6.1 Einführung

Division mit Rest, Kongruenzen, Teilbarkeitslehre und Primzahlen (vgl. Kapitel 7), das sind Stichworte, die den meisten Studierenden des Lehramtes für die Primarstufe viel Kopfzerbrechen bereiten, viel zu schwer und obendrein auch noch sinnlos für den späteren Beruf ...

Wenn man jedoch einmal von der leider weit verbreiteten Meinung Abschied nimmt, in der Grundschule würden nur die vier Grundrechenarten gelehrt (quasi die Standardrechenverfahren der Addition, Subtraktion, Multiplikation und Division als Krone der 4 Jahre Mathematik) und sich mit den eigentlichen Aufgaben und Inhalten des Mathematikunterrichts in der Primarstufe beschäftigt, so stößt man bald auf eine Vielzahl von Fähigkeiten, die im Mathematikunterricht der Grundschule gefördert werden können und sollen.

Wichtig ist hierbei die Unterscheidung zwischen Struktur- und Anwendungsorientierung:

Zum einen ist es Aufgabe des Mathematikunterrichts, daß Kinder „elementare mathematische Fertigkeiten verständig erwerben“[33] und „Grundkenntnisse über Zahlen, Formen und Größen gewinnen“ unter Betonung des „Regelhaften, Gesetzmäßigen und Formelhaften“ (Strukturorientierung des Unterrichts).

Zum anderen - und das wird häufig übersehen - sollen Kinder im Mathematikunterricht „Fähigkeiten zur Lösung mathematischer Probleme“ entwickeln, so daß „Ausschnitte der Lebenswirklichkeit aufgearbeitet werden können“ (Anwendungsorientierung des Unterrichts).

Der Mathematikunterricht soll u.a. die Kinder befähigen,

- „zu mathematisieren“ (Sachprobleme in die Mathematik übersetzen, diese mit mathematischen Mitteln lösen und anschließend die gefundene Lösung auf das Sachproblem übertragen)
- „zu argumentieren“ (Aussagen begründen, Behauptungen anzweifeln und überprüfen, Widersprüche aufdecken)
- „kreativ zu sein“ (Gesetzmäßigkeiten und Beziehungen erkennen und nutzen, Aufgaben systematisch variieren, eigene Lösungswege entwickeln)

Aus diesem Grunde ist es also durchaus sinnvoll, daß angehende Lehrer(innen) Einblick in die Struktur der Zahlen gewinnen, damit sie in der Lage sind, Kindern Probleme zu stellen, welche diese in obigen grundlegenden Fähigkeiten fördern. In Unterkapitel 6.8 werden Beispiele aus der Grundschule vorgestellt, deren mathematischer Hintergrund durchaus komplex ist. Je mehr Einblick der/die Lehrer(in) in die jeweiligen Hintergründe hat, desto flexibler kann er/sie auf die Schüler(innen) und deren Aussagen eingehen, desto einsichtiger kann er/sie den Unterrichtsstoff vermitteln und auf eventuell auftretende Fehler, Miß- und Unverständnisse eingehen.

[33] Alle Zitaten entstammen den Richtlinien Mathematik für die Grundschule in NRW.

6.2 Vorüberlegungen

Es ist 2 Uhr mittags, wie spät ist es in 11 Stunden?

Es ist 7 Uhr. Man überlege sich einmal selbst, wie spät es ist, wenn 9, 14, 25, 36, 50 oder 81 Stunden vergehen.

Denkpause

Mit dem Überlegen fertig? Na, dann geht´s los.

Das Rechnen auf der Uhr, das Lesen von Uhrzeiten auf Analoguhren (nur mit einem Stundenzeiger) unterscheidet sich erheblich von der gewohnten Addition. Auf einem Zifferblatt mit 12 Strichen ist 2+11 nicht 13 sondern 1 (Uhr), da die 13 auf dem Zifferblatt nicht existiert.

Es ist 7 Uhr und der Zeiger läuft beispielsweise 25 Stundeneinteilungen weiter. Nach 12 Stunden wäre es wieder 7 Uhr, nach weiteren 12 ebenso. Es sind bis dahin 24 Stunden vergangen, dies bedeutet, daß es nach 25 Stunden 8 Uhr ist.
Oder anders: $7+25 = 32$, nach 25 Stunden müßte es also 32 Uhr sein, das ist natürlich unsinnig.
Was bedeutet nun 32 für die Analoguhr? Von der 12-Uhr-Stellung muß der Zeiger um 32 Stundeneinteilungen weitergehen[34]. In 32 „steckt“ 2 mal die 12, das heißt der Zeiger dreht zweimal die ganze Runde und kommt dann wieder bei der 12 an. $2 \cdot 12$ sind aber erst 24, zu 32 fehlen noch 8. Der Zeiger muß also von der 12 noch 8 Einteilungen weiterwandern, und dann ist es 8 Uhr.

Es geht bei Uhrzeiten also nicht um die Summe der einzelnen Stunden, ...

$$7+25 = 32$$
$$\downarrow$$
$$32:12 = 2 + (8:12), \text{ also bleibt hier der } \underline{\text{Rest 8}}$$

oder anders: $32 = 2 \cdot 12 + \underline{8}$

... sondern um die Reste, die bei Division der Summen durch 12 übrigbleiben.

Bemerkung:
Die in der Grundschule früher verwendete (und auch heute leider wieder z.T. übliche) Schreibweise $32:12 = 2$ Rest 8 ist formal falsch, da sich an „Rest 8“ nicht mehr erkennen läßt, bei welcher Division der Rest entstanden ist und es daher zu widersprüchlichen Aussagen kommen kann:

Beispiel: $32:12 = 2$ Rest 8 $\wedge$ $26:9 = 2$ Rest 8

$\Rightarrow \quad 32:12 = 26:9$ (TRANS „=“)

$\Rightarrow \quad 2\frac{8}{12} = 2\frac{8}{9}$ das ist ein Widerspruch!

[34] Jede Uhrzeit wird zur 12-Uhr-Stellung in Beziehung gesetzt, die 12-Uhr-Stellung bildet sozusagen den Ausgangspunkt. Zum Beispiel bedeutet 5 Uhr, daß es fünf Stunden nach zwölf ist.

In der Grundschule wird meist die Schreibweise $32:12 = 2 + (8:12)$ benutzt. Alternativ ist auch die Schreibweise $32 = 2 \cdot 12+8$ möglich.

Diese Schreibweise läßt sich wie folgt verallgemeinern:

Definition Division mit Rest

Wird a in Abhängigkeit von b wie folgt dargestellt:
$a = q \cdot b + r$ mit $0 \le r < b$ und $a,b,q,r \in \mathbb{N}_0$, $b \neq 0$,
so nennt man dies D i v i s i o n m i t R e s t .

Anmerkung: Hierbei gibt q an, wie oft b in a „reinpaßt“, der Rest, der übrigbleibt, ist r.

Genauso, wie sich natürliche Zahlen mittels Division mit Rest darstellen lassen, ist dies auch für ganze Zahlen a,b möglich:

a läßt sich bezüglich Division durch b wie folgt schreiben:

$a = q \cdot b + r$ mit $0 \le r < |b|$

und $a,b,q \in \mathbb{Z}$, $b \neq 0$ und (wichtig!) $r \in \mathbb{N}_0$, d.h. die Reste sind immer positiv.

Welche Reste lassen nun die im Uhrenbeispiel vorkommenden Zahlen 9, 14, 25, 36, 50, 81 bei Division durch 12?

$9 = 0 \cdot 12 + \mathbf{9}$
$14 = 1 \cdot 12 + \mathbf{2}$
$25 = 2 \cdot 12 + 1$
$36 = 3 \cdot 12 + 0$
$50 = 4 \cdot 12 + \mathbf{2}$
$81 = 6 \cdot 12 + \mathbf{9}$

Es fällt auf, daß jeweils 9 und 81, sowie 14 und 50 den gleichen Rest lassen. Solche Zahlen nennt man **restgleich** bzgl. der Division durch 12.

Wann lassen natürliche Zahlen a und b also bei Division durch m den gleichen Rest (z.B. 14 und 50 bei Division durch 12)? Offensichtlich dann, wenn sie sich wie folgt schreiben lassen:

$a = q_1 \cdot m + \mathbf{r}$
$b = q_2 \cdot m + \mathbf{r}$

Dabei sind die genauen Werte von q_1 und q_2 hier irrelevant. Wichtig ist lediglich, daß derselbe Rest r vorliegt.

Für „a und b sind restgleich bzgl. Division durch m“ sagt man auch „a **kongruent** b **modulo** m“:

Definition kongruent

Zwei Zahlen $a,b \in \mathbb{Z}$, die bei Division durch eine Zahl $m \in \mathbb{N}$ den gleichen Rest r lassen, heißen k o n g r u e n t m o d u l o m .
In Zeichen: $a \equiv b\ (m) \Leftrightarrow \exists q_1,q_2 \in \mathbb{Z}, r \in \mathbb{N}_0 : (a = q_1 \cdot m + r \ \wedge \ b = q_2 \cdot m + r)$, $0 \le r < m$

Für unser Uhrenbeispiel bedeutet das beispielsweise:

$9 \equiv 81\ (12)$, $14 \equiv 50\ (12)$, $12 \equiv 36\ (12)$

Nach 14 Stunden zeigt der Stundenzeiger auf dieselbe Zahl wie nach 50 Stunden, nämlich 2 Stundeneinteilungen weiter als zuvor.

Anders ausgedrückt:

14 und 50 lassen bei Division durch 12 (eine volle Umdrehung des Stundenzeigers) denselben Rest (2).

Weniger naheliegend ist zum Beispiel die Kongruenz $22 \equiv -2\ (12)$.
(Man beachte $a,b \in \mathbb{Z}$!) Für unser Uhrenbeispiel bedeutet dies:

Wandert der Stundenzeiger um 22 Stundeneinteilungen „vorwärts“ (im Uhrzeigersinn), so entspricht dies einem „Rückwärts“-Wandern (gegen den Uhrzeigersinn) um zwei Stundeneinteilungen: Startet man die Betrachtung jeweils um 12 Uhr, so steht der Zeiger nach dem Wandern beides Mal auf 10 Uhr.

Anders ausgedrückt:

22 und -2 lassen denselben Rest bei Division durch 12:

$22 = 1 \cdot 12 + 10$

$-2 = -1 \cdot 12 + 10$ (Man beachte: $q \in \mathbb{Z}$ (hier: -1), hingegen $r \in \mathbb{N}$ (hier:10))

An unserem Uhrenbeispiel läßt sich eine weitere Beobachtung machen:

$$36 = 3 \cdot 12 + \mathbf{0}$$

Es fällt auf, daß 36 den Rest 0 läßt, also 12 in die 36 restlos „reinpaßt“ (was genau daran liegt, daß nach 36 Stunden der Stundenzeiger dreimal „rum“ ist, d.h. auf derselben Zahl - das ist der Rest bei Division durch 12 - wie zuvor steht).

Für den interessanten Fall, daß eine Zahl bei Division durch eine andere den Rest 0 läßt, gibt es folgende Schreibweise:

Definition Teilbarkeit in $\mathbb{N}_0$

Seien $a,b \in \mathbb{N}_0$.

Es gilt a teilt b ($a \mid b$) genau dann, wenn es eine Zahl $q \in \mathbb{N}_0$ gibt, so daß

$b = q \cdot a + 0$ bzw. $a \cdot q = b$ gilt .

In Zeichen: $a \mid b \Leftrightarrow \exists q \in \mathbb{N}_0 : (a \cdot q = b)$

Jede Teilbarkeitsaussage läßt sich also mit Hilfe der Definition auf eine Gleichung zurückführen.

Von der Darstellung von Zahlen mittels Division mit Rest sind wir zu zwei weiteren zentralen Begriffen der Zahlentheorie gelangt: Kongruenz und Teilbarkeit.

Entgegen der Reihenfolge, in der wir die Begriffe eingeführt haben, werden wir nun mit der Teilbarkeit beginnen (Unterkapitel 6.3) und mit Hilfe der dort bewiesenen Sätze anschließend näher auf die Division mit Rest (6.4) und Kongruenzen (6.5) eingehen.

6.3 Teilbarkeit

6.3.1 Definition

Betrachten wir nun den Begriff der T e i l b a r k e i t , also den Fall, in dem bei Division mit Rest der Rest 0 bleibt, näher.

Zur Erinnerung hier noch mal die Definition:

Definition Teilbarkeit in $\mathbb{N}_0$

Seien $a,b \in \mathbb{N}_0$.
Es gilt a teilt b ($a \mid b$) genau dann, wenn es eine Zahl $q \in \mathbb{N}_0$ gibt, so daß $a \cdot q = b$ gilt.

