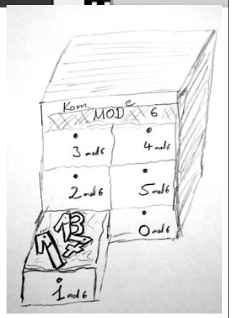
LÖSUNGEN: Erste Übungen zu Kongruenzen



1. *Bestimme den Rest beim Teilen durch 6. Welche Zahlen sind kongruent modulo 6? Schreibe diese mit der zugehörigen Fachnotation auf.*

2; 5; 7; 11; 14; 15; 20; 54; 61; 93; 102; 109; 602

$\mathbf{2 \equiv 2 \text{ mod } 6}$, $\mathbf{5 \equiv 5 \text{ mod } 6}$, $\mathbf{7 \equiv 1 \text{ mod } 6}$, $\mathbf{11 \equiv 5 \text{ mod } 6}$,
$\mathbf{14 \equiv 2 \text{ mod } 6}$, $\mathbf{15 \equiv 3 \text{ mod } 6}$, $\mathbf{20 \equiv 2 \text{ mod } 6}$, $\mathbf{54 \equiv 0 \text{ mod } 6}$,
$\mathbf{61 \equiv 1 \text{ mod } 6}$, $\mathbf{93 \equiv 3 \text{ mod } 6}$, $\mathbf{102 \equiv 0 \text{ mod } 6}$, $\mathbf{109 \equiv 1 \text{ mod } 6}$,
$\mathbf{602 \equiv 2 \text{ mod } 6}$

2. Die Zahlen 15 und 25 sind kongruent modulo 2, denn $15 \equiv 1 \text{ mod } 2$ und $25 \equiv 1 \text{ mod } 2$.
Finde sämtliche natürlichen Zahlen m, für die 15 und 25 kongruent modulo m sind und notiere ebenso.

$\mathbf{15 \equiv 0 \text{ mod } 5}$ **und** $\mathbf{25 \equiv 0 \text{ mod } 5}$, $\mathbf{15 \equiv 5 \text{ mod } 10}$ **und** $\mathbf{25 \equiv 5 \text{ mod } 10}$

3. *Finde mindestens eine Zahl x > 0 so, dass die Relation erfüllt ist:*

a.) $2+x \equiv 4 \text{ mod } 7$ ***x = 2 (oder 9, oder 16, ...)***
b.) $12+x \equiv 4 \text{ mod } 7$ ***x = 6 (oder 13, oder 20, ...)***
c.) $120+x \equiv 5 \text{ mod } 11$ ***x = 6 (oder 17, oder 28, ...)***

4. *Die Kongruenzrelation hat die folgende Eigenschaft, die man in der Mathematik „Transitivität“ nennt:*

Wenn $a \equiv b \text{ mod } m$ *und* $b \equiv c \text{ mod } m$ *, dann gilt auch* $a \equiv c \text{ mod } m$ *.*

Zeige die Transitivität anhand von je zwei verschiedenen Zahlentripeln a, b, c bezüglich der Kongruenzrelation modulo 3 und der Kongruenzrelation modulo 7 auf.

Modulo 3

2, 32, 35: $\mathbf{2 \equiv 32 \text{ mod } 3}$ **,** $\mathbf{32 \equiv 35 \text{ mod } 3}$ ***also ist*** $\mathbf{2 \equiv 35 \text{ mod } 3}$
17, 20, 23: $\mathbf{17 \equiv 20 \text{ mod } 3}$ **,** $\mathbf{20 \equiv 23 \text{ mod } 3}$ ***also ist*** $\mathbf{17 \equiv 23 \text{ mod } 3}$

