  $\bar{0}$  alle Zahlen enthält, die durch 5 teilbar sind, die Klasse  $\bar{1}$  umfasst alle Zahlen, die beim Teilen durch 5 den Rest 1 lassen usw.:

$$\bar{0} = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$$

$$\bar{1} = \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}$$

$$\bar{2} = \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\}$$

$$\bar{3} = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}$$

$$\bar{4} = \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}$$

-8 und 7 wären beispielsweise bei diesem Modul *Repräsentanten* für die Restklasse  $\bar{2}$ , da  $-8 \in \bar{2}$  und  $7 \in \bar{2}$  ( $-8 \equiv 2 \pmod{5}$  und  $7 \equiv 2 \pmod{5}$ ).

Üblicherweise nimmt man für das Modul  $m$  alle Zahlen  $z \in \mathbb{Z}$  mit  $0 \leq z \leq m-1$  als Repräsentanten. Für  $m = 5$  wären neben  $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$  aber zum Beispiel auch  $\bar{-1}, \bar{-4}, \bar{6}, \bar{7}, \dots$  Elemente von  $R_5$ , wobei jedoch  $\bar{1}$  und  $\bar{6}$  dasselbe Element von  $R_5$  darstellen ( $\bar{1} = \bar{6}$ ), denn:

$$\bar{1} = \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}, \quad \bar{6} = \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}.$$

Ob zwei Restklassen  $\bar{a}$  und  $\bar{b}$  für ein Modul  $m$  gleich sind, kann man erkennen, indem man die Kongruenz der beiden Zahlen  $a$  und  $b$  überprüft. Formal:

#### Satz 4

Für alle  $a, b \in \mathbb{Z}$  und jeden Modul  $m \in \mathbb{N}$  gilt:

$$a \equiv b \pmod{m} \Leftrightarrow \bar{a} = \bar{b}$$



Auch ohne den Vergleich der Mengen, hätten wir also feststellen können, dass die zwei Restklassen  $\bar{1}$  und  $\bar{6}$  gleich sind, da  $1 \equiv 6 \pmod{5}$  gilt.

### 4.4.1 Rechnen mit Restklassen

Mit Hilfe der Rechengesetze für Kongruenzen können wir nun überlegen, ob wir auf einfache Weise auch die Summe zweier Zahlen einer Restklasse zuordnen können. Nehmen wir mal zwei Beispiele:



1) In welcher Restklasse modulo 10 liegt die Summe von 134 und 235?

Zunächst bestimmen wir die Restklassen der einzelnen Summanden:

$$134 \equiv 4 \pmod{10} \quad \Rightarrow 134 \in \bar{4}$$

$$235 \equiv 5 \pmod{10} \quad \Rightarrow 235 \in \bar{5}$$

Nun addieren wir die beiden Zahlen und bestimmen die Restklasse:

$$134 + 235 = 369 \equiv 9 \pmod{10} \quad \Rightarrow 369 \in \bar{9}$$

2) In welcher Restklasse (modulo 10) liegt  $341 + 236$ ?

$$346 \equiv 6 \pmod{10} \quad \Rightarrow 346 \in \bar{6}$$

$$38 \equiv 8 \pmod{10} \quad \Rightarrow 38 \in \bar{8}$$

$$346 + 38 = 384 \equiv 4 \pmod{10} \quad \Rightarrow 384 \in \bar{4}$$

Nun können wir uns überlegen, ob man direkt über die Addition der Restklassen auch zu einem Ergebnis kommen könnte.

Nach den Rechengesetzen für Kongruenzen (4.2) können wir, wenn wir einmal den zweiten Fall erneut als Beispiel nehmen, rechnen:

$$346 + 38 \equiv 6 + 8 \pmod{10},$$

$$\text{also } 346 + 38 \equiv 14 \pmod{10}.$$

Da  $14 \equiv 4 \pmod{10}$  gilt, folgt  $346 + 38 \equiv 4 \pmod{10}$ ,

$$\text{also } 346 + 38 \in \overline{4} = \overline{14}$$

Wir hätten also auch gleich die beiden Repräsentanten der Restklassen addieren können, um zu unserem Ergebnis zu gelangen.



### Definition Addition von Restklassen

Seien  $\overline{a}$  und  $\overline{b}$  zwei Restklassen aus  $R_m$ , dann versteht man unter der Verknüpfung  $\overline{a} \oplus \overline{b}$  die eindeutig bestimmte Restklasse  $\overline{a + b}$ :

$$\overline{a} \oplus \overline{b} = \overline{a + b}$$

Dabei ist die Addition unabhängig von der Wahl des Repräsentanten. Wir können also zwei Restklassen addieren, indem wir aus jeder Restklasse einen Repräsentanten wählen, diese beiden Repräsentanten addieren und anschließend die Restklasse bestimmen, in der die Summe liegt.