In Zeichen: $a \mid b \Leftrightarrow \exists q \in \mathbb{N}_0 : (a \cdot q = b)$

a heißt dann T e i l e r von b, b heißt V i e l f a c h e s von a.
1 und b nennt man triviale Teiler von b, alle anderen Teiler heißen echte Teiler von b.

Beispiel: $2 \mid 48$, da $2 \cdot 24 = 48$ (hier ist $q = 24$)

Man beachte, daß $m \mid n$ etwas völlig anderes als $\frac{m}{n}$ oder m:n ist.
Die erste Schreibweise ist eine 🕮 Aussage, während die beiden anderen 🕮 Terme sind (vgl. Kap. 2).

Bemerkung:
Um zu zeigen, daß $a \mid b$ gilt, muß man nicht nur die Existenz einer geeigneten Zahl q zeigen, welche die Gleichung $a \cdot q = b$ erfüllt, sondern auch, daß q tatsächlich Element der Menge $\mathbb{N}_0$ ist.

Wenn man z.B. ein F e r i e n h a u s in Dänemark mieten möchte, geht man in der Regel genauso vor:
Um ein Haus zu mieten, muß man nicht nur in einem Katalog ein geeignetes Haus auswählen, welches die eigenen Ansprüche erfüllt, sondern man muß außerdem noch ins Reisebüro laufen und überprüfen (überprüfen lassen), ob das gefundene Haus auch tatsächlich zu der Menge der noch nicht belegten Häuser gehört. Die Überprüfung der letzten Bedingung ist hierbei für eine erfolgreiche Gestaltung des Sommerurlaubes überaus entscheidend!

Mit Hilfe der vorgestellten Definition läßt sich bei jedem Zahlenpaar (a,b) mit $a,b \in \mathbb{N}_0$ entscheiden, ob $a \mid b$ oder $b \mid a$ erfüllt ist oder nicht. Die Teilbarkeit hält damit eine Beziehung zwischen Zahlen fest und ist daher eine 🕮 Relation (vgl. auch Kap. 8).
Wir sprechen ab jetzt von der T e i l b a r k e i t s r e l a t i o n .

6.3.2 Eigenschaften

Für die Teilbarkeitsrelation gelten viele schöne (häufig sehr naheliegende) Eigenschaften, die zumeist bewiesen werden, indem man die Teilbarkeitsaussage mit Hilfe der Definition in eine Gleichung umformt:

Satz 6.1

Folgende Aussagen gelten für alle $a \in \mathbb{N}_0$:

(i) $1 \mid a$

(ii) $a \mid a$ (Reflexivität von „$\mid$“)

(iii)[35] $a \mid 0$

(iv) $0 \mid a \Rightarrow a = 0$

Beweis:

(i) - (iii): Die Beweise führe der Leser selbst. (**A1**)

(iv) $0 \mid a$

$\Rightarrow \exists q \in \mathbb{N}_0 : (0 \cdot q = a)$ (def. „$\mid$“)

$\Rightarrow a = 0$ ($\forall q \in \mathbb{N}_0$: $(0 \cdot q = 0)$)

t

Satz 6.2

Folgende Aussagen gelten für alle $a,b,c \in \mathbb{N}_0$:

(i) $a \mid b \wedge b \mid a \Leftrightarrow a = b$ (Identitivität von „$\mid$“)[36]

(ii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (Transitivität von „$\mid$“)

Beweis:

(i) Zu zeigen: $a \mid b \wedge b \mid a \Leftrightarrow a = b$

Bevor der eigentliche Beweis erfolgt kann man diese Aussage dem Leser nicht genug ans Herz legen; sie ist Grundlage für eine wichtige Beweisidee in der Zahlentheorie.
Wenn die Gleichheit zweier natürlicher Zahlen a und b gezeigt werden soll, genügt es zu zeigen, daß sowohl a ein Teiler von b als auch b ein Teiler von a ist. Die Identitivität liefert dann die Gleichheit von a und b.

(„$\Rightarrow$“):

1. Fall: $a = 0$

$\Rightarrow 0 \mid b \wedge b \mid 0$ (in die Vor. eingesetzt)

$\Rightarrow b = 0$ (Satz 6.1)

$\Rightarrow a = b$

2. Fall: $a \neq 0$

$a \mid b \wedge b \mid a$

[35] Man mache sich klar, daß $n \mid 0$ nicht dasselbe wie n:0 ist.

[36] Strenggenommen wird nur die Hinrichtung ($a \mid b \wedge b \mid a \Rightarrow a = b$) als Identitivität bezeichnet.

$\Rightarrow \quad \exists q_1 \in \mathbb{N}_0 : (a \cdot q_1 = b) \qquad \clubsuit$

$\wedge \ \exists q_2 \in \mathbb{N}_0 : (b \cdot q_2 = a) \qquad \spadesuit$ (def. „$|$“)

Mit dem Einsetzungsverfahren erhält man:

$\Rightarrow \quad \exists q_1, q_2 \in \mathbb{N}_0 : ((a \cdot q_1) \cdot q_2 = a)$ (♣ in ♠ einsetzen)

$\Rightarrow \quad \exists q_1, q_2 \in \mathbb{N}_0 : (a \cdot (q_1 \cdot q_2) = a)$ (ASS „$\cdot$“)

$\Rightarrow \quad \exists q_1, q_2 \in \mathbb{N}_0 : (q_1 \cdot q_2 = 1)$ (KÜRZ „=“ bzgl. „$\cdot$“, $\underline{a \neq 0}$)

$\Rightarrow \quad q_1 = 1 \ \wedge \ q_2 = 1$ ($q_1, q_2 \in \mathbb{N}_0$)

Das heißt also, daß q_1, q_2 beide 1 sind.
Setzt man diese Werte für q_1 und q_2 nun in ♣ und ♠ ein, so gilt:

$\Rightarrow \quad a \cdot 1 = b \ \wedge \ b \cdot 1 = a$

$\Rightarrow \quad a = b$

(„$\Leftarrow$“):

$a = b \ \Rightarrow \ a|b \ \wedge \ b|a$ (Satz 6.1, REFL „$|$“)

t

(ii) $a|b \ \wedge \ b|c$

$\Rightarrow \quad \exists q_1 \in \mathbb{N}_0 : (a \cdot q_1 = b) \qquad \clubsuit$

$\wedge \ \exists q_2 \in \mathbb{N}_0 : (b \cdot q_2 = c) \qquad \spadesuit$ (def. „$|$“)

Zu zeigen: $a|c$
Es geht also um die Existenz eines q mit der Eigenschaft $a \cdot q = c$.
(Das geeignete 🕮 Ferienhaus muß gefunden werden.)
Woher kann das q nun kommen? Wohl nur aus ♣ und ♠. Dabei fällt auf, daß die rechte Seite von ♠ genau die erwünschte rechte Seite ist, nämlich c. Dagegen ist die Variable a in der linken Seite von ♣ enthalten, nämlich in $a \cdot q_1$.
Um beides in eine Gleichung zu bekommen, setzen wir ♣ in ♠ ein.

$\Rightarrow \quad \exists q_1, q_2 \in \mathbb{N}_0 : ((a \cdot q_1) \cdot q_2 = c)$ (♣ in ♠ eingesetzt)

$\Rightarrow \quad \exists q_1, q_2 \in \mathbb{N}_0 : (a \cdot (q_1 \cdot q_2) = c)$ (ASS „$\cdot$“)

Es wurde also ein geeignetes 🕮 Ferienhaus gefunden ($q_1 \cdot q_2$), jetzt muß noch überprüft werden, ob es noch frei ist.
Es gilt $q_1 \cdot q_2 \in \mathbb{N}_0$, denn das Produkt zweier natürlicher Zahlen ist wieder eine natürliche Zahl (Abgeschlossenheit von $\mathbb{N}_0$ bzgl. „$\cdot$“).

$\Rightarrow \quad a|c$ (def „$|$“, $q_1 \cdot q_2 \in \mathbb{N}_0$)

t

Satz 6.3

Folgende Aussagen gelten für alle $a,b,c \in \mathbb{N}_0$:

(i) $a|b \ \Rightarrow \ a|b \cdot c$

(ii) $a|b \ \wedge \ a|c \ \Rightarrow \ a|b + c$

(iii) $a|b \ \wedge \ a|c \ \Rightarrow \ a|m \cdot b + n \cdot c$ mit $m,n \in \mathbb{N}_0$ beliebig

(iv) $a|b + c \ \wedge \ a|b \ \Rightarrow \ a|c$

(v) $a|b \ \Rightarrow \ a \cdot c|b \cdot c$

(vi) $a \cdot c|b \cdot c \ \wedge \ c \neq 0 \ \Rightarrow \ a|b$

Beweis:

(i) $a|b$

$\Rightarrow$ $\exists q_1 \in \mathbb{N}_0 : (a \cdot q_1 = b)$ (def. „$|$“)

$\Rightarrow$ $\exists q_1 \in \mathbb{N}_0 : ((a \cdot q_1) \cdot c = b \cdot c)$ (Eigenschaft der Gleichheit)

$\Rightarrow$ $\exists q_1 \in \mathbb{N}_0 : (a \cdot (q_1 \cdot c) = b \cdot c)$ (ASS „$\cdot$“)

Die rechte Seite der Gleichung ist jetzt so, wie man sie gern hätte. Entscheidend ist nun, ob $q_1 \cdot c$ aus der Menge $\mathbb{N}_0$ (also ein freies 🕮 Ferienhaus) ist. Da aber das Produkt zweier natürlicher Zahlen wieder eine natürliche Zahl ist, kann die Frage bejaht werden (Abgeschlossenheit von $\mathbb{N}_0$ bzgl. „$\cdot$“).

$\Rightarrow$ $a|b \cdot c$ (def. „$|$“, $q_1 \cdot c \in \mathbb{N}_0$)

t

Diese Aussage kann man auch beweisen, ohne auf die „Ebene der Gleichungen“ zu gehen:

Es gilt nach Voraussetzung $a|b$ und nach Def. „$|$“ gilt $b|b \cdot c$. Mit TRANS „$|$“ läßt sich daraus dann $a|b \cdot c$ folgern.

(ii) $a|b \wedge a|c$

$\Rightarrow$ $\exists q_1, q_2 \in \mathbb{N}_0 : (a \cdot q_1 = b \wedge a \cdot q_2 = c)$ (def. „$|$“)

Auf der rechten Seite soll laut Behauptung b+c stehen, also ist es sinnvoll, die beiden Gleichungen zu addieren.

$\Rightarrow$ $\exists q_1, q_2 \in \mathbb{N}_0 : (a \cdot q_1 + a \cdot q_2 = b + c)$ (Addition der Gleichungen)

$\Rightarrow$ $\exists q_1, q_2 \in \mathbb{N}_0 : (a \cdot (q_1 + q_2) = b + c)$ (DIST)

Die Summe zweier natürlicher Zahlen ist wieder eine natürliche Zahl, d.h. $q_1 + q_2 \in \mathbb{N}_0$ (Abgeschlossenheit von $\mathbb{N}_0$ bzgl. „+“).

$\Rightarrow$ $a|b + c$ (def. „$|$“, $q_1 + q_2 \in \mathbb{N}_0$)

t

(iii) Der Leser versuche, den Beweis zu dieser Aussage mit Hilfe von (i) und (ii) selbst zu führen. (**A2**)

(iv) Der Beweis ist in Ü3 c) gefordert.

(v) $a|b$

$\Rightarrow$ $\exists q \in \mathbb{N}_0 : (a \cdot q = b)$ (def. „$|$“)

$\Rightarrow$ $\exists q \in \mathbb{N}_0 : ((a \cdot q) \cdot c = b \cdot c)$ (Eigenschaft der Gleichheit)

$\Rightarrow$ $\exists q \in \mathbb{N}_0 : (a \cdot (q \cdot c) = b \cdot c)$ (ASS „$\cdot$“)

$\Rightarrow$ $\exists q \in \mathbb{N}_0 : (a \cdot (c \cdot q) = b \cdot c)$ (KOM „$\cdot$“)

$\Rightarrow$ $\exists q \in \mathbb{N}_0 : ((a \cdot c) \cdot q = b \cdot c)$ (ASS „$\cdot$“)

Bemerkung: Die letzten drei Schritte lassen sich mit der Begründung ASS „$\cdot$“, KOM „$\cdot$“ zu einem zusammenfassen.

