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.

Info

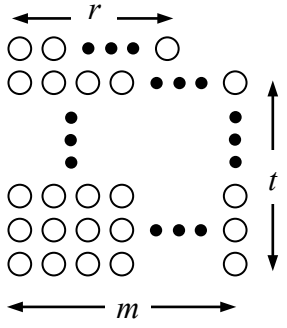
In der Grundschule befasst man sich ebenfalls mit der Division, da man sich aber auf natürliche Zahlen beschränkt, wird die Division mit Rest ausgeführt, wenn sie nicht restlos aufgeht.
Die Division mit Rest ist nicht nur ein Behelf, so lange keine Brüche eingeführt worden sind, sondern diese Art des Rechnens ist für manche Problemlösungen sinnvoll und nützlich.

4.1 Teilen mit Rest

Das Teilen mit Rest entspricht stark der Welt der Kinder. Teilt man eine bestimmte Anzahl von Dingen (Süßigkeiten, Spielsachen) auf eine Schar von Kindern auf, so kann beim Aufteilen ein Rest entstehen. Das wesentliche Ergebnis des Teilens ist hier die Anzahl der Dinge, die jedes Kind erhält.
Teilt man eine natürliche Zahl a durch eine andere, genannt m, so gibt die Häufigkeit t an, wie oft m in a enthalten ist. Dazu kann ein Rest bleiben, der logischerweise kleiner sein muss als m, denn sonst könnte man den Rest ja noch wenigstens ein Mal durch m teilen und so den Rest verkleinern. Geht die Division auf, so ist $r = 0$. Für den Rest r gilt also immer $0 \leq r < m$.
Formal schreiben wir $a = m \cdot t + r$
Beispiel: Teilt man $a = 45$ durch $m = 7$, so ist $m = 7$ $t = 6$ Mal in $a = 45$ enthalten und es bleibt ein Rest r von 3.
Als Gleichung: $45 = 7 \cdot 6 + 3$

Info

Neben der rein algebraischen Darstellung wollen wir noch eine anschauliche über allgemeine Punktmuster begleitend mitverfolgen.
Die Division durch m stellen wir dadurch dar, dass m Punkte in einer Zeile nebeneinander liegen. Die Häufigkeit t ist die Anzahl der vollständigen m-Zeilen, die gebildet werden können. Am Ende bleibt ein Rest r, der eine unvollständige Zeile von r Punkten ergibt.



Die Allgemeinheit des Punktemusters wird durch die ••• Punkte dargestellt. In einem konkreten Fall stellt man die Zahlen auch durch die korrekten Punktanzahlen dar.

4.2 Definition der Kongruenz

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

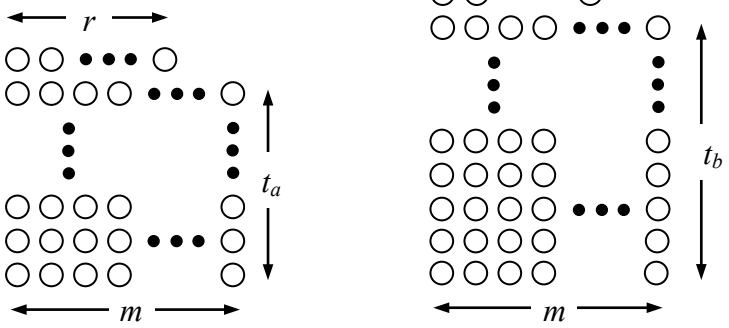
Def!

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

Bsp.

Beispiele:
$12 \equiv 26 \bmod 7$, denn 12 = 1·7+5 und 26 = 3·7+5
12 und 26 lassen also beide den Rest 5 beim Teilen durch 7.
$6 \equiv -2 \bmod 8$, denn 6 = 0·8 + 6 und –2 = –1·8 + 6
6 und –2 lassen also beide den Rest 6 beim Teilen durch 8.
Das letzte Beispiel mit der negativen Zahl macht deutlich, dass wir keine negativen Reste zulassen, während die Vielfachheit *t*, also wie oft der Modul *m* in eine Zahl passt, durchaus negativ sein darf.

Im allgemeinen Punktmuster zeigt sich die Kongruenz dadurch, dass die oberste Zeile mit dem Rest *r* die gleiche Gestalt hat.



Beim Teilen durch *m* erzeugen die beiden Zahlen *a* (links) und *b* (rechts) ein unterschiedlich hohes Rechteck aus vollständigen *m*-Zeilen. Die obere, unvollständige *r*-Zeile ist in beiden Mustern gleich.