Modulo 7

5, 75, 82: $\mathbf{5 \equiv 75 \text{ mod } 7}$ **,** $\mathbf{75 \equiv 82 \text{ mod } 7}$ ***also ist*** $\mathbf{5 \equiv 82 \text{ mod } 7}$
4, 39, 46: $\mathbf{4 \equiv 39 \text{ mod } 7}$ **,** $\mathbf{39 \equiv 46 \text{ mod } 7}$ ***also ist*** $\mathbf{4 \equiv 46 \text{ mod } 7}$

Anmerkung: In den Beispielen wurde bereits darauf geachtet, dass die Anwendung der Transitivität „durchscheint“: Möchte man z.B. 5 und 82 mit mod 7 vergleichen, so kann man ganz einfach die 75 als „70 mehr als 5“ und somit kongruent zu 5 mod 7 erkennen, zur 82 fehlt dann nur noch der letzte „7er-Schritt“.

5. ***a.)*** *Zeige, dass die Zahlen 17 und 32 kongruent modulo 3, aber beide nicht kongruent zu 25 modulo 3 sind.*

Individuelle Lösungen möglich, entweder unter der einfachen Berechnung von 17, 32 und 25 jeweils durch 3 mit Rest, oder bereits unter der Betrachtung von Differenzen.

b.) *Bearbeite a.) erneut unter Verwendung der folgenden, in Fachbüchern häufig zu findenden Definition für ganze Zahlen a,b und eine natürliche Zahl m:*

„Man nennt a kongruent zu b modulo m, falls a-b durch m teilbar ist."

Hier muss nun Bezug auf die Differenz genommen werden. 32 – 17= 15, lässt sich durch 3 teilen, 25 – 17 = 8 dagegen nicht.

c.) *Zeige mithilfe der Definition aus b.), dass sowohl die Zahlen -17 und 13, als auch -17 und -5 kongruent modulo 3 sind.*

13 – (-17) = 30 , lässt sich durch 3 teilen.

-17 – (-5) = - 12 , lässt sich durch 3 teilen.

d.) *Man kann zeigen, dass die Definition aus b.) äquivalent zur von uns verwendeten Definition „teilt mit dem gleichen Rest" ist. Beschreibe, welchen Vorteil die „neue" Definition hat.*

Der Vorteil liegt darin, dass auch negative ganze Zahlen in die Kongruenz-Relation aufgenommen werden können. Dies ist bei der Definition über das aus der Grundschulmathematik bekannte „Teilen mit Rest" nicht (ohne Weiteres) möglich.

6. a.) *Über eine Zahl a ist bekannt, dass wenn man sie im WTR durch 4 teilt, hinter dem Komma die Ziffern 75 erscheinen. Welcher Rest entsteht also bei der Rechnung a:4 ?*

Der entstandene Rest erzeugt in Bruchschreibweise ¾ hinter dem Komma, also muss a = 3 sein.

b.) *wie a.), man teilt jedoch durch 5 und erhält die Ziffer 4 hinter dem Komma.*

Der entstandene Rest erzeugt in Bruchschreibweise $0{,}4=\frac{2}{5}$ ***hinter dem Komma, also muss a = 2 sein.***

c.) *wie a.), man teilt jedoch durch 13 und erhält die Ziffernfolge 615384…*

Z.B. mithilfe des WTR findet man heraus: Der entstandene Rest erzeugt in Bruchschreibweise $0{,}615384=\frac{8}{13}$ ***hinter dem Komma, also muss a = 8 sein.***

d.) *Erstelle eine Regel, mit deren Hilfe man im WTR in wenigen Schritten den Rest bestimmen kann. Führe Sie für die folgenden Rechnungen durch:*

7:4, 19:11, 54:7, 91:11, 103:26, 1100:13

Die Regel könnte so lauten:

Führe die Rechnung durch, ersetze die Zahl vor dem Komma durch eine 0 und multipliziere die so erhaltene Zahl mit dem Divisor. Das Ergebnis ist der gesuchte Rest.