$\Rightarrow$ $a \cdot c|b \cdot c$ (def. „$|$“, $q \in \mathbb{N}_0$)

t

(vi) Achtung, ganz wichtig: $\underline{c \neq 0}$

$a \cdot c \mid b \cdot c$

$\Rightarrow \quad \exists q \in \mathbb{N}_0 : ((a \cdot c) \cdot q = b \cdot c)$ (def. „$\mid$“)

$\Rightarrow \quad \exists q \in \mathbb{N}_0 : ((a \cdot q) \cdot c = b \cdot c)$ (ASS „$\cdot$“, KOM „$\cdot$“)

$\Rightarrow \quad \exists q \in \mathbb{N}_0 : (a \cdot q = b)$ (KÜRZ „$\cdot$“ bzgl. „=“, $\underline{c \neq 0}$)

$\Rightarrow \quad a \mid b$ (def. „$\mid$“, $q \in \mathbb{N}_0$)

t

Satz 6.4

Folgende Aussagen gelten für alle $a,b \in \mathbb{N}_0$:

(i) $a \mid b \ \wedge \ b \neq 0 \quad \Rightarrow \quad a \leq b$

(ii) $b < a \ \wedge \ b \neq 0 \quad \Rightarrow \quad a \nmid b$

Beweis:

(i) $a \mid b$

$\Rightarrow \quad \exists q \in \mathbb{N}_0 : (a \cdot q = b)$ ☎ (def. „$\mid$“)

Es gilt sogar $q \in \mathbb{N}$, denn $q \neq 0$, da laut Voraussetzung $b \neq 0$. (Wäre $q = 0$, wäre auch $a \cdot q = 0$ und damit $b = 0$.)

$q \in \mathbb{N}$

$\Rightarrow \quad 1 \leq q$

$\Rightarrow \quad 1 \cdot a \leq q \cdot a$ (MON „$\cdot$“ bzgl. „$\leq$“)

$\Rightarrow \quad a \leq a \cdot q$ (KOM „$\cdot$“)

$\Rightarrow \quad a \leq b$ (☎)

t

(ii) (indirekter Beweis)

Annahme: $a \mid b$

$\Rightarrow \quad a \leq b$ ((i), $b \neq 0$)

das ist ein Widerspruch zu $b < a$ (wegen TRICH),

d.h. die Annahme ist falsch und damit gilt die Behauptung.

t

Die Teilbarkeit kann analog zur Definition der Teilbarkeit in $\mathbb{N}_0$ auch in $\mathbb{Z}$ definiert werden:

Definition Teilbarkeit in $\mathbb{Z}$

Seien $n,m \in \mathbb{Z}$.
Es gilt m teilt n ($m \mid n$) genau dann, wenn es eine Zahl $q \in \mathbb{Z}$ gibt, so daß $m \cdot q = n$ gilt.
In Zeichen: $m \mid n \;\Leftrightarrow\; \exists q \in \mathbb{Z}: (m \cdot q = n)$

Beispiel: $-3 \mid 9$, da $(-3) \cdot (-3) = 9$ und $-3 \in \mathbb{Z}$ (hier ist $q = -3$)

Bemerkung:
Auch hier ist wieder eine geeignete Zahl q (ein 🕮 Ferienhaus in Nordeuropa) zu suchen, und anschließend ist zu überprüfen, ob dieses q aus der Menge $\mathbb{Z}$ ist (also ob das Ferienhaus frei ist).
Die Sätze (6.1) – (6.4) lassen sich zum Großteil auch auf $\mathbb{Z}$ übertragen, dazu müssen einige Aussagen abgeändert werden (diese sind fettgedruckt) :

Satz 6.5

Folgende Aussagen gelten für alle $a,b,c \in \mathbb{Z}$.

(i) $1 \mid a \;\wedge\; a \mid a \;\wedge\; a \mid 0$

(ii) $0 \mid a \;\Rightarrow\; a = 0$

(iii) $a \mid b \;\wedge\; b \mid a \;\Leftrightarrow\; |a| = |b|$

(iv) $a \mid b \;\wedge\; b \mid c \;\Rightarrow\; a \mid c$ (Transitivität von „$\mid$“ in $\mathbb{Z}$)

(v) $a \mid b \;\Rightarrow\; a \mid b \cdot c$

(vi) $a \mid b \;\wedge\; a \mid c \;\Rightarrow\; a \mid b+c$

(vii) $a \mid b \;\wedge\; a \mid c \;\Rightarrow\; a \mid m \cdot b + n \cdot c$ mit $m,n \in \mathbb{Z}$ beliebig

(viii) $a \mid b \;\Rightarrow\; a \cdot c \mid b \cdot c$

(ix) $a \cdot c \mid b \cdot c \;\wedge\; c \neq 0 \;\Rightarrow\; a \mid b$

(x) $a \mid b \;\wedge\; b \neq 0 \;\Rightarrow\; |a| \leq |b|$

Bemerkung:
Die Beweise der Sätze in $\mathbb{N}_0$ lassen sich mit geringen Abwandlungen auf die Sätze in $\mathbb{Z}$ übertragen.

Auch wenn dieses Unterkapitel dem/der Leser(in) etwas trocken erscheinen mag, so sollte er/sie beachten, daß die hier vorgeführten Beweise als Fundgrube für Beweisideen dienen können, da sie Beweisstrukturen enthalten, die für den Nachweis von Teilbarkeitsaussagen typisch sind.

Nun erfolgen Betrachtungen über die allseits beliebten Begriffe ggT und kgV, die einerseits in der Schule eine wesentliche Rolle spielen (z.B. Bruchrechnung) und andererseits zentrale Begriffe in der elementaren Zahlentheorie sind.

6.3.3 Der größte gemeinsame Teiler (ggT)

Die Klasse 4b der Grundschule Wassermaus möchte ihre Spielecke mit (quadratischen) Teppichfliesen auslegen. Die (rechteckige) Spielecke ist 3,2m (320cm) lang und 2,4m (240cm) breit. Im ortsansässigen Baumarkt gibt es quadratische Teppichfliesen verschiedenster Größe (in 1cm-Abstufung). Die Lehrerin überlegt mit ihren Schüler(innen), welche Fliesen geeignet sind.

Was rätst Du der Klasse?

Denkpause

Da weder die Lehrerin noch die Schüler(innen) Lust haben, ihre freie Zeit mit dem Zuschneiden von Fliesen zu verbringen, wählen sie Fliesen, mit denen man ohne Zuschneiden die gesamte Spielecke auslegen kann. Offensichtlich muß dazu die Zahl, welche die Länge der Teppichfliesen in cm angibt, sowohl restlos in 320 als auch restlos in 240 enthalten sein, damit kein Verschnitt entsteht. Anders ausgedrückt bedeutet dies, daß diese Zahl sowohl ein Teiler von 320 als auch von 240 sein muß.

Um diese Zahl zu finden, scheint es sinnvoll zunächst alle Teiler von 320 und 240 zu notieren, d.h. die Menge der Teiler dieser Zahlen in aufzählender Form anzugeben. Die Menge der Teiler von 320 nennt man dabei T e i l e r m e n g e von 320 (nicht zu verwechseln mit 🕮 Teilmenge!), abgekürzt mit T(320), die Menge der Teiler von 240 entsprechend T(240):

$T(320) = \{1,2,4,5,8,10,16,20,32,40,64,80,160,320\}$

$T(240) = \{1,2,3,4,5,6,8,10,12,15,16,20,24,30,40,48,60,80,120,240\}$

Definition Teilermenge

Sei $n \in \mathbb{N}$, dann heißt die Menge aller positiven Teiler von n die T e i l e r m e n g e von n (T(n)).[37]

In Zeichen: $T(n) = \{k \mid k \in \mathbb{N} \wedge k \mid n\}$

Die von uns gesuchte Zahl, welche die Länge der Teppichfliesen in cm angibt, soll ja sowohl ein Teiler von 320 als auch von 240, also ein g e m e i n s a m e r T e i l e r von 320 und 240 sein.

Diese Zahl muß demnach sowohl in T(320) als auch in T(240) enthalten sein, d.h. sie muß Element der 🕮 Schnittmenge von T(320) und T(240) sein:

$T(320) = \{\mathbf{1},\mathbf{2},\mathbf{4},\mathbf{5},\mathbf{8},\mathbf{10},\mathbf{16},\mathbf{20},32,\mathbf{40},64,\mathbf{80},160,320\}$

$T(240) = \{\mathbf{1},\mathbf{2},3,\mathbf{4},\mathbf{5},6,\mathbf{8},\mathbf{10},12,15,\mathbf{16},\mathbf{20},24,30,\mathbf{40},48,60,\mathbf{80},120,240\}$

Also gilt: $T(240) \cap T(320) = \{1,2,4,5,8,10,16,20,40,80\}$

[37] Teilermengen sind nie leer, da jede Zahl mindestens 1 und sich selbst als Teiler hat.

Definition gemeinsamer Teiler

Seien $n,m \in \mathbb{N}$, dann heißt jedes Element k der Schnittmenge der Teilermengen T(n) und T(m) g e m e i n s a m e r T e i l e r von n und m.

In Zeichen: k ist gemeinsamer Teiler von n und m $\Leftrightarrow$ $k \in T(n) \cap T(m)$

Für die Zahl, welche die Länge der Teppichfliesen in cm angibt, kommt also jede der Zahlen 1,2,4,5,8,10,16,20,40 und 80 in Frage. Teppichfliesen der Größe 1cm x 1cm versprechen allerdings viel Arbeit beim Verlegen, so daß die Lehrerin sich mit den Schüler(innen) schnell darauf einigt, möglichst große Fliesen auszuwählen, um den Verlegeaufwand tunlichst gering zu halten. Gesucht ist nun also die größte Zahl, die sowohl ein Teiler von 320 als auch von 240 ist, d.h. der größte gemeinsame Teiler der beiden Zahlen. Dies ist offensichtlich das größte Element der Menge der gemeinsamen Teiler $T(320) \cap T(240)$.

Das größte Element einer Menge nennt man auch das Maximum dieser Menge. Dies läßt sich wie folgt definieren:

Definition Maximum

Das M a x i m u m einer Menge M von Zahlen ist das größte Element der Menge.

In Zeichen: $\max(M) \in M \wedge \forall m \in M: (m \leq \max(M))$

Beispiele: $\max(\{3,6,9,12\}) = 12$, $\max(\mathbb{Z}^-) = -1$

Der größte gemeinsame Teiler ist dementsprechend das Maximum der Menge der gemeinsamen Teiler:

Definition größter gemeinsamer Teiler (ggT)

Seien $n,m \in \mathbb{N}$, dann heißt das Maximum der Menge der gemeinsamen Teiler von n und m der g r ö ß t e g e m e i n s a m e T e i l e r (ggT) von n und m.

In Zeichen: $ggT(n,m) = \max(T(n) \cap T(m))$

Die von uns gesuchte Zahl, der größte gemeinsame Teiler von 320 und 240, ist folglich $\max(T(320) \cap T(240)) = \max(\{1,2,4,5,8,10,16,20,40,80\}) = 80$. Die schlaue Klasse 4b wählt demzufolge die Teppichfliesen der Größe 80cm x 80cm und verfügt schon bald über eine neugestaltete Spielecke.[38]

Der Begriff ggT beinhaltet, daß der ggT(n,m) sowohl Teiler von n als auch von m ist, und daß es keinen Teiler von n und m gibt, der größer als der ggT(n,m) ist:

Satz 6.6 (Satz ggT)

Seien $n,m \in \mathbb{N}$, dann gilt:

(i) $ggT(n,m) \mid n \wedge ggT(n,m) \mid m$

(ii) $\forall t \in \mathbb{N}: (t \mid n \wedge t \mid m \Rightarrow t \leq ggT(n,m))$

[38] Zur Gestaltung einer Spielecke vgl. Wallrabenstein, Wulf: Das Zelt, unser Kreis und meine Nische. Von Spielräumen zu Freiräumen. In: Spielzeit. Friedrich Jahresheft XIII, 1995.

Beweis:

(i) Da ggT(n,m) ein Element der Schnittmenge von T(n) und T(m) ist, folgt die Behauptung sehr schnell mit der Definition von Schnittmenge.

$ggT(n,m) = \max(T(n) \cap T(m))$

$\Rightarrow ggT(n,m) \in T(n) \cap T(m)$ (def. Maximum)

$\Rightarrow ggT(n,m) \in T(n) \ \wedge \ ggT(n,m) \in T(m)$ (def. „$\cap$“)

$\Rightarrow ggT(n,m) \mid n \ \wedge \ ggT(n,m) \mid m$ (def. Teilermenge)

(ii) Da der ggT(n,m) das Maximum der Menge ist, sind aller weiteren Teiler von n und m kleiner als derselbe.

$t \mid n \wedge t \mid m$

$\Rightarrow t \in T(n) \wedge t \in T(m)$ (def. Teilermenge)

$\Rightarrow t \in T(n) \cap T(m)$ (def. „$\cap$“)

$\Rightarrow t \leq ggT(n,m)$ (def. „ggT“)

t

Neben der - recht aufwendigen - Bestimmung des ggT zweier Zahlen über die Bildung der Menge der gemeinsamen Teiler existieren weitere Verfahren, die sich vor allem bei größeren Zahlen anbieten: der Euklidische Algorithmus (vgl. Unterkap. 6.6) und die Bestimmung des ggT über die Primfaktorzerlegungen der zu untersuchenden Zahlen (vgl. Unterkap. 7.6).