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.

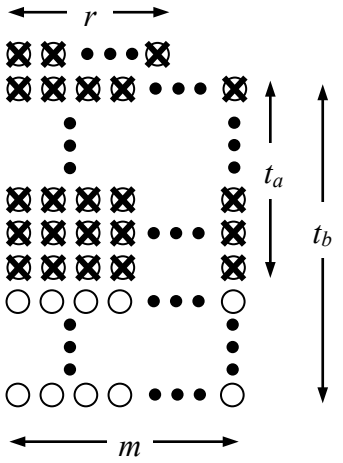
Satz.

Satz 4.1
Zwei Zahlen *a* und *b* sind kongruent modulo *m* genau dann, wenn ihre Differenz *a – b* durch *m* teilbar ist.
Formal: $a \equiv b \bmod m \Leftrightarrow \exists t \in \mathbb{Z} : a - b = tm$

Beweis
(da eine Äquivalenz zu beweisen ist, zerfällt der Beweis in zwei Teile)
„$\Rightarrow$“
$a \equiv b \bmod m$
$\Rightarrow a = t_a m + r \ und \ b = t_b m + r$ beide Gleichungen werden subtrahiert
$\Rightarrow a - b = t_a m + r - (t_b m + r)$ Klammern auflösen, ordnen
$\Rightarrow a - b = t_a m - t_b m$ *m* ausklammern, $t_a - t_b = t \in \mathbb{Z}$
$\Rightarrow a - b = tm$ □

„$\Leftarrow$“
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:
$a = t_a m + r_a \ und \ b = t_b m + r_b$ mit $0 \le r_a, r_b < m$ Subtraktion
$\Rightarrow a - b = t_a m + r_a - (t_b m + r_b)$ Einsetzen der Voraussetzung
$\Rightarrow tm = t_a m + r_a - (t_b m + r_b)$ Ordnen
$\Rightarrow (t - t_a + t_b)m = r_a - r_b$
Das besagt, dass $r_a - r_b$ ein ganzzahliges Vielfaches von *m* ist.
Aus $0 \le r_a < m \ und \ 0 \le r_b < m$ folgt $-m < r_a - r_b < m$.
Das einzige ganzzahlige Vielfache von *m* in diesem Intervall ist $0 \cdot m$.
$\Rightarrow r_a - r_b = 0 \Rightarrow r_a = r_b$ □

Im allgemeinen Punktmuster ist diese Eigenschaft unmittelbar einsichtig. Die Subtraktion beider Zahlen führt dazu, dass die unvollständige *r*-Zeile verschwindet, da diese in beiden Zahlen gleich ist. Die weitere Differenz besteht dann nur aus vollständigen *m*-Zeilen, so dass sich am Ende ein Rechteck aus m Punkten nebeneinander und $t_b - t_a$ (wenn $b > a$) übereinander ergibt.



4.3 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 kombinieren. Dabei ist allerdings die Division nicht zulässig, man muss sich auf +, – und · beschränken.

Satz.

Satz 4.2
Sei $m \in \mathbb{N}$ ein Modul und seien $a,b,c,d \in \mathbb{Z}$

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

Beweis

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

„für +“ Addition beider Gleichungen (*)

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

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

$\Rightarrow a+c \equiv b+d \bmod m$

„für –“ Subtraktion beider Gleichungen (*)

$\Rightarrow a-b-(c-d) = (t_1-t_2)m$ Umordnen

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

$\Rightarrow a-c \equiv b-d \bmod m$

„für · “

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

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

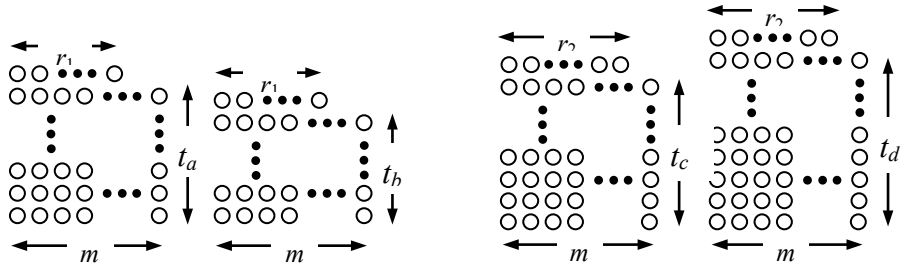
$\Rightarrow ac = (t_a m + r_1)(t_c m + r_2) \text{ und } bd = (t_b m + r_1)(t_d m + r_2)$ Ausmultipl.