**Beispiel** (modulo 10):

$$\overline{5} = \{\dots, -25, -15, -5, 5, 15, 25, \dots\}$$

$$\overline{8} = \{\dots, -22, -12, -2, 8, 18, 28, \dots\}$$

Nun gilt  $\overline{5} \oplus \overline{8} = \overline{13} = \overline{3}$ . Wenn die Addition unabhängig von der Wahl der Repräsentanten ist, müsste auch zum Beispiel gelten:

$$\overline{-5} \oplus \overline{18} = \overline{3} \quad \text{oder} \quad \overline{-15} \oplus \overline{-12} = \overline{3}.$$

Überprüfung:

$$\overline{-5} \oplus \overline{18} = \overline{-5 + 18} = \overline{13} = \overline{3}, \quad \text{da } 13 \equiv 3 \pmod{10},$$

$$\overline{-15} \oplus \overline{-12} = \overline{-15 - 12} = \overline{-27} = \overline{3}, \quad \text{da } -27 \equiv 3 \pmod{10}.$$

Die Wahl der Repräsentanten spielt also keine Rolle.

Genauso wie die Restklassenaddition können wir die Restklassenmultiplikation einführen:



### Definition Multiplikation von Restklassen

Seien  $\bar{a}$  und  $\bar{b}$  zwei Restklassen aus  $R_m$ , dann versteht man unter der Verknüpfung  $\bar{a} \otimes \bar{b}$  die eindeutig bestimmte Restklasse  $\overline{ab}$ :

$$\bar{a} \otimes \bar{b} = \overline{ab}$$



**Beispiele** (modulo 5):

$$\bar{2} \otimes \bar{3} = \overline{2 \cdot 3} = \overline{6} = \bar{1}$$

$$\bar{3} \otimes \bar{4} = \overline{3 \cdot 4} = \overline{12} = \bar{2}$$

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Für eine Restklassenmenge lässt sich die Multiplikation sehr übersichtlich in einer Multiplikationstafel darstellen. Das Beispiel rechts ist die Tafel modulo 5.

## 4.5 Gruppen

Beenden wollen wir dieses Kapitel mit der Einführung des Begriffes „Gruppe“.

Ein Paar  $(G, \circ)$  aus einer nichtleeren Menge  $G$  und einer Verknüpfung „ $\circ$ “ heißt *Gruppe*, wenn folgende Eigenschaften erfüllt sind:

- 1) Mit  $a, b \in G$  liegt stets auch  $a \circ b$  in  $G$ . (Abgeschlossenheit)
- 2)  $(a \circ b) \circ c = a \circ (b \circ c)$  für alle  $a, b, c \in G$  (Assoziativität)
- 3) Es gibt ein neutrales Element  $e \in G$  mit  $e \circ a = a \circ e = a$  für alle  $a \in G$ .
- 4) Zu jedem  $a \in G$  gibt es ein inverses Element  $a^{-1} \in G$ , so dass  $a \circ a^{-1} = a^{-1} \circ a = e$ .

Wenn zusätzlich zu den vier Eigenschaften die Kommutativität gegeben ist ( $a \circ b = b \circ a$  für alle  $a, b \in G$ ), so heißt die Gruppe  $(G, \circ)$  kommutativ.

Nun untersuchen wir die beiden Verknüpfungsgebilde  $(R_m, \oplus)$ ,  $(R_m, \otimes)$  für alle  $m \in \mathbb{N}$  hinsichtlich der Gruppeneigenschaften.

### Restklassenaddition:

Als Hilfe betrachten wir für den Fall  $m = 5$  die zugehörige Gruppentafel.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

- 1) Zunächst ist die Restklassenaddition abgeschlossen:

$$\bar{a} \oplus \bar{b} \in R_m \text{ für alle } \bar{a}, \bar{b} \in R_m.$$

In der Gruppentafel tauchen nur Elemente aus  $R_5$  auf.

- 2) Die Restklassenaddition ist assoziativ:

$$(\bar{a} \oplus \bar{b}) \oplus \bar{c} = \overline{a + b} \oplus \bar{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \bar{a} \oplus \overline{b + c} = \bar{a} \oplus (\bar{b} \oplus \bar{c})$$

für alle  $\bar{a}, \bar{b}, \bar{c} \in R_m$ .

- 3)  $\bar{0}$  ist das neutrale Element in  $R_m$  bezüglich  $\oplus$ :

$$\bar{a} \oplus \bar{0} = \overline{a+0} = \bar{a} \text{ für alle } \bar{a} \in R_m.$$

Das neutrale Element  $\bar{0}$  erkennt man in der Gruppentafel daran, dass die erste Zeile und Spalte (blau) mit der Randzeile und -spalte übereinstimmt.