6.3.4 Das kleinste gemeinsame Vielfache (kgV)

Der Halleysche Komet kehrt alle 76 Jahre in Sonnennähe zurück, ein anderer periodischer Komet alle 95 Jahre. Irgendwann näherten sich beide Kometen gleichzeitig der Sonne. Nach wieviel Jahren kehren beide Kometen gleichzeitig zurück?

Denkpause

Offensichtlich ist nach Zahlen gesucht, in denen sowohl 76 als auch 95 restlos enthalten ist, also nach Zahlen, die sowohl ein Vielfaches von 76 als auch von 95 sind.

Um diese Zahlen zu finden, scheint es sinnvoll (entsprechend der Vorgehensweise bei der Bestimmung des ggT in 6.3.3), die Vielfachen von 76 und 95 in aufzählender Form anzugeben. Die Menge der Vielfachen von 76 nennt man V i e l f a c h e n m e n g e von 76, abgekürzt mit V(76), die Menge der Vielfachen von 95 entsprechend V(95):

V(76) = {76, 152, 228, 304, 380, 456, 532, 608, 684, 760, 836, ...}

V(95) = {95, 190, 285, 380, 475, 570, 665, 760, 855, ...}

Definition Vielfachenmenge

Sei $n \in \mathbb{N}$, dann heißt die Menge aller positiven Vielfachen von n die Vielfachenmenge von n (V(n)).
In Zeichen: $V(n) = \{k \mid k \in \mathbb{N} \wedge n \mid k\}$

Die von uns gesuchten Zahlen sollen ja sowohl Vielfache von 76 als auch von 95, also gemeinsame Vielfache von 76 und 95 sein.

Diese Zahlen müssen demnach sowohl in V(76) als auch in V(95) enthalten sein, d.h. sie müssen Elemente der 🕮 Schnittmenge von V(76) und V(95) sein:

V(76) = {76, 152, 228, 304, **380**, 456, 532, 608, 684, **760**, 836, ...}

V(95) = {95, 190, 285, **380**, 475, 570, 665, **760**, 855, ...}

Also gilt: $V(76) \cap V(95) = \{380, 760, ...\}$

Definition gemeinsames Vielfaches

Seien $n,m \in \mathbb{N}$, dann heißt jedes Element k der Schnittmenge der Vielfachenmengen V(n) und V(m) gemeinsames Vielfaches von n und m.

In Zeichen: k ist gemeinsames Vielfaches von n und m $\Leftrightarrow$ $k \in V(n) \cap V(m)$

Für die Zahlen, welche die Anzahl der Jahre bis zum erneuten Erscheinen beider Kometen angeben, kommen folglich die Zahlen 380 und 760 und weitere in Betracht. Alle in Frage kommenden Zahlen können natürlich so nicht ermittelt werden, da Vielfachenmengen unendlich sind und sie daher auch nur ausschnittsweise in aufzählender Form angegeben werden können.

Nach wieviel Jahren können wir denn mit dem nächsten gleichzeitigen Erscheinen der beiden Kometen rechnen?

Gesucht ist nun also die kleinste Zahl, die sowohl ein Vielfaches von 76 als auch von 95 ist. Dies ist offenkundig das kleinste Element der Menge der gemeinsamen Vielfachen (hier: $V(76) \cap V(95)$).

Das kleinste Element einer Menge nennt man auch das Minimum dieser Menge, dieses läßt sich wie folgt definieren:

Definition Minimum

Das Minimum einer Menge M von Zahlen ist das kleinste Element der Menge.

In Zeichen: $\min(M) \in M \wedge \forall m \in M: (\min(M) \leq m)$

Beispiele: $\min(\{3,6,9,12,...\}) = 3$, $\min(\mathbb{N}) = 1$

Das kleinste gemeinsame Vielfache ist dementsprechend das Minimum der Menge der gemeinsamen Vielfachen:

Definition kleinstes gemeinsames Vielfache (kgV)

Seien $n,m \in \mathbb{N}$, dann heißt das Minimum der Menge der gemeinsamen Vielfache von n und m der k l e i n s t e g e m e i n s a m e V i e l f a c h e (kgV) von n und m.
In Zeichen: $kgV(n,m) = \min(V(n) \cap V(m))$

Die von uns gesuchte Zahl, das kleinste gemeinsame Vielfache von 76 und 95, ist demzufolge $\min(V(76) \cap V(95)) = \min(\{380, 760, ...\}) = 380$.

Das nächste Mal kehren die beiden Kometen demnach nach 380 Jahren gleichzeitig in Sonnennähe zurück.

Der Begriff kgV beinhaltet, daß der kgV(n,m) sowohl Vielfaches von n als auch von m ist, und daß es kein Vielfaches von n und m gibt, das kleiner ist als das kgV(n,m):

Satz 6.7 (Satz kgV)

Seien $n,m \in \mathbb{N}$, dann gilt:
(i) $n \mid kgV(n,m) \wedge m \mid kgV(n,m)$
(ii) $\forall k \in \mathbb{N}: (n \mid k \wedge m \mid k \Rightarrow kgV(n,m) \leq k)$

Dem/der aufmerksamen Leser(in) wird nicht entgangen sein, daß dieser Satz dem Satz ggT auffallend ähnlich ist. Auch der Beweis verläuft völlig analog und wird deshalb hier nicht durchgeführt.

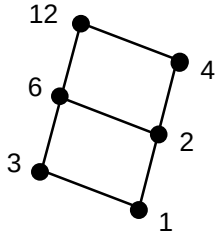
Eine weitere, nur bedingt einsetzbare Methode zur Bestimmung von ggT und kgV läßt sich für die im nächsten Abschnitt vorgestellten Diagramme entwikkeln.

6.3.5 Hasse-Diagramme

Eine anschauliche Möglichkeit, die Teilbarkeitsrelation innerhalb der Teilermenge einer natürlichen Zahl a zu verdeutlichen, bieten die sogenannten **H a s s e - D i a g r a m m e** .

Zunächst ein Beispiel:

$T(12) = \{1,2,3,4,6,12\}$



Man interpretiert ein solches Diagramm wie folgt:

a teilt b genau dann, wenn man von dem zu a gehörenden Punkt auf einem aufsteigenden Weg zu dem zu b gehörenden Punkt gelangen kann;
eine direkte Verbindung zwischen den Punkten der Zahlen a und b gibt es nur dann, wenn es in der zugrunde liegenden Teilermenge keine Zahl c gibt, für die gilt: $a|c \wedge c|b$ (denn dann würde die Verbindung von a nach b über c gehen).
Obigem Diagramm ist also beispielsweise zu entnehmen: $3|6$, $3|12$, $2|6$, $2|4$, $2|12$, $3\nmid 4$ [da man nicht auf einem ausschließlich aufsteigenden Weg von 3 zu 4 gelangen kann] usw.

Hasse-Diagramme sind außerdem bedingt zur Bestimmung der gemeinsamen Teiler und insbesondere des ggT sowie des kgV einsetzbar und eignen sich gut zur Veranschaulichung der Zusammenhänge zwischen diesen Begriffen im Unterricht.

Zur weiteren Vertiefung des Umgangs mit Hasse-Diagrammen sei auf Ü5 verwiesen.

LÖ S U N G E N der Arbeitsaufgaben dieses Unterkapitels:

A1 (i) Sei $a \in \mathbb{N}_0$ beliebig gewählt.
$\exists q \in \mathbb{N}_0: (1 \cdot q = a)$, nämlich $q = a$
$\Rightarrow 1|a$ (Def. „|“)

bzw. einfacher: Es gilt $1 \cdot a = a \Rightarrow 1|a$ (Def. „|“)

(ii) Sei $a \in \mathbb{N}_0$ beliebig gewählt.
$\exists q \in \mathbb{N}_0: (a \cdot q = a)$, nämlich $q = 1$
$\Rightarrow a|a$ (Def. „|“)

(iii) Sei $a \in \mathbb{N}_0$ beliebig gewählt.
$\exists q \in \mathbb{N}_0: (a \cdot q = 0)$, nämlich $q = 0$
$\Rightarrow a|0$ (Def. „|“)

A2 Zu zeigen: $a|b \wedge a|c \Rightarrow a|m \cdot b + n \cdot c$ mit $m,n \in \mathbb{N}_0$ beliebig

Aus $a|b$ folgt nach Satz 6.3 (i) $a|b \cdot m$, aus $a|c$ folgt $a|c \cdot n$ ($m,n \in \mathbb{N}_0$ beliebig).
Aus diesen beiden Teilbarkeitsaussagen läßt sich nun mit Hilfe von Satz 6.3 (ii) $a|b \cdot m + c \cdot n$ schließen und nach Anwendung des Kommutativgesetzes der Multiplikation folgt dann die Behauptung.

Anmerkung: Ein Beweis über die Def. „|“ ist auch möglich (vgl. Ü4).

6.4 Division mit Rest

Auf die in Unterkapitel 6.2 eingeführte Schreibweise der Division mit Rest soll nun näher eingegangen werden.

Zur Erinnerung:

Definition Division mit Rest

Wird a in Abhängigkeit von b wie folgt dargestellt:
$a = q \cdot b + r$ mit $0 \le r < b$ und $a,b,q,r \in \mathbb{N}_0$, $b \neq 0$,
so nennt man dies D i v i s i o n m i t R e s t .

Entscheidend für die Verwendung der Division mit Rest ist die Tatsache, daß solche q und r für beliebige natürliche Zahlen a,b ($b \neq 0$) existieren, und zwar - dies ist besonders spannend - eindeutig existieren. Wenn man also zu vorgegebenen natürlichen Zahlen a und b ein q und ein r gefunden hat, so kann man sicher sein, daß dies die einzige Möglichkeit ist, a in Abhängigkeit von b in obiger Weise darzustellen:

Satz 6.7 (Satz über Division mit Rest)

Seien $a \in \mathbb{N}_0$, $b \in \mathbb{N}$.
Dann existieren eindeutig Zahlen $q,r \in \mathbb{N}_0$, so daß gilt:
$a = q \cdot b + r$ mit $0 \le r < b$
In Zeichen: $\forall a \in \mathbb{N}_0 \ \forall b \in \mathbb{N}: (\dot{\exists} q,r \in \mathbb{N}_0: (a = q \cdot b + r \ \wedge \ 0 \le r < b))$

Man überlege, warum $b = 0$ in der Formulierung des Satzes ausgeschlossen wurde. (**A3**)

Beweis:
In dem Beweis ist zweierlei zu zeigen:

1) Es erfolgt ein sogenannter Existenzbeweis, in dem gezeigt wird, daß es zu jedem Zahlenpaar (a,b) auch ein passendes Zahlenpaar (q,r) gibt (mit $0 \le r < b$, weil r sonst kein Rest ist).

2) Es wird gezeigt, daß die gefundenen Zahlen q und r auch eindeutig bestimmt sind, das heißt, daß es nicht noch ein anderes Zahlenpaar gibt, das die Bedingungen ebenfalls erfüllt.

ad **1)**:
Beim Beweis verwenden wir die 🕮 Wohlordnungseigenschaft (Minimalprinzip) welches aussagt, daß es in jeder nicht leeren Menge ein kleinstes Element gibt. Alternativ wäre beispielsweise auch ein Beweis über das 🕮 Prinzip des Archimedes möglich.

Seien $a \in \mathbb{N}_0, b \in \mathbb{N}$ beliebig gewählt.

1. Fall: $a = 0$

$\Rightarrow \ a = 0 \cdot b + 0$,

d.h. es existieren $q,r \in \mathbb{N}_0$ mit $0 \le r < b$ (nämlich $q = 0$, $r = 0$)

2. Fall: $a > 0$

Vorüberlegungen:

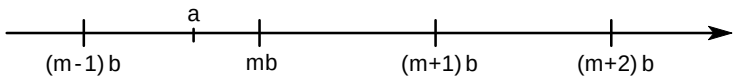
Wir suchen nun auch in diesem Fall ein q (und ein zugehöriges r) mit $a = q \cdot b + r$. Dieses $q \cdot b$ ist das größte Vielfache von b, das kleiner als (oder gleich) a ist, da r die Bedingung $0 \leq r < b$ erfüllen muß. Daher ist es sinnvoll, die Vielfachen von b näher zu betrachten.

Leider steht uns kein Maximalprinzip zur Verfügung, mit dem wir dann das größte Vielfache < a bestimmen könnten. Immerhin verfügen wir über ein Minimalprinzip.

Wie hilft uns dieses weiter?

Mit dem Minimalprinzip können wir das kleinste Vielfache von b, das größer als a (oder gleich a) ist, bestimmen (nennen wir dieses $m \cdot b$). Das nächstkleinere Vielfache von b ($(m-1) \cdot b$) ist dann natürlich kleiner als a und damit das größte Vielfache < a.