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

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:

$ac \equiv bd \bmod m$ ∎

Die Rechenregeln für + und – lassen sich auch gut mit allgemeinen Punktmustern veranschaulichen.



Die linken beiden Punktmuster stellen die Kongruenz von *a* und *b* dar, die rechten beiden zeigen die Kongruenz von *c* und *d*. Addiert man *a* und *c* einerseits und *b* und *d* andererseits, so wird der Rest modulo *m*

allein von $r_1 + r_2$ bestimmt, das aber bei beiden Summen in gleicher Weise. Gleiches gilt für die Differenz.

Info

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. $10 \equiv 3 \bmod 7$. Folglich ist $100 = 10^2 \equiv 3^2 = 9 \equiv 2 \bmod 7$.
Für 1000 rechnet man dann ähnlich:
$1000 = 100 \cdot 10 \equiv 2 \cdot 3 = 6 \bmod 7$
Und weiter:
$10.000 = 100 \cdot 100 \equiv 2 \cdot 2 = 4 \bmod 7$
Das ist natürlich erheblich einfacher als die Division tatsächlich durchzuführen: $10.000 = 1428 \cdot 7 + 4$

4.4 Die 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 Verwandschaftsbeziehung, 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:

Def!

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* $b \circ c \Rightarrow a \circ c$

Bsp.

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.
Die Eigenschaft „ist parallel zu“ für die Geraden einer Ebene ist eine Äquivalenzrelation auf der Menge der Geraden. (Eine Gerade ist zu

sich selbst parallel in dem Sinn, dass sie überall den gleichen Abstand, nämlich den Abstand Null, zu sich selbst hat.)
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.

Satz 4.3
Die Kongruenzrelation ist für alle Moduln *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 Rest 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*.

4.5 Restklassen

Nun wird die Menge, auf der eine Äquivalenzrelation definiert ist, von dieser in Klassen aufgeteilt, d.h. wir können jedes Element der Menge genau einer Klasse zuordnen. Für die Kongruenzrelation nennt man die zugehörigen Klassen Restklassen.

Def!

Definition
Jede Menge $\overline{a} = \left\{ x \in \mathbb{Z} \middle| x \equiv a \bmod m \right\}$ nennt man eine *Restklasse modulo m*. Das Element *a*, das wegen der Reflexivität auch in $\overline{a}$ liegt, heißt *Repräsentant* der Restklasse $\overline{a}$. 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 $\overline{0}$ alle Zahlen enthält, die durch 5 teilbar sind, die Klasse $\overline{1}$ umfasst alle Zahlen, die beim Teilen durch 5 den Rest 1 lassen usw.:

$\overline{0} = \{...,-15,-10,-5,0,5,10,15,...\}$

$\overline{1} = \{...,-14,-9,-4,1,6,11,16,...\}$

$\overline{2} = \{...,-13,-8,-3,2,7,12,17,...\}$

$\overline{3} = \{...,-12,-7,-2,3,8,13,18,...\}$

$\overline{4} = \{...,-11,-6,-1,4,9,14,19,...\}$

Die Restklassen werden zur Menge R_5 zusammengefasst, also

$R_5 = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$

Mit der Schreibweise $\overline{2}$ wählt man also 2 als Repräsentanten für die Restklasse, die 2 enthält. Ebenso ist aber auch 6 beim Modul $m = 5$ Repräsentant für die Restklasse $\overline{1}$, da $6 \in \overline{1}$ ($6 \equiv 1 \bmod 5$). Folglich kann man für die Restklasse $\overline{1}$ auch $\overline{6}$ schreiben. $\overline{1}$ und $\overline{6}$ stellen dieselbe Menge dar, denn:

$\overline{1} = \{...,-14,-9,-4,1,6,11,16,...\}$, $\overline{6} = \{...,-14,-9,-4,1,6,11,16,...\}$.

Also gilt: $\overline{1} = \overline{6}$

Üblicherweise nimmt man beim Modul m alle Zahlen $z \in \mathbb{Z}$ mit $0 \le z \le m-1$ als Repräsentanten. Für $m = 5$ wären das $\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}$. Die Menge aller Restklassen zum Modul m bezeichnet man mit R_m. Also gilt $R_5 = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}$. Aber zum Beispiel sind auch $\overline{-1},\overline{-4},\overline{5},\overline{7},\overline{13}$ alle Elemente von R_5, allerdings sind diese Repräsentanten unhandlicher.