$7:4=1{,}75$ ➔ $0{,}75\cdot 4=\underline{3}$, $19:11=1{,}\overline{72}$ ➔ $0{,}\overline{72}\cdot 11=\underline{8}$

$54:7\approx 7{,}7142857$ ➔ $0{,}7142857\cdot 7\approx\underline{5}$,

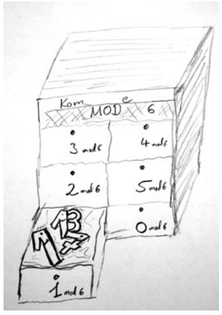
$103:26\approx 3{,}961538$ ➔ $0{,}961538\cdot 26\approx\underline{25}$,

$1100:13\approx 7{,}692308$ ➔ $0{,}692308\cdot 13\approx\underline{9}$

***e.)** (1) Erstelle mit einer Software deiner Wahl ein Programm, das nach Eingabe der Zahlen a und m den Rest der Rechnung a:m bestimmt.*

(2) Erstelle ein zweites Programm, das nach Eingabe dreier Zahlen a, b und m prüft,ob $a \equiv b \mod m$ *erfüllt ist.*

Lösungsbeispiele für die Apps sind im Ordner 7_Apps zu finden.
Sie wurden von Frau Monika Eisenmann zur Verfügung gestellt.



**LÖSUNGEN: Weitere Übungen: Erste Anwendungen

1. *Beim Snowboarden gibt es Sprünge, die „One-Eighty“ (180), „Three-Sixty“ (360), „Five-Forty“ (540) oder „Seven-Twenty“ (720) genannt werden. Dabei gibt der Name an, um wie viel Grad sich der Springer um die eigene Achse dreht – 180°, 360°, 540° oder 720°.*

a.) *Die Sprünge 180 und 540 unterscheiden sich im Resultat von den beiden anderen Sprüngen. Beschreibe den Unterschied.*

Der One-Eighty und der Five-Forty sind Drehungen mit einem Halbkreis am Ende, der Snowboarder wechselt dabei das Bein, das in Fahrtrichtung zeigt (also welches Bein „nach vorne“ zeigt). Die anderen Sprünge sind jeweils Vollkreise, wenn der Snowboarder mit dem linken Bein in Fahrtrichtung nach vorne anfährt, so wird dieses Bein auch nach dem Sprung nach vorne zeigen.

b.) *Man kann nun unendlich viele weitere Sprünge „erfinden“, deren Namen nach demselben Namensgebungsprinzip funktionieren. Welche Sprünge haben das gleiche Resultat wie ein 180? Stelle eine Regel mithilfe der Fachbegriffe aus der Kongruenzrechnung auf.*

Alle Sprünge, die sich aus der Drehwinkel-Addition von 180° und einem ganzzahligen Vielfachen von 360° zusammensetzen, haben dasselbe Resultat.

2. *In einer Ampel werden die Sekunden ab dem Startzeitpunkt hochgezählt. Die Ampel schaltet immer in der Reihenfolge Rot → Rot & Gelb → Grün → Gelb → Rot → … . Die Zeiten zwischen den jeweiligen Umschaltvorgängen verändern sich nicht.*

a.) *Beschreibe den Zusammenhang dieser Ampelschaltung zur Kongruenz-Relation.*

Sei der Startzeitpunkt t_1= 0s. Wenn zu diesem Zeitpunkt Rot erscheint, dann ist nach jeweils 4 Schaltphasen wieder Rot, also zu allen Zeitpunkten t mit $t \equiv 0 \bmod 4$.

Für Rot & Gelb gilt entsprechend der Zeitpunkt t_1= 1s und alle t mit $t \equiv 1 \bmod 4$ ***, usw.***

b*.) *Programmiere eine Ampelschaltung in Scratch oder dem MIT App Inventor 2. Verwende dazu den Operator mod.*

Ein eigenes Lösungsbeispiel für Geogebra und die App (MIT-App-Inventor, Autorin: Monika Eisenmann) sind im Ordner im Ordner 7_Apps zu finden.