Der/die Leser(in) mache sich diesen Zusammenhang an folgendem Zahlenstrahl klar:



Nun zurück zu unserem Beweis, in dem wir zuerst eine Menge konstruieren, die alle Faktoren n enthält, mit denen das Produkt $n \cdot b$ größer als a (oder gleich) ist (z.B. die im Zahlenstrahl aufgeführten m, m+1 und m+2 liegen in dieser Menge):

Sei $M = \{n \in \mathbb{N} \mid n \cdot b \geq a\}$

Idee: Zuerst soll gezeigt werden, daß M nicht leer ist, damit das Wohlordnungsprinzip (Minimalprinzip) auch anwendbar ist.

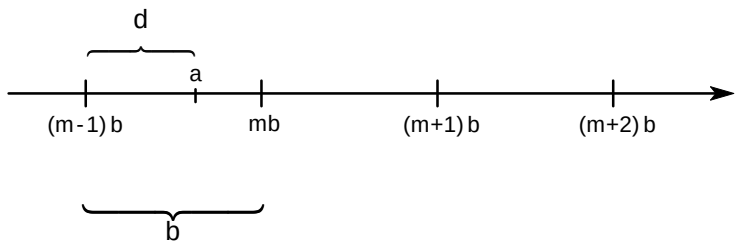
$a \in M$, denn $a \cdot b \geq a$ ($b \in \mathbb{N}$)

$\Rightarrow M \neq \emptyset$

$\Rightarrow \exists m \in \mathbb{N}: (m = \min(M))$ (WOHLORD, $M \subseteq \mathbb{N}$)

$\Rightarrow \exists m \in \mathbb{N}: ((m-1) \cdot b < a)$ (denn: Ann.: $(m-1) \cdot b \geq a \Rightarrow m-1 \in M$ ein Widerspruch zu $m = \min(M)$, da $m-1 < m$)

$\Rightarrow \exists m,d \in \mathbb{N}: ((m-1) \cdot b + d = a)$ g (def. „<“)



Nun wäre es schön, wenn d < b gelten würde (das er gilt erkennt man an obigem Zahlenstrahl). Denn dann hätten wir ja ein passendes q mit zu-gehörigem r gefunden

(nämlich q = m – 1 und r = d). Der Fall $d = b$ wäre auch o.k., da sich dann $a = m \cdot b$ ergeben würde (also: $q = m$ und $r = 0$). Um diese beiden schönen Fälle zu erhalten, versuchen wir, den Fall b < d auszuschließen:

Annahme: $b < d$

$\Rightarrow \quad \exists k \in \mathbb{N}: (b + k = d)$ (def. „<“)

$\Rightarrow \quad \exists k \in \mathbb{N}: ((m-1) \cdot b + (b + k) = (m-1) \cdot b + d)$ (Eigenschaft „=“)

$\Rightarrow \quad \exists k \in \mathbb{N}: ((m-1) \cdot b + (b + k) = a)$ (g)

$\Rightarrow \quad \exists k \in \mathbb{N}: (m \cdot b - b + b + k = a)$ (DIST, ASS)

$\Rightarrow \quad \exists k \in \mathbb{N}: (m \cdot b + k = a)$

$\Rightarrow \quad m \cdot b < a$ (Def. „<“, $k \in \mathbb{N}$)

Das ist ein Widerspruch zu $m \in M$, also ist die Annahme falsch und wegen TRICH gilt: $d \le b$.

$d \le b \quad \Rightarrow \quad d < b \ \vee \ d = b$

1. Fall : $d = b$

$\Rightarrow \quad (m-1) \cdot b + b = a$ (g)

$\Rightarrow \quad ((m-1) + 1) \cdot b = a$ (DIST)

$\Rightarrow \quad m \cdot b = a$

$\Rightarrow \quad a = m \cdot b + 0$

Also erfüllen hier $q = m$ und $r = 0$ die Behauptung.

2. Fall : $d < b$

Da gilt: $a = (m-1) \cdot b + d$ (siehe g) und $0 \le d < b$, erfüllen $q = m - 1$ und $r = d$ die Behauptung.

Damit erhalten wir in allen Fällen, daß es zu einem beliebigen Zahlenpaar (a,b) ein passendes Zahlenpaar (q,r) gibt mit $a = q \cdot b + r$ und $0 \le r < b$.

ad **2)**: Zu zeigen ist nun, daß die in 1) gefundenen q und r auch eindeutig sind, das heißt, daß es außer diesen nicht noch andere Zahlen gibt, die die Bedingungen des Satzes erfüllen.

Seien $a \in \mathbb{N}_0$ und $b \in \mathbb{N}$ gegeben mit

$a = q_1 \cdot b + r_1 \quad$ mit $0 \le r_1 < b$, $q_1, r_1 \in \mathbb{N}_0$

$a = q_2 \cdot b + r_2 \quad$ mit $0 \le r_2 < b$, $q_2, r_2 \in \mathbb{N}_0$

Daß mindestens eine solche Darstellung für a und b existiert, haben wir eben unter 1) bewiesen. Nun soll gezeigt werden, daß es nur eine Darstellung gibt, es sich also stets um dieselben q und r handelt. Zu zeigen ist also: $q_1 = q_2$ und $r_1 = r_2$.

$$\left.\begin{aligned} a &= q_1 \cdot b + r_1 \\ a &= q_2 \cdot b + r_2 \end{aligned}\right\} \quad \Rightarrow \quad q_1 \cdot b + r_1 = q_2 \cdot b + r_2$$

$$\Rightarrow \quad q_1 \cdot b = q_2 \cdot b + (r_2 - r_1) \qquad \text{❄}$$

Wenn $r_1 = r_2$ gilt, läßt sich aus ❄ direkt auf die Gleichheit von q_1 und q_2 schließen:

$$\left.\begin{array}{l} q_1 \cdot b = q_2 \cdot b + (r_2 - r_1) \\ r_1 = r_2 \end{array}\right\} \quad \Rightarrow \quad q_1 \cdot b = q_2 \cdot b$$

$$\Rightarrow \quad q_1 = q_2 \qquad (\text{KÜRZ „=“ bzgl. „}\cdot\text{“, } b \neq 0)$$

Jetzt ist noch zu zeigen, daß $r_1 = r_2$ auch tatsächlich gilt:

(indirekter) Beweis:

Annahme: $r_1 \neq r_2$

$\Rightarrow \quad r_1 < r_2 \ \vee \ r_2 < r_1$ (TRICH)

o.B.d.A. $r_1 < r_2$

$\Rightarrow \quad r_2 - r_1 \in \mathbb{N}$ (def. „–“)

Es gilt: $q_1 \cdot b = q_2 \cdot b + (r_2 - r_1)$ (❄)

$\Rightarrow \quad b \mid q_2 \cdot b + (r_2 - r_1)$ (def. „|“)

Wenn b eine Summe $(q_2 \cdot b + (r_2 - r_1))$ und den einen Summanden $(q_2 \cdot b)$ teilt, dann muß b auch den zweiten Summanden $(r_2 - r_1)$ teilen (vgl. auch Satz 6.3(iv)):

$\Rightarrow \quad b \mid r_2 - r_1$

$\Rightarrow \quad b \leq r_2 - r_1 \qquad E$ ($r_2 - r_1 \in \mathbb{N}$, Satz 6.4)

Das kann aber nicht gelten, denn:

Aus der Voraussetzung $(0 \leq)\ r_2 < b$ und $r_1 < r_2$ folgt $r_2 - r_1 < b$ und dazu steht E im Widerspruch (wegen TRICH),

d.h. die Annahme ist falsch (analog ergibt sich ein Widerspruch für $r_2 < r_1$),

also gilt $r_1 = r_2$.

Insgesamt gilt damit $r_1 = r_2$ und $q_1 = q_2$ (siehe oben),
d.h. die (formal unterschiedlichen) Darstellungen von a sind identisch, die Division mit Rest damit eindeutig.

t

Bemerkung:
Die Existenz und die Eindeutigkeit der Division mit Rest lassen sich auch über Vollständige Induktion „in einem“ zeigen, also ohne die Existenz und die Eindeutigkeit getrennt zu untersuchen.

LÖSUNG der Arbeitsaufgabe dieses Unterkapitels:

A3 $b = 0$ wurde ausgeschlossen, da $0 \leq r < b$ mit $b = 0$ nicht möglich ist.

6.5 Kongruenzen

6.5.1 Definition und Zusammenhang zur Teilbarkeit

Betrachten wir nun den Begriff der Kongruenz, also den Fall, in dem zwei Zahlen bei Division den gleichen Rest lassen, näher.

Zur Erinnerung:

Definition kongruent

Zwei Zahlen $a,b \in \mathbb{Z}$, die bei Division durch eine Zahl $m \in \mathbb{N}$ den gleichen Rest r lassen, heißen k o n g r u e n t m o d u l o m .

In Zeichen: $a \equiv b\ (m) \Leftrightarrow \exists q_1,q_2 \in \mathbb{Z},\ r \in \mathbb{N}_0 : (a = q_1 \cdot m + r \ \wedge\ b = q_2 \cdot m + r),\ 0 \le r < m$

Kongruenzen lassen sich also über Division mit Rest definieren.

Weniger offensichtlich ist der Zusammenhang zwischen der Kongruenz und der Teilbarkeit. Um diesem auf die Spur zu kommen, wollen wir uns zunächst wieder konkreten Beispielen zuwenden:
Der Leser suche einige Zahlen, die bezüglich eines festen Moduls m (z.B. 12) restgleich sind und untersuche die Differenzen dieser restgleichen Zahlen.

Denkpause

Wie in Unterkapitel 6.2 (Uhrenbeispiel) herausgestellt, gilt:
$9 \equiv 81\ (12)$ und $14 \equiv 50\ (12)$.

Man erhält: $81 - 9 = 72$ und für 72 gilt: $72 = 6 \cdot 12$
$50 - 14 = 36$ und für 36 gilt: $36 = 3 \cdot 12$

Weitere Beispiele legen die Vermutung nahe, daß die Differenz zweier kongruenter Zahlen stets ein Vielfaches des Moduls ist:

Satz 6.8

Seien $a,b \in \mathbb{Z}$, $m \in \mathbb{N}$. $\quad a \equiv b\ (m) \Leftrightarrow m \mid a - b$ [39]

Beweis:

Zuerst einmal ist es wichtig festzuhalten, daß die Aussage eine Äquivalenz ($\Leftrightarrow$) beinhaltet. Wir müssen also beide Richtungen zeigen.

„$\Rightarrow$“: $\quad a \equiv b\ (m)$

$\Rightarrow \exists q_1,q_2 \in \mathbb{Z},\ r \in \mathbb{N}_0 : (a = m \cdot q_1 + r \ \wedge\ b = m \cdot q_2 + r)$ (def.„$\equiv$“)

Da wir ja wissen wollen, was es mit $a - b$ auf sich hat, wird die eine Gleichung von der anderen subtrahiert. Man erhält:

[39] Natürlich gilt auch: $a \equiv b\ (m) \Leftrightarrow m \mid b - a$ (aus $m \mid a - b$ folgt wegen Satz 6.5 (v) $m \mid b - a$).

$\Rightarrow \quad \exists q_1,q_2\in\mathbb{Z},\ r\in\mathbb{N}_0\colon (a-b=(m\cdot q_1+r)-(m\cdot q_2+r))$ (Eigenschaft „=“)

$\Rightarrow \quad \exists q_1,q_2\in\mathbb{Z},\ r\in\mathbb{N}_0\colon (a-b=m\cdot q_1+r-m\cdot q_2-r)$ (DIST)

$\Rightarrow \quad \exists q_1,q_2\in\mathbb{Z}\colon (a-b=m\cdot q_1-m\cdot q_2)$

$\Rightarrow \quad \exists q_1,q_2\in\mathbb{Z}\colon (a-b=m\cdot(q_1-q_2))$ (DIST)

Schon fertig? Nö! Jetzt ist (wie bei den 🕮 Ferienhäusern) zu überlegen, ob die gefundene Zahl (q_1-q_2) auch eine ganze Zahl ist, das heißt ob man tatsächlich ein freies Ferienhaus ausgesucht hat. Das ist in diesem Fall kein Problem, denn die Differenz zweier ganzer Zahlen liegt wiederum selbst in $\mathbb{Z}$.