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

Satz.

Satz 4.4

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

$a \equiv b \bmod m \Leftrightarrow \overline{a} = \overline{b}$

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

4.5.1 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 einmal zwei Beispiele:

Bsp.

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

Zunächst bestimmen wir die Restklassen der einzelnen Summanden:

$134 \equiv 4 \bmod 10 \quad \Rightarrow 134 \in \overline{4}$

$235 \equiv 5 \bmod 10 \quad \Rightarrow 235 \in \overline{5}$

Nun addieren wir die beiden Zahlen und bestimmen die Restklasse:

$134 + 235 = 369 \equiv 9 \bmod 10 \quad \Rightarrow 369 \in \overline{9}$

2) In welcher Restklasse (modulo 10) liegt 346 + 38?

$346 \equiv 6 \mod 10 \quad \Rightarrow 346 \in \overline{6}$
$38 \equiv 8 \mod 10 \quad \Rightarrow 38 \in \overline{8}$
$346 + 38 = 384 \equiv 4 \mod 10 \quad \Rightarrow 384 \in \overline{4}$

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:

$346 + 38 \equiv 6 + 8 \mod 10$,
also $346 + 38 \equiv 14 \mod 10$.
Da $14 \equiv 4 \mod 10$ gilt, folgt $346 + 38 \equiv 4 \mod 10$,
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.

Def!

Definition der 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 Restklasse $\overline{a+b}$.
Also kurz: $\overline{a} \oplus \overline{b} = \overline{a+b}$

Bsp.

Beispiel (modulo 10):
$\overline{5} = \{...,-25,-15,-5,5,15,25,...\} \quad \overline{8} = \{...,-22,-12,-2,8,18,28,...\}$
Also gilt $\overline{5} \oplus \overline{8} = \overline{13} = \overline{3}$.

Bei der Definition der Addition von Restklassen haben wir ein Problem, das öfter in der Mathematik auftaucht: Wir definieren eine Operation für zwei Mengen, indem wir konkret mit dem Repräsentanten rechen. Was ist aber, wenn wir einen anderen Repräsentanten wählen? Die Definition ist nur dann tragfähig, wenn sie von der Wahl des Repräsentanten unabhängig ist. Diese Eigenschaft nennt man Wohldefiniertheit.
Tatsächlich ist die Addition von Restklassen wohldefiniert, also unabhängig von der Wahl des Repräsentanten. Wir wollen das zunächst an einem Beispiel untersuchen. Als Modul wählen wir wieder $m = 10$:
Nach der obigen Definition gilt: $\overline{-5} \oplus \overline{18} = \overline{3}$
Für $\overline{-5}$ wählen wir nun $\overline{15}$, denn es gilt $-5 \equiv 15 \mod 10$ und für $\overline{18}$ wählen wir $\overline{28}$, da $18 \equiv 28 \mod 10$. Mit den neuen Repräsentanten rechnen wir $\overline{15} \oplus \overline{28} = \overline{43} = \overline{3}$, da $43 \equiv 3 \mod 10$.
Der allgemeine Beweis folgt genau dieser Logik:

Es sei $\bar{a} \oplus \bar{b} = \overline{a+b}$. Wenn nun a' ein anderer Repräsentant für $\bar{a}$ und b' ein anderer Repräsentant für $\bar{b}$ ist, dann gilt:
$\bar{a} \oplus \bar{b} = \overline{a'} \oplus \overline{b'} = \overline{a'+b'}$.
Wir müssen nun zeigen, dass $\overline{a'+b'} = \overline{a+b}$.
Wegen $a' \equiv a \bmod m$ und $b' \equiv b \bmod m$ gilt auch
$a'+b' \equiv a+b \bmod m$, also gilt $\overline{a'+b'} = \overline{a+b}$. ∎

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. Die Wahl der Repräsentanten spielt keine Rolle. Genau das ist es, was sich hinter der Wohldefiniertheit verbirgt.

Genauso wie die Restklassenaddition können wir die Restklassenmultiplikation einführen:

Def!

Definition der 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 $\overline{ab}$:
$\bar{a} \otimes \bar{b} = \overline{ab}$

Bsp.