In der ersten Lösung für GeoGebra wurden die Schaltphasen mithilfe eines Schiebereglerwertes „mod 4“ verwirklicht. Dies erzeugt stets gleich lange Phasen, was bei einer Ampelschaltung unrealistisch ist. Deshalb wurde noch eine Ampelschaltung mod 8 in GeoGebra bereitgestellt, die (bei eingestellter Animation am Schieberegler) den zeitlichen Unterschieden der Phasen einer Ampelschaltung eher gerecht wird.

3. ** Informiere dich (z.B. im Internet) über das „Jahr-2000-Problem“ (auch „Millenium-Bug“ genannt), fasse es kurz zusammen und stelle den Zusammenhang mit einer Kongruenz-Relation her.*

Kern des „Jahr-2000-Problems“ war die Tatsache, dass viele Anwendungen nicht mit einer exakten Jahreszahl, sondern mit den letzten beiden Ziffern programmiert waren – dies entspricht der Jahreszahl mod 100. Für das Jahr 2000 erwartete man

in diesen Anwendungen Probleme beim Sprung von 99 auf 00, da z.B. 99 größer als 00 ist, obgleich das Jahr 2000 nach dem Jahr 1999 datiert ist. Vor dem Jahr 2000 wurde mit Spannung erwartet, ob / welche / wie gravierende Fehler es geben wird, da ein Überblick über das Ausmaß der Verbreitung dieses Problems fehlte. Aufgrund rechtzeitiger Problematisierung in großen Konzernen gab es letztlich sehr wenige echte Probleme. Einen Überblick darüber findet man z.B. in Wikipedia.

4. ** Kleiner Satz von Fermat (der „Nicht-Primzahl-Test“): Wenn man zu einer Zahl p eine Zahl a findet, die kein Vielfaches von p ist und für die a^{p-1} nicht kongruent zu 1 mod p ist, dann ist p keine Primzahl*

a.) *Zeige, dass mit a=2 gefolgert werden kann, dass 15 keine Primzahl ist.*

$2^{15-1}=16384\equiv 5 \bmod 15$ ***, also nicht kongruent zu 1 mod 15,***

deshalb ist 15 keine Primzahl.

b.) *Finde je eine Zahl mit der gezeigt werden kann, dass 9 bzw. 21 keine Primzahl ist.*

Für die Zahl 9 mit 2: $2^{9-1}=256\equiv 4 \bmod 9$

Für die Zahl 21 mit 3: $3^{21-1}=3486784401\equiv 9 \bmod 21$

Anmerkung: Letzteres geht auch mit 2, mit 3 ist es aber nicht ganz so einfach, den modulo-Rest zu erhalten, da die Zahlen zu groß werden. Ist also vom Lösevorgang her „spannender“. Es funktioniert z.B. in einer Tabellenkalkulation, wenn man die Nachkommastellenanzahl z.B. auf 6 festlegt.

c.)** *Recherchiere die Hintergründe und Anwendungen unter den Stichworten „Kleiner Satz von Fermat“ und „Fermatscher Primzahltest“ und fasse sie übersichtlich zusammen.*

In Wikipedia findet man ausführliche Informationen zu den beiden Stichworten, insbesondere auch die Tatsache, dass der Fermatsche Primzahltest in seiner „Urform“ keine Anwendung findet, es jedoch Weiterentwicklungen dazu gibt (APCRL-Test).

Nachteilig ist, dass Wikipedia (mittlerweile) mathematisch fundiert und daher nicht leicht verständliche Herleitungen bereit hält Eine für <u>mathematisch begabte</u> Schülerinnen und Schüler (daher die Kennzeichnung mit **) geeignete Darstellung der Herleitung des kleinen Fermatschen Satzes findet man beispielsweise im Buch „Mathematik sehen und verstehen“ von Dörte Haftendorn (Springer-Spektrum, Berlin 2016, S. 22 – 26).