$\Rightarrow \quad m\,|\,a-b$ (def. „$|$“, $q_1-q_2\in\mathbb{Z}$)

„$\Leftarrow$“: Naheliegend wäre, beim Beweis der Rückrichtung mit der Teilbarkeitsaussage $m\,|\,a-b$ zu starten. Unglücklicherweise führt uns dieser Beweisbeginn nicht zu der Aussage $a \equiv b\ (m)$ (der/die ungläubige Leser(in) versuche sich an diesem Unterfangen). Daher bleibt uns wenig anderes übrig, als auf die Grundlage der beiden hier verwendeten Begriffe Teilbarkeit und Kongruenzen zurückzugreifen: auf die immer gern gesehene Division mit Rest:

$$\dot{\exists}\, q_1,q_2,r_1,r_2\in\mathbb{N}_0\colon (\quad a=m\cdot q_1+r_1 \ \wedge\ 0\le r_1<m$$
$$\text{und}\quad b=m\cdot q_2+r_2 \ \wedge\ 0\le r_2<m\ ) \qquad \text{(Satz 6.10)}$$

Zusätzlich kennen wir auch noch die Voraussetzung. Doch bevor diese zum Einsatz kommt, machen wir uns klar, was wir eigentlich zeigen wollen: a und b sollen kongruent modulo m sein, müssen also gleiche Reste bei Division durch m lassen. Deswegen ist nun zu zeigen, daß $r_1=r_2$ gilt.
Da wir wissen, daß $m\,|\,a-b$ gilt, bilden wir zuerst $a-b$:

$\Rightarrow \quad a-b \;=\; (m\cdot q_1+r_1)-(m\cdot q_2+r_2)$ (Subtr. v. Gleichungen)

$\Rightarrow \quad a-b \;=\; m\cdot q_1+r_1\ -m\cdot q_2-r_2$ (Satz 4.4)

$\Rightarrow \quad a-b \;=\; m\cdot(q_1-q_2)+(r_1-r_2)$ ☺ (KOM, DIST)

Nun kommt die Voraussetzung zum Einsatz:

$m\,|\,a-b$ (Vor.)

$\Rightarrow \quad m\,|\,m\cdot(q_1-q_2)+(r_1-r_2)$ (☺)

Wenn m eine Summe und einen der Summanden $(m\,|\,m\cdot(q_1-q_2))$ teilt, dann muß m auch den zweiten Summanden teilen (vgl. auch Satz 6.3(iv)):

$\Rightarrow \quad m\,|\,r_1-r_2$ (Satz 6.3(iv))

$\Rightarrow \quad m\,|\,|r_1-r_2|$ ❀

Begründung:
Wenn r_1-r_2 eine positive Zahl (oder Null) ist, ist $|r_1-r_2|=r_1-r_2$.
Wenn r_1-r_2 negativ ist, so gilt $|r_1-r_2|=-(r_1-r_2)$ (nach Def. Betrag, Kap.1).
Teilt nun m aber r_1-r_2, so teilt m auch $-(r_1-r_2)=(-1)\cdot(r_1-r_2)$, denn nach Satz 6.5(v) gilt, daß auch das (–1)-fache von m geteilt wird.
In beiden Fällen erhält man also $m\,|\,|r_1-r_2|$.

Betrachten wir nun $|r_1-r_2|$ genauer:

$0\le r_1<m \ \wedge\ 0\le r_2<m$ (Vor.)

$\Rightarrow \quad 0\le |r_1-r_2|<m$ ❁

Schön wäre, es würde gelten: $0=|r_1-r_2|$ (dann folgt direkt die Gleichheit von r_1 und r_2), dazu müßte $0<|r_1-r_2|$ ausgeschlossen werden:

Annahme: $0 < |r_1 - r_2|$

Es gilt : $m \mid |r_1 - r_2|$ (❁)

$\Rightarrow$ $m \le |r_1 - r_2|$ (Satz 6.4(i), Annahme)[40]

Das ist wegen TRICH ein Widerspruch zu ❁! Also gilt: $0 = |r_1 - r_2|$:

$0 = |r_1 - r_2|$

$\Rightarrow$ $0 = r_1 - r_2$ (def. Betrag)

$\Rightarrow$ $r_1 = r_2$

r_1 und r_2 sind die Reste von a und b bei Division durch m. Wenn a und b bei Division durch m denselben Rest lassen, sind sie kongruent modulo m.

$\Rightarrow$ $a \equiv b \ (m)$ (def. „≡“)

t

Dieser Satz kann uns im folgendem viel Arbeit ersparen, denn über die Teilbarkeit sind bereits viele Sätze bekannt. Über die Kongruenzrelation hingegen, wissen wir erst wenig.

6.5.2 Eigenschaften

In vielerlei Beziehung ähnelt die Kongruenzrelation der uns vertrauten Gleichheitsrelation. Eine weitere Eigenschaft, die die Kongruenz mit der Gleichung gemein hat, folgt nun:

Satz 6.9 („≡“ ist eine Äquivalenzrelation)

Seien $a,b,c \in \mathbb{Z}$, $m \in \mathbb{N}$		
(i)	$a \equiv a \ (m)$	(REFL „≡“)
(ii)	$a \equiv b \ (m) \Rightarrow b \equiv a \ (m)$	(SYM „≡“)
(iii)	$a \equiv b \ (m) \ \wedge \ b \equiv c \ (m) \ \Rightarrow \ a \equiv c \ (m)$	(TRANS „≡“)

Beweis:

Wie in Satz 6.8 herausgestellt, kann man Kongruenzen auf Teilbarkeitsaussagen zurückführen. Für die Teilbarkeitsrelation wurden die entsprechenden Aussagen in Satz 6.5 bewiesen. Daher kann man sich dies für den Beweis zunutze machen.

(i) Sei $a \in \mathbb{Z}$ beliebig gewählt:

$a \equiv a \ (m)$ ist äquivalent mit der Aussage $m \mid a - a$ (nach Satz 6.8), das heißt, es ist jetzt $m \mid a - a$ zu zeigen. $a - a$ ist aber gleich 0 und Satz 6.5 besagt, daß jede ganze Zahl 0 teilt, damit ist der Beweis fertig. Also jetzt noch einmal formal:

$m \mid 0$ (Satz 6.5)

$\Rightarrow$ $m \mid a - a$ $(0 = a - a)$

$\Rightarrow$ $a \equiv a \ (m)$ (Satz 6.8)

t

[40] Der Satz läßt sich hier anwenden, da in diesem Fall $|r_1 - r_2| \neq 0$.

(ii) Seien $a,b \in \mathbb{Z}$ beliebig gewählt mit $a \equiv b\ (m)$.
Zu zeigen: $b \equiv a\ (m)$
Beweis:

$a \equiv b\ (m)$
$\Rightarrow$ $m \mid a-b$ (Satz 6.8)
$\Rightarrow$ $m \mid (-1)(a-b)$ (Satz 6.5)
$\Rightarrow$ $m \mid b-a$ (DIST)
$\Rightarrow$ $b \equiv a\ (m)$ (Satz 6.8)

t

(iii) Seien $a,b,c \in \mathbb{Z}$ beliebig gewählt mit $a \equiv b\ (m) \wedge b \equiv c\ (m)$.
Zu zeigen: $a \equiv c\ (m)$

Beweis:

$a \equiv b\ (m) \wedge b \equiv c\ (m)$

Zuerst wird wieder die Umformung in eine Teilbarkeitsaussage vorgenommen.

$\Rightarrow$ $m \mid a-b \wedge m \mid b-c$ (Satz 6.8)

Da a und c in einem Term erscheinen sollen ($a \equiv c\ (m) \Leftrightarrow m \mid a-c$)[41], nehmen wir Satz 6.5 zur Hilfe und addieren die Terme $(a-b)$ und $(b-c)$.

$\Rightarrow$ $m \mid (a-b)+(b-c)$ (Satz 6.5)
$\Rightarrow$ $m \mid (a-c)+(b-b)$
$\Rightarrow$ $m \mid a-c$
$\Rightarrow$ $a \equiv c\ (m)$ (Satz 6.8)

t

6.5.3 Rechnen mit Kongruenzen

Nun können wir mit Hilfe von Satz 6.8 all die hübschen Teilbarkeitsaussagen auf die Kongruenzen loslassen:

Satz 6.10 (Rechenregeln für Kongruenzen)

Kongruenzen (mit gleichem Modul) können (wie Gleichungen) addiert, subtrahiert, multipliziert, potenziert und (mit Einschränkung) dividiert werden:

Seien $a,b,c,d \in \mathbb{Z}$, $k,m,n \in \mathbb{N}$ und gelte: $a \equiv b\ (m) \wedge c \equiv d\ (m)$

(i) $a+c \equiv b+d\ (m)$

(ii) $a-c \equiv b-d\ (m)$

(iii) $a \cdot c \equiv b \cdot d\ (m)$

(iv) $a \equiv b\ (m) \Rightarrow a^n \equiv b^n\ (m)$

(v) $ak \equiv bk\ (m) \Rightarrow a \equiv b\ \left(\frac{m}{ggT(k,m)}\right)$

[41] Hier läßt sich schön erkennen, daß es sich bei vielen Beweisen anbietet, „rückwärts“ vorzugehen (🕮 Insel) bzw. zumindest das Beweisziel gedanklich so umzuformen, daß man sieht, wie die Voraussetzungen umgeformt werden müssen, damit das Beweisziel erreicht wird.

Dividieren ist bei Kongruenzen ist also nicht ohne weiteres möglich (vgl. auch die nach dem Beweis erfolgenden Erläuterungen). Hier müssen - im Gegensatz zu Gleichungen - Einschränkungen gemacht werden. Nur wenn der Modul und die Zahl, durch die dividiert wird, teilerfremd sind (ggT(k,m) = 1), ist das Dividieren problemlos möglich. Ist dies nicht der Fall, ändert sich der Modul wie in (v) ausgeführt.

Wurzelziehen macht gar keinen Sinn.

Beweis:

(i) $a \equiv b\ (m) \ \wedge\ c \equiv d\ (m)$

Da wir für Teilbarkeiten schon einige Aussagen zur Verfügung haben (Unterkapitel 6.3), formen wir die Kongruenzaussage aus Satz 6.10 mit Hilfe von Satz 6.8 in eine Teilbarkeitsaussage um.

$\Rightarrow$ $m \mid a-b \ \wedge\ m \mid c-d$ (Satz 6.8)

Da es in (i) um Summen geht, werden nun die Terme (b – a) und (c – d) addiert.
Dabei ist Satz 6.5 hilfreich.

$\Rightarrow$ $m \mid (a-b) + (c-d)$ (Satz 6.5)
$\Rightarrow$ $m \mid (a+c) - (b+d)$ (ASS, KOM)

Jetzt ist zu sehen, daß m eine Differenz teilt und es läßt sich wunderbar die Rückrichtung von Satz 6.8 anwenden.

$\Rightarrow$ $a+c \ \equiv\ b+d\ (m)$ (Satz 6.8)

t

(ii) Der Leser überlege sich, warum aus (i) mit wenig Aufwand (ii) folgt. (**A4**)

(iii) $a \equiv b\ (m) \ \wedge\ c \equiv d\ (m)$
$\Rightarrow$ $m \mid a-b \ \wedge\ m \mid c-d$ (Satz 6.8)

Wieder wird sich des Satzes 6.8 bedient. Demnach ist das Beweisziel $ac \equiv bc$ äquivalent zu $m \mid (a \cdot c) - (b \cdot d)$.
Es ist jetzt also irgendwie $a \cdot c$ und $b \cdot d$ zu erzeugen. Hilfreich ist hier der Teil (vi) von Satz 6.5:

$\Rightarrow$ $m \mid (a-b) \cdot d \ \wedge\ m \mid (c-d) \cdot a$ (Satz 6.5 (vi))
$\Rightarrow$ $m \mid a \cdot d - b \cdot d \ \wedge\ m \mid c \cdot a - d \cdot a$ (DIST)
$\Rightarrow$ $m \mid (a \cdot d - b \cdot d) + (c \cdot a - d \cdot a)$ (Satz 6.5 (v))
$\Rightarrow$ $m \mid (a \cdot d - d \cdot a) + (c \cdot a - b \cdot d)$ (ASS, KOM)
$\Rightarrow$ $m \mid (c \cdot a - b \cdot d)$ (KOM „$\cdot$“)
$\Rightarrow$ $c \cdot a \equiv b \cdot d\ (m)$ (Satz 6.8)

t

(iv) ist eine Übungsaufgabe, die im Übungsteil den Leser erwartet.

(v) wird nicht bewiesen (für den Beweis benötigen wir Teilbarkeitssätze, die uns hier nicht zur Verfügung stehen)

Dies sind die wichtigsten Rechenregeln für Kongruenzen. Als Merkregel lassen sich diese Gesetze am einfachsten mit den Rechenregeln für Gleichungen (Kap. 1.4) vergleichen. Abgesehen von den Einschränkungen beim Dividieren kann man mit Kongruenzen so rechnen, als ob sie Gleichungen wären.