Beispiele (modulo 5):
$\bar{2} \otimes \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{1}$
$\bar{3} \otimes \bar{4} = \overline{3 \cdot 4} = \overline{12} = \bar{2}$

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

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

4.6 Gruppen

Beenden wollen wir dieses Kapitel mit der Einführung des Begriffes „Gruppe“.
Ein Paar (G,∘) aus einer nichtleeren Menge G und einer Verknüpfung „∘“ 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 Verknüpfungen auf der Menge der Restklassen $(R_m,\oplus)$, $(R_m,\otimes)$ 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:
   $\bar{a} \oplus \bar{b} \in R_m$ für alle $\bar{a},\bar{b} \in R_m$, denn die Definition dieser Addition ergibt wieder eine Restklasse aus 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 $\oplus$:
   $\bar{a} \oplus \bar{0} = \overline{a+0} = \bar{a}$ 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 $\oplus$:
   $\bar{a} + \overline{m-a} = \overline{a+m-a} = \bar{m} = \bar{0}$ 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:
   $\bar{a} \oplus \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$ für alle $\bar{a},\bar{b} \in R_m$.

Aus diesen Erkenntnissen folgt

Satz.

Satz 4.5
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:
$\bar{a} \otimes (\bar{b} \otimes \bar{c}) = \bar{a} \otimes \overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \otimes \bar{c} = (\bar{a} \otimes \bar{b}) \otimes \bar{c}$ für alle $\bar{a}, \bar{b}, \bar{c} \in R_m$.
3) Das neutrale Element der Restklassenmultiplikation ist $\bar{1}$:
$\bar{a} \otimes \bar{1} = \overline{a \bullet 1} = \bar{a} = \overline{1 \bullet a} = \bar{1} \otimes \bar{a} = \bar{a}$ für alle $\bar{a} \in R_m$.
4) Betrachten wir einmal die oben erstellte Multiplikationstafel (modulo 5). Es 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 zu $\bar{0}$, denn $\bar{0} \otimes \bar{a} = \bar{0} \neq \bar{1}$ für alle $\bar{a} \in R_m, m > 1$.

Diese Situation erinnert stark an die Multiplikation mit rationalen Zahlen. Auch hier gibt es für die 0 kein inverses Element. Die rationalen Zahlen mit der Null bilden also bezüglich der Multiplikation keine Gruppe. Nimmt man dagegen die 0 heraus, so bilden alle anderen rationalen Zahlen eine Gruppe für die Multiplikation.
Folglich nehmen wir nun die Restklasse $\bar{0}$, das neutrale Element der Restklassenaddition, heraus und untersuchen die Menge der verbleibenden Restklassen.

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

$\otimes$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Die Multiplikationstabellen für $m = 5$ und $m = 6$

In der linken Tabelle für $m = 5$ sehen wir, dass die $\bar{1}$ in jeder Zeile genau ein Mal vorkommt, dass also jedes Element ein inverses Element hat. In der rechten für $m = 6$ sehen wir, dass das nicht gegeben ist. Zusätzlich erkennen wir, dass die Restklasse $\bar{0}$, die wir gerade herausgenommen hatten, als Multiplikationsergebnis wieder auftaucht. Hier ist also zusätzlich die Abgeschlossenheit nicht erfüllt. $R_5 \setminus \{\bar{0}\}$ ist also bezüglich der Multiplikation eine Gruppe, $R_6 \setminus \{\bar{0}\}$ ist es nicht. Wir wollen diese Thematik nicht weiter vertiefen und lediglich das Ergebnis angeben:

Satz. $(R_m \setminus \{\bar{0}\}, \otimes)$ ist genau dann eine Gruppe, wenn m eine Primzahl ist.

In allen Fällen ist die Multiplikationstabelle symmetrisch, denn $\bar{a} \otimes \bar{b} = \overline{ab} = \overline{ba} = \bar{b} \otimes \bar{a}$ für alle $\bar{a}, \bar{b} \in R_m$. Also sind die Gruppen dann auch kommutativ.

4.7 Übungsaufgaben

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

2. Der 3.11.2004 ist ein Mittwoch.
   a. Welcher Wochentag ist der 3.11.2005?
   b. 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. $a \equiv b \bmod m \Rightarrow a^2 \equiv b^2 \bmod m$
   b. $a^2 \equiv b^2 \bmod m \Rightarrow a \equiv b \bmod m$

   Begründen Sie Ihre Antworten.