- 4) Das inverse Element zu jedem  $\bar{a} \in R_m$  ist  $\overline{m-a}$  bezüglich  $\oplus$ :  
 $\bar{a} + \overline{m-a} = \overline{a+m-a} = \overline{m} = \bar{0}$  für alle  $\bar{a} \in R_m$ .

In der Gruppentafel kann man sehen, dass das neutrale Element  $\bar{0}$  in jeder Spalte und in jeder Zeile genau einmal auftritt. In diesem Beispiel sind  $\bar{1}$  und  $\bar{4}$ ,  $\bar{2}$  und  $\bar{3}$  zueinander und  $\bar{0}$  zu sich selbst invers.

- 5) Bezüglich der Hauptdiagonalen (gelb) erkennt man die Symmetrie der Tafel, aus der sich außerdem die Kommutativität ergibt:  
 Die Restklassenaddition ist kommutativ:  
 $\bar{a} \oplus \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} \oplus \bar{a}$  für alle  $\bar{a}, \bar{b} \in R_m$ .

Aus diesen Erkenntnissen folgt

### Satz 5

Für alle  $m \in \mathbb{N}$  ist  $(R_m, \oplus)$  eine kommutative Gruppe.



### Restklassenmultiplikation:

- 1) Die Restklassenmultiplikation ist abgeschlossen:  
 $\bar{a} \otimes \bar{b} \in R_m$  für alle  $\bar{a}, \bar{b} \in R_m$ .
- 2) Die Assoziativität gilt ebenfalls:  
 $\bar{a} \otimes (\bar{b} \otimes \bar{c}) = \overline{a \otimes (bc)} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \otimes \bar{c} = (\bar{a} \otimes \bar{b}) \otimes \bar{c}$  für alle  $\bar{a}, \bar{b}, \bar{c} \in R_m$ .
- 3) Das neutrale Element der Restklassenmultiplikation ist  $\bar{1}$ :  
 $\bar{a} \otimes \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \otimes \bar{a} = \bar{a}$  für alle  $\bar{a} \in R_m$ .
- 4) Betrachten wir einmal die oben erstellte Multiplikationstafel (modulo 5), fällt auf, dass das neutrale Element nicht in jeder Spalte einmal auftritt.  
 In keiner Menge  $R_m$  mit  $m > 1$  gibt es ein inverses Element, denn  $\bar{0} \otimes \bar{a} = \bar{0} \neq \bar{1}$  für alle  $\bar{a} \in R_m, m > 1$ .

Schon hier können wir aufhören und erkennen, dass  $(R_m, \otimes)$  keine Gruppe ist.

Zwar ist auch die Kommutativität gegeben ( $\bar{a} \otimes \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \otimes \bar{a}$  für alle  $\bar{a}, \bar{b} \in R_m$ ), dennoch ist die nötige Gruppeneigenschaft „inverses Element“ nicht gegeben.

# Ü

## 4.6 Übungsaufgaben

### 1. Zeitrechnung

- Es ist der 16. November, 16 Uhr. Welches Datum und Uhrzeit hat man nach 1000 Stunden.
- Es ist der 16. November 2007. Welches Datum hat man nach 1000 Tagen?

### 2. Der 3.11.2004 ist ein Mittwoch.

- Welcher Wochentag ist der 3.11.2005?
- Welcher Wochentag war der 3.11.2003?

*Ein vollkommen angemessener Lösungsweg für das Problem ist, in einem Kalender nachzuschauen. Tun Sie das, es ist immer gut, wenn man vorher weiß, was das Ergebnis ist.*

**Aufgabe:** Wie könnten Sie das Problem ohne Hilfsmittel im Kopf lösen? Stellen Sie ihre Überlegungen dar.

### 3. Welche Implikation ist richtig, welche ist falsch?

- $a \equiv b \pmod{m} \Rightarrow a^2 \equiv b^2 \pmod{m}$
  - $a^2 \equiv b^2 \pmod{m} \Rightarrow a \equiv b \pmod{m}$
- Begründen Sie Ihre Antworten.

### 4. Es sei $a \equiv b \pmod{m}$ und $d$ ein Teiler von $m$ . Dann gilt auch

$$a \equiv b \pmod{d}$$

- Machen Sie die Aussage an einem Beispiel deutlich.
- Begründen Sie die Aussage an Zahlentabellen mit  $m = 10$  und  $d = 5$ .
- Begründen Sie die Aussage mit einem allgemeinen Punktemuster.
- Beweisen Sie die Aussage formal.