Zum Dividieren bei Kongruenzen:

Die Divisionsregel für Kongruenzen ist eigentlich eine Kürzungsregel, denn es kann jeweils nur durch diejenige Zahl dividiert werden, die auf beiden Seiten der Kongruenz als Faktor enthalten ist:
Aus der Kongruenz $24x \equiv 12\ (7)$ kann beispielsweise der Faktor 12 (oder 2, 3, 4 oder 6) gekürzt werden. Aus der Kongruenz $5x \equiv 12\ (7)$ kann man aber nicht den Faktor 5 kürzen - so gerne man es auch möchte.[42]

Wenn Wegkürzen nicht möglich ist, muß man einen Umweg gehen:

Um in der Kongruenz $5x \equiv 9\ (7)$ den Faktor 5 zu beseitigen, sucht man ein Vielfaches von 5, das bei Division durch 7 den Rest 1 läßt:

Das 3-fache von 5 ist geeignet, da $15 \equiv 1\ (7)$. Jetzt multiplizieren wir unsere Ausgangskongruenz mit $3 \equiv 3\ (7)$ und erhalten:

	$5x \equiv 9\ (7)$	
$\Rightarrow$	$5x \equiv 2\ (7)$	($9 \equiv 2\ (7)$, TRANS „$\equiv$“)
$\Rightarrow$	$15x \equiv 6\ (7)$	(Mult. v. Kongr., $3 \equiv 3\ (7)$)
$\Rightarrow$	$x \equiv 6\ (7)$	($15 \equiv 1\ (7) \Rightarrow 15x \equiv x\ (7)$, Mult. v. Kongr., TRANS „$\equiv$“)
$\Rightarrow$	$x \equiv -1\ (7)$	($6 \equiv -1\ (7)$, TRANS „$\equiv$“)

Alternativ kann man auch ein Vielfaches von 5 suchen, das bei Division durch 7 den Rest –1 läßt. Geeignet ist in diesem Beispiel das 4-fache von 5:

	$5x \equiv 9\ (7)$	
$\Rightarrow$	$5x \equiv 2\ (7)$	($9 \equiv 2\ (7)$, TRANS „$\equiv$“)
$\Rightarrow$	$20x \equiv 8\ (7)$	(Mult.v.Kongr., $4 \equiv 4\ (7)$)
$\Rightarrow$	$-x \equiv 8\ (7)$	($20 \equiv -1\ (7) \Rightarrow 20x \equiv -x\ (7)$, Mult. v. Kongr., TRANS „$\equiv$“)
$\Rightarrow$	$-x \equiv 1\ (7)$	($8 \equiv 1\ (7)$, TRANS „$\equiv$“)
$\Rightarrow$	$x \equiv -1\ (7)$	(Mult.v.Kongr., $-1 \equiv -1\ (7)$)

Allgemein:
Möchte man bei einer Kongruenz der Form $a \cdot x \equiv b\ (m)$ den Faktor a beseitigen, um die möglichen Lösungen für x zu ermitteln und ein Kürzen nicht möglich ist, da a kein Teiler von b ist, sucht man ein Vielfaches von a, das kongruent 1 oder –1 ist. Dazu geht man ihre Vielfachen der Reihe nach durch.
Hat man das passende Vielfache (n-fache) gefunden, so multipliziert man die Kongruenz mit der Kongruenz $n \equiv n\ (m)$, die ja wegen REFL „$\equiv$“ immer gilt.

Man erhält:	$n \cdot a \cdot x \equiv n \cdot b\ (m)$	
$\Rightarrow$	$x \equiv n \cdot b\ (m)$	($n \cdot a \equiv 1\ (m) \Rightarrow n \cdot a \cdot x \equiv x\ (m)$, TRANS „$\equiv$“)

oder:	$n \cdot a \cdot x \equiv n \cdot b\ (m)$	
$\Rightarrow$	$-x \equiv n \cdot b\ (m)$	($n \cdot a \equiv -1\ (m) \Rightarrow n \cdot a \cdot x \equiv -x\ (m)$, TRANS „$\equiv$“)
$\Rightarrow$	$x \equiv -n \cdot b\ (m)$	($-1 \equiv -1\ (m)$, Mult.v.Kongr.)

So sind wir das a also losgeworden, ohne zu dividieren. Man kommt demnach auch ohne einen Divisionssatz aus.

[42] Als weiterer Nachteil erweist sich die weiter oben angeführte Einschränkung, daß Kürzen nur bei teilerfremden Zahlen problemlos möglich ist, da sich sonst der Modul ändert. Häufig möchte man aber gerade vermeiden, daß der Modul verändert wird (da man als Lösung eine Kongruenz mit einem bestimmten Modul benötigt) und kann somit nicht auf die Divisionsregel zurückgreifen.

Das Beseitigen eines Faktors innerhalb einer Kongruenz ist also ziemlich anstrengend. Zum Glück bieten Kongruenzen dafür im Vergleich zu Gleichungen einen entscheidenden Vorteil:
Große Zahlen lassen sich stets durch restgleiche kleinere ersetzen. Betrachtet man Kongruenzen modulo 5, braucht man somit nur mit Zahlen von 0 bis 4 umzugehen.
Beispiel:
$74x \equiv 323\ (5)$ läßt sich umformen zu $4x \equiv 3\ (5)$

Nun folgt ein Satz, welcher die Zusammenhänge zwischen der Kongruenz, der Teilbarkeitsrelation und der Division mit Rest herausstellt. Wie der Aufbau des Kapitels zeigt, lassen sich mit Hilfe der Division mit Rest die Teilbarkeitsaussage und die Kongruenz einführen.
Wichtig ist nun, daß man sich bei zahlentheoretischen Problemstellungen immer bewußt ist, daß sich jede Division mit Rest in eine Teilbarkeitsaussage oder wahlweise in eine Kongruenz umformulieren läßt, weiterhin kann man jede Kongruenz als Teilbarkeitsaussage oder als Division mit Rest deuten usw.
Der Leser sollte daher in der Lage sein, die folgenden vier Äquivalenzen ((iv) erlaubt die Umformung in eine Gleichung) flexibel zu benutzen, um so verschiedene Herangehensweisen an Probleme zu besitzen.

Satz 6.11

Es gilt	$a \equiv b\ (m)$	(i)
$\Leftrightarrow$	$m \mid a - b$	(ii)
$\Leftrightarrow$	$\exists q_1, q_2 \in \mathbb{Z}:\ (a = q_1 \cdot m + r\ \wedge\ b = q_2 \cdot m + r)$ mit $0 \le r < m$	(iii)
$\Leftrightarrow$	$\exists x \in \mathbb{Z}:\ (a = x \cdot m + b)$	(iv)

Die Aussage des Satzes läßt sich wie folgt verbalisieren:

Eine Zahl a ist genau dann kongruent zu einer anderen Zahl b modulo m,

- wenn die Differenz der beiden Zahlen (a – b oder b – a) durch den Modul teilbar ist
- wenn a und b bei Division durch den Modul denselben Rest lassen
- wenn sich die eine der beiden Zahlen (a) aus der anderen (b) ergibt, indem man zu der anderen ein ganzzahliges Vielfaches des Moduls addiert.

Bemerkung: Die einzelnen Äquivalenzen ergeben sich wie folgt:

(i) $\Leftrightarrow$ (ii): Das ist die Aussage von Satz 6.8 .

(i) $\Leftrightarrow$ (iii): Das folgt aus der Definition der Kongruenz.

(ii) $\Leftrightarrow$ (iv): Das folgt aus der Definition Teilbarkeit.

Aus diesen drei Äquivalenzen lassen sich alle möglichen Äquivalenzen herleiten.

LÖSUNG der Arbeitsaufgabe dieses Unterkapitels:

A4 $\quad n \equiv k\ (m)\ \wedge\ -a \equiv -b\ (m)\ \Rightarrow\ n - a \equiv k - b\ (m)$

6.6 Euklidischer Algorithmus

Über die Bestimmung der Menge der gemeinsamen Teiler den ggT von Zahlen wie 320 und 240 zu berechnen (vgl. 6.3.3), ist verhältnismäßig einfach. Was aber, wenn der ggT größerer Zahlen bestimmt werden soll, z.B. von 18438 und 7350 ?

Euklid (griech. Mathematiker, lehrte um 300 v. Chr. in Alexandria) hatte auch dafür eine Lösung:
den sogenannten E u k l i d i s c h e n A l g o r i t h m u s [43]:

Gegeben seien $a,b \in \mathbb{N}$ mit $b < a$.[44] Ausgehend von diesen beiden Zahlen führt man nun eine fortgesetzte Division mit Rest durch. Nach Satz über Division mit Rest existieren jeweils eindeutige $q_i, r_i \in \mathbb{N}_0$:

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

Im nächsten Schritt nimmt man nun b und r_1 und führt wieder eine Division mit Rest durch.

$b = q_2 \cdot r_1 + r_2$ mit $0 \le r_2 < r_1$

Jetzt macht man weiter, indem man statt b und r_1 nun r_1 und r_2 nimmt.

$r_1 = q_2 \cdot r_2 + r_3$ mit $0 \le r_3 < r_2$

$r_2 = q_2 \cdot r_3 + r_4$ mit $0 \le r_4 < r_3$

$\vdots$

Das Verfahren wird solange fortgeführt, bis irgendwann der Rest 0 bleibt.

$r_{n-1} = q_{n+1} \cdot r_n + \underline{r_{n+1}}$ mit $0 \le r_{n+1} < r_n$

$r_n = q_{n+2} \cdot r_{n+1} + \mathbf{0}$

Der in der zweitletzten Zeile auftretende Rest (r_{n+1}), also <u>der letzte von 0 verschiedene Rest</u>, ist der ggT der Ausgangszahlen a und b (dies wird im nachfolgenden Satz festgehalten - und anschließend bewiesen).

Fraglich ist, ob auch immer der Rest 0 erscheint. Dies muß aber so sein, da die Reste von Schritt zu Schritt immer kleiner werden. Betrachtet man nämlich die Ungleichungen, die sich laut Division mit Rest ergeben, so hat man:

$b > r_1 > r_2 > r_3 > \ldots > r_n > r_{n+1} \ge 0$

Schlimmstenfalls wird der Rest vom vorhergehenden zum nächsten Schritt nur um 1 kleiner. Da aber b eine feste natürliche Zahl ist, ist irgendwann Schluß (vgl. 🕮 Wohlordnungsprinzip).

Nach endlich vielen Schritten ist dann tatsächlich der Rest 0 erreicht, dies passiert in der Zeile: $r_n = q_{n+2} \cdot r_{n+1} + \mathbf{0}$

---

[43] Algorithmus: standardisiertes, nach festen Regeln ablaufendes Rechenverfahren.

[44] $b<a$ stellt keine Einschränkung der Anwendbarkeit des Verfahrens dar, denn falls $a=b$, gilt $ggT(a,b) = a$ (bzw. b), falls $a<b$, vertauscht man a und b, d.h. man nimmt für a die größere Zahl.

Führen wir den Euklidischen Algorithmus einmal an obigem Beispiel durch:

$$
\begin{aligned}
18438 &= 2 \cdot 7350 + 3738 \\
7350 &= 1 \cdot 3738 + 3612 \\
3738 &= 1 \cdot 3612 + 126 \\
3612 &= 28 \cdot 126 + 84 \\
126 &= 1 \cdot 84 + \underline{42} \\
84 &= 2 \cdot 42 + \mathbf{0}
\end{aligned}
$$

Man erhält somit: ggT(18438,7350) = 42 .

Der/die Leser(in) trainiere die Anwendung dieses Verfahrens an Ü10 a).

Warum in aller Welt soll nun genau 42 der ggT von 18438 und 7350 sein?

Versuchen wir zunächst zu zeigen, daß 42 zumindest ein gemeinsamer Teiler von 18438 und 7350 ist:

Aus der letzten Zeile des Euklidischen Algorithmus (E.A.) ergibt sich $42 \mid 84$., es gilt auch $42 \mid 42$. Betrachten wir nun die vorletzte Zeile des E.A., dann läßt sich erkennen, daß beide Summanden von 42 geteilt werden und somit wird auch ihre Summe von 42 geteilt, also: $42 \mid 126$.

Da folglich 42 ein Teiler von 126 ist, teilt 42 auch jedes Vielfache von 126, also auch $28 \cdot 126$. Da 42 somit $28 \cdot 126$ und 84 teilt, wird auch deren Summe 3612 von 42 geteilt.

Analog kann man nun schrittweise folgern, daß auch 3738 (dritte Zeile des E.A.), 7350 (zweite Zeile) und schließlich auch 18438 (erste Zeile) von 42 geteilt werden.

Damit erhält man also: $42 \mid 7350$ und $42 \mid 18438$, d.h. 42 ist ein gemeinsamer Teiler von 7350 und 18438.