4. Es sei $a \equiv b \bmod m$ und d ein Teiler von m. Dann gilt auch $a \equiv b \bmod d$
   a. Machen Sie die Aussage an einem Beispiel deutlich.
   b. Begründen Sie die Aussage an Zahlentabellen mit $m = 10$ und $d = 5$.
   c. Begründen Sie die Aussage mit einem allgemeinen Punktemuster.
   d. Beweisen Sie die Aussage formal.

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

   Genauer:

   a. $a + b \equiv c \bmod m$ und $b \equiv d \bmod m \Rightarrow a + d \equiv c \bmod m$
   b. $a \cdot b \equiv c \bmod m$ und $b \equiv d \bmod m \Rightarrow a \cdot d \equiv c \bmod m$

   Beweisen Sie diese Gesetzmäßigkeiten.

6. Berechnen Sie x.
   i. $3^6 \equiv x \bmod 7$ mit $0 \le x \le 6$
   ii. $5^6 \equiv x \bmod 7$ mit $0 \le x \le 6$
   iii. $3^{10} \equiv x \bmod 11$ mit $0 \le x \le 10$
   iv. $4^{12} \equiv x \bmod 13$ mit $0 \le x \le 12$
   v. $5^{12} \equiv x \bmod 13$ mit $0 \le x \le 12$
   a. Haben Sie eine Vermutung über eine Regelmäßigkeit? Schreiben Sie sie allgemein auf.
   b. Berechnen Sie nun (möglichst geschickt) $7^{112} \equiv x \bmod 11$ mit $0 \le x \le 10$.

7. Berechnen Sie $3^{132} \equiv x \bmod 11$, wobei x eine Zahl sein soll mit $0 \le x < 11$.
   Anleitung: Berechnen Sie möglichst geschickt zunächst $3 \equiv x_1 \bmod 11$, $3^2 \equiv x_2 \bmod 11$, $3^3 \equiv x_3 \bmod 11$ u.s.w., mit $0 \le x_i < 11$, 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 für die Restklassen von R_7 auf. Nehmen Sie dazu R_6 und R_5 (siehe Skript).
   a. In welchen Zeilen der Multiplikationstafel von R_5, R_6 und R_7 tauchen als Ergebnis alle Restklassen der betreffenden Restklassenmenge auf?
   b. Schreiben Sie alle Lösungen auf für $\bar{a} \cdot \bar{b} = \bar{0}$ in R_5, R_6 und R_7.
   c. 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, R_6 und R_7?
   d. Stellen Sie Vermutungen an, wann Nullteiler auftauchen. Überprüfen Sie die Vermutungen an weiteren Beispielen.

10.

a. 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: Zwei Menschen sind Geschwister, wenn sie dasselbe Elternpaar haben.)

b. Zeigen Sie, dass „sind Aufgabengruppenpartner“ eine Äquivalenzrelation ist.
Erläuterung: Zwei Menschen *a*, *b* sind Aufgabengruppenpartner, wenn sie in einer Vorlesung „XY“ (im selben Semester) ihre Aufgaben in einer Gruppe abgeben.
Was ist die Grundmenge und was sind die Äquivalenzklassen, in die die Grundmenge zerfällt?

11. Zwei Beweise

a. 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 $\overline{a}$ die Äquivalenzklasse bezüglich $\otimes$, in der $a \in M$ liegt.
Dann gilt: $c \in \overline{a}\ \textit{und}\ c \in \overline{b} \Rightarrow \overline{a} = \overline{b}$

12. Graph einer Äquivalenzrelation

Die Abbildung zeigt sechs Punkte, von denen zwei Paare durch eine Strecke verbunden sind. Wir betrachten die Relation „sind verbunden“ auf der Menge dieser sechs Punkte. Jeder Punkt sei (per definition) mit sich selbst verbunden, so dass die Reflexivität immer erfüllt ist. Ergänzen Sie nun weitere Verbindungsstrecken so, dass die Relation „sind verbunden“ auf der Menge dieser sechs Punkte eine Äquivalenzrelation ist.

a. Finden Sie eine Lösung.
b. Finden Sie alle möglichen Lösungen.
c. Beschreiben Sie die aus den Lösungen erkennbare Regelmäßigkeit.

13. (nach einer Mathematik-Olympiaden-Aufgabe (Bundesrunde) für die 8. Klasse)
Zeigen Sie, dass die Zahl $21^{39} + 39^{21}$ durch 45 teilbar ist.