### 5. „In einer Kongruenz darf man eine Zahl durch eine kongruente Zahl ersetzen.“

Genauer:

$$a + b \equiv c \pmod{m} \text{ und } b \equiv d \pmod{m} \Rightarrow a + d \equiv c \pmod{m}$$

Beweisen Sie diese Gesetzmäßigkeit.

### 6. Berechnen Sie $x$ .

- $3^6 \equiv x \pmod{7}$  mit  $0 \leq x \leq 6$
  - $5^6 \equiv x \pmod{7}$  mit  $0 \leq x \leq 6$
  - $3^{10} \equiv x \pmod{11}$  mit  $0 \leq x \leq 10$
  - $4^{12} \equiv x \pmod{13}$  mit  $0 \leq x \leq 12$
  - $5^{12} \equiv x \pmod{13}$  mit  $0 \leq x \leq 12$
- Haben Sie eine Vermutung über eine Regelmäßigkeit? Schreiben Sie sie allgemein auf.
  - Berechnen Sie nun (möglichst geschickt)  $7^{112} \equiv x \pmod{11}$  mit  $0 \leq x \leq 10$ .

7. Berechnen Sie  $3^{132} \equiv x \pmod{11}$ , wobei  $x$  eine Zahl sein soll mit  $0 \leq x < 11$ .  
Anleitung: Berechnen Sie möglichst geschickt zunächst  $3 \equiv x_1 \pmod{11}$ ,  $3^2 \equiv x_2 \pmod{11}$ ,  $3^3 \equiv x_3 \pmod{11}$  u.s.w., mit  $0 \leq x_i < 11$ , bis Sie eine Regelmäßigkeit entdecken, mit der Sie dann das eigentliche Problem lösen können.
8. Ist die Menge  $A = \{1, \frac{1}{3}, 3\}$  mit der normalen Multiplikation eine Gruppe? Welche der vier Eigenschaften sind ggf. nicht erfüllt?
9. Stellen Sie die Multiplikationstafel auf für die Restklassen von  $R_5$  und  $R_6$  (siehe Vorlesung).
- In welchen Zeilen der Multiplikationstafel von  $R_5$  tauchen als Ergebnis alle Restklassen von  $R_5$  auf?  
Wie ist das in der Tafel von  $R_6$ ?
  - Schreiben Sie alle Lösungen auf für  $\bar{a} \cdot \bar{b} = \bar{0}$   
In  $R_5$ .  
In  $R_6$ .
  - Eine Restklasse  $\bar{a} \in R_m, \bar{a} \neq \bar{0}$  heißt Nullteiler von  $R_m$ , wenn es eine Restklasse  $\bar{b} \in R_m, \bar{b} \neq \bar{0}$  gibt mit  $\bar{a} \cdot \bar{b} = \bar{0}$ . Was sind nach Aufgabe b. die Nullteiler von  $R_5$  und  $R_6$ ?
  - Suchen Sie in  $R_7$  nach Nullteilern.
  - Stellen Sie Vermutungen an, wann Nullteiler auftauchen.  
Überprüfen Sie die Vermutungen an weiteren Beispielen.
- 10.
- Untersuchen Sie, ob die Relation „sind Cousin/Cousine“ eine Äquivalenzrelation auf der Menge aller Menschen ist.  
Untersuchen Sie dazu alle drei Eigenschaften Reflexivität, Symmetrie und Transitivität.  
Definition: Zwei Menschen sind Cousin/Cousine, wenn Vater oder Mutter des einen und Vater oder Mutter des anderen Menschen Geschwister sind. („sind Geschwister“ ist wie in der Vorlesung die enge Definition)
  - Zeigen Sie, dass „sind Aufgabengruppenpartner“ eine Äquivalenzrelation ist.  
Erläuterung: Zwei Menschen  $a, b$  sind Aufgabengruppenpartner, in Zeichen  $a$  AGP  $b$ , wenn sie in der Vorlesung „Arithmetik als Prozess“ in diesem Semester ihre Aufgaben in einer Gruppe abgeben.  
Was ist die Grundmenge und was sind die Äquivalenzklassen, in die die Grundmenge zerfällt?
11. Zwei Beweise
- Beweisen Sie für die Menge aller Restklassen  $R_{10}$  zum Modul  $m = 10$ : Keine Zahl  $n \in \mathbb{N}$  gehört gleichzeitig zu zwei Restklassen.

- b. Beweisen Sie allgemein: Es sei  $M$  eine Menge und  $\otimes$  eine für die Elemente von  $M$  definierte Äquivalenzrelation. Wie in der Vorlesung eingeführt bezeichne  $\bar{a}$  die Äquivalenzklasse bezüglich  $\otimes$ , in der  $a \in M$  liegt.  
Dann gilt:  $c \in \bar{a}$  und  $c \in \bar{b} \Rightarrow \bar{a} = \bar{b}$