Nun ist noch zu zeigen, daß 42 der größte gemeinsame Teiler dieser beiden Zahlen ist, daß also jeder gemeinsamer Teiler von 7350 und 18438 teilt kleiner oder gleich 42 ist:

Sei t ein beliebiger gemeinsamer Teiler der beiden Zahlen, dann teilt t sowohl 7350 als auch 18438. Da t also 7350 teilt, teilt es auch $2 \cdot 7350$.
Betrachtet man nun zuerst die erste Zeile des E.A., ist ersichtlich, daß damit die Summe und der erste Summand von m geteilt werden. Dann (vgl. Satz 6.3 (iv)) wird auch der zweite Summand (hier: 3738) von t geteilt. Wird 7350 und $1 \cdot 3738$ von t geteilt, dann auch 3612 usw.

Man erhält schließlich, daß $t \mid 42$ gilt. Daraus folgt nach Satz 6.4: $t \leq 42$,
d.h. jeder gemeinsame Teiler von 18438 und 7350 (t beliebig!) ist kleiner oder gleich 42, d.h. 42 ist der größte gemeinsame Teiler.

Die Allgemeingültigkeit dieses Verfahrens soll nun bewiesen werden:

Satz 6.12

Seien $a,b \in \mathbb{N}$ und sei r_{n+1} der letzte von 0 verschiedene Rest beim Euklidischen Algorithmus. Dann gilt: $ggT(a,b) = r_{n+1}$.

Beweis:

Im Beweis können die in obigem Beispiel durchgeführten Überlegungen verwendet werden, der formale Beweis verläuft prinzipiell analog.

Der Beweis orientiert sich (wie die Überlegungen am Beispiel) an den einzelnen Zeilen des Euklidischen Algorithmus, so daß die für den Beweis relevanten Zeilen des Algorithmus hier noch einmal angeführt seien:

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

$b = q_2 \cdot r_1 + r_2$ mit $0 \le r_2 < r_1$

$\vdots$

$r_{n-2} = q_n \cdot r_{n-1} + r_n$ mit $0 \le r_n < r_{n-1}$

$r_{n-1} = q_{n+1} \cdot r_n + r_{n+1}$ mit $0 \le r_{n+1} < r_n$

$r_n = q_{n+2} \cdot r_{n+1} + \mathbf{0}$

Zuerst soll gezeigt werden, daß r_{n+1} ein gemeinsamer Teiler von a und b ist:

Aus der letzten Zeile des E.A. folgt mit Def. „|“: $r_{n+1} | r_n$.
Wegen REFL „|“ gilt außerdem: $r_{n+1} | r_{n+1}$.
Nach Satz 6.3 (iii) gilt dann auch: $r_{n+1} | q_{n+1} \cdot r_n + r_{n+1}$,
aus der vorletzten Zeile des E.A. ergibt sich damit: $r_{n+1} | r_{n-1}$.
Analog läßt sich zeigen, daß $r_{n+1} | r_{n-2}$ gilt und daß r_{n+1} mit entsprechender Argumentation jeden Rest, der in den darüberstehenden Zeilen auftaucht, teilt.
Schließlich ergibt sich: $r_{n+1} | r_2$ und $r_{n+1} | r_1$, daraus folgt: $r_{n+1} | b$ (zweite Zeile des E.A.) und damit erhält man: $r_{n+1} | a$ (erste Zeile des E.A.).

Folglich ist r_{n+1} ein gemeinsamer Teiler von a und b.

Ist r_{n+1} auch der größte gemeinsame Teiler?

Sei $k \in T(a) \cap T(b)$ beliebig $\Rightarrow$ $k|a \wedge k|b$

$k\|b \Rightarrow k\|q_1 \cdot b$			(Satz 6.3 (ii))
$k\|a \wedge k\| q_1 \cdot b$	$\Rightarrow$	$k\|r_1$	(6.3 (iv), erste Zeile des E.A.)
$k\|r_1 \Rightarrow k\| q_2 \cdot r_1$			(Satz 6.3 (ii))
$k\|b \wedge k\| q_2 \cdot r_1$	$\Rightarrow$	$k\|r_2$	(6.3 (iv), zweite Zeile des E.A.)
$\vdots$			
$k\|r_n \Rightarrow k\|q_{n+1} \cdot r_n$			(Satz 6.3 (ii))
$k\|r_{n-1} \wedge k\|q_{n+1} \cdot r_n$	$\Rightarrow$	$k\|r_{n+1}$	(6.3 (iv), vorletzte Zeile des E.A.)
	$\Rightarrow$	$k \le r_{n+1}$	(Satz 6.4 (i), $r_{n+1} \neq 0$ nach Vor.)
	$\Rightarrow$	$k \le ggT(a,b)$	(def. „ggT“)

Alle gemeinsamen Teiler von a und b sind somit kleiner als r_{n+1} , also ist r_{n+1} der **g**gT(a,b).
Der letzte Beweisteil führt uns netterweise auf eine wesentliche Eigenschaft des ggT: Jeder gemeinsame Teiler zweier Zahlen teilt den ggT dieser Zahlen:

Satz 6.13

Seien $a,b \in \mathbb{N}$, dann sind alle gemeinsamen Teiler von a und b auch Teiler des ggT(a,b).

In Zeichen: $\forall t \in \mathbb{N}: (t \mid a \wedge t \mid b \Rightarrow t \mid ggT(a,b))$

Beweis:

Sei $t \in \mathbb{N}$ beliebig mit $t \mid a \wedge t \mid b$

$t \mid b \Rightarrow t \mid q_1 \cdot b$		(Satz 6.3 (ii))
$t \mid a \wedge t \mid q_1 \cdot b \Rightarrow t \mid r_1$		(6.3 (iv), erste Zeile des E.A.)
$t \mid r_1 \Rightarrow t \mid q_2 \cdot r_1$		(Satz 6.3 (ii))
$t \mid b \wedge t \mid q_2 \cdot r_1 \Rightarrow t \mid r_2$		(6.3 (iv), zweite Zeile des E.A.)
$\vdots$		
$t \mid r_n \Rightarrow t \mid q_{n+1} \cdot r_n$		(Satz 6.3 (ii))
$t \mid r_{n-1} \wedge t \mid q_{n+1} \cdot r_n \Rightarrow t \mid r_{n+1}$		(6.3 (iv), vorletzte Zeile des E.A.)
	$\Rightarrow t \mid ggT(a,b)$	(Satz 6.12)

t

Der Euklidische Algorithmus (genauer gesagt sein Beweis) hat uns also sozusagen als Bonus die Aussage aus Satz 6.13 (und ihren Beweis) geliefert. Außerdem haben wir nun neben der Bestimmung des ggT über die Menge der gemeinsamen Teiler ein weiteres Verfahren zur Verfügung, das besonders für die Bestimmung des ggT größerer Zahlen geeignet ist.

Aber der E.A. liefert noch mehr:

Aus diesem Algorithmus läßt sich eine weitere Charakterisierung des ggT ableiten.

Bisher haben wir folgende Charakterisierungen kennengelernt:

- der ggT als Maximum der Menge der gemeinsamen Teiler
- der ggT als der gemeinsame Teiler der größer ist als alle anderen gemeinsamen Teiler

Nachfolgend werden wir anhand des E.A. zeigen, daß sich der ggT zweier Zahlen als Vielfachsumme dieser Zahlen darstellen läßt. Anschließend werden wir die dritte Charakterisierung des ggT beweisen, nämlich daß der ggT zweier Zahlen die kleinste Zahl ist, die sich als Vielfachsumme dieser Zahlen darstellen läßt.

Hierfür betrachten wir die Zahlen 87 und 36:

$87 = 2 \cdot 36 + 15$
$36 = 2 \cdot 15 + 6$
$15 = 2 \cdot 6 + \underline{3}$
$6 = 2 \cdot 3 + 0$

Nach Satz 6.12 gilt: ggT(87,36) = 3 .

Geht man jetzt von der vorletzten Zeile aus, so läßt sich der ggT(87,36) = 3 folgendermaßen schreiben:

$$3 = 15 - 2 \cdot 6 \qquad ❶$$

Wird nun die vor-vorletzte Zeile umgeformt, so erhält man folgenden Term für 6:

$$6 = 36 - 2 \cdot 15 \qquad ❷$$

❷ in ❶ eingesetzt ergibt:

$$\begin{aligned} 3 &= 15 - 2 \cdot (36 - 2 \cdot 15) \\ &= 15 - 2 \cdot 36 + 4 \cdot 15 \\ &= 5 \cdot 15 - 2 \cdot 36 \qquad ❸ \end{aligned}$$

Nun haben wir uns zur vor-vor-vorletzten Zeile (1. Zeile) vorgearbeitet.
Wird diese umgeformt, erhält man für 15:

$$15 = 87 - 2 \cdot 36 \qquad ❹$$

❹ in ❸ eingesetzt ergibt:

$$\begin{aligned} 3 &= 5 \cdot (87 - 2 \cdot 36) - 2 \cdot 36 \\ &= 5 \cdot 87 - 10 \cdot 36 - 2 \cdot 36 \\ &= 5 \cdot 87 - 12 \cdot 36 \qquad ❺ \end{aligned}$$

3 - der ggT(87,36) - wird hier geschrieben als eine Summe von ganzzahligen Vielfachen der Zahlen 87 und 36:

ggT(87,36) $= 5 \cdot \mathbf{87} + (-12) \cdot \mathbf{36}$

Man sagt dazu auch Vielfachsumme oder L i n e a r k o m b i n a t i o n .

Obiges Verfahren, mit dem man für beliebige Paare natürlicher Zahlen eine Darstellung des ggT als Linearkombination erhält, läßt sich natürlich auch <u>schneller und übersichtlicher</u> durchführen. Wir schlagen dafür folgende Notation vor, die wir an Hand des obigen Beispiels für den E.A. vorstellen möchten:

$18438 = 2 \cdot 7350 + 3738 \quad (\Leftrightarrow \quad 3738 = 18438 - 2 \bullet 7350)$
$7350 = 1 \cdot 3738 + 3612 \quad (\Leftrightarrow \quad 3612 = 7350 - 1 \cdot 3738)$
$3738 = 1 \cdot 3612 + 126 \quad (\Leftrightarrow \quad 126 = 3738 - 1 \cdot 3612)$
$3612 = 28 \cdot 126 + 84 \quad (\Leftrightarrow \quad 84 = 3612 - 28 \cdot 126)$
$126 = 1 \cdot 84 + \underline{42} \quad (\Leftrightarrow \quad 42 = 126 - 1 \cdot 84)$
$84 = 2 \cdot 42 + \mathbf{0}$

Nach Satz 6.12 gilt: ggT(18438,7350) = 42 .

Nun läßt sich 42 als Linearkombination von 18438 und 7350 darstellen, indem man jede Zeile des Algorithmus (bis auf die letzte) nach dem jeweiligen Rest umformt und von unten nach oben die Reste schrittweise durch die entsprechenden Terme ersetzt.

Wichtig ist dabei nach dem Ersetzen das Auflösen der Klammern mittels DIST. Man darf allerdings die erhaltenen Terme nicht vollständig ausmultiplizieren, da die jeweiligen Reste für die weiteren Ersetzungen erhalten bleiben müssen. Bevor man dann die nächste Ersetzung vornimmt, sollte man die vervielfachten Reste immer geeignet zusammenfassen, z.B. $1 \cdot 15$ und $4 \cdot 15$ zu $5 \cdot 15$ (vgl. ❸).

Auch wenn der/die Leser(in) dieses kleinschrittige Vorgehen vielleicht für übertrieben hält, so vermeidet man jedoch so die meisten lästigen Rechenfehler, die sich sehr häufig bei einer schnelleren Vorgehensweise einschleichen. Aus diesem Grunde ist es sinnvoll, sich an folgender **E A Z - R e g e l** (**E**uklidischer **A**lgorithmus **z**urück) zu orientieren:

1. **E**rsetzen der Reste durch die aus dem E.A. erhaltenen Terme
2. teilweises **A**usmultiplizieren
3. **Z**usammenfassen der vervielfachten Reste

$$42 = 126 - 1 \cdot 84$$

$$\overset{E}{=} 126 - 1 \cdot \underline{(3612 - 28 \cdot 126)} \overset{A}{=} 126 - 1 \cdot 3612 + 28 \cdot 126 \overset{Z}{=} 29 \cdot 126 - 1 \cdot 3612$$

$$\overset{E}{=} 29 \cdot \underline{(3738 - 1 \cdot 3612)} - 1 \cdot 3612 \overset{A}{=} 29 \cdot 3738 - 29 \cdot 3612 - 1 \cdot 3612 \overset{Z}{=}$$

$$29 \cdot 3738 - 30 \cdot 3612$$

$$\overset{E}{=} 29 \cdot 3738 - 30 \cdot \underline{(7350 - 1 \cdot 3738)} \overset{A}{=} 29 \cdot 3738 - 30 \cdot 7350 + 30 \cdot 3738 \overset{Z}{=}$$

$$59 \cdot 3738 - 30 \cdot 7350$$

$$\overset{E}{=} 59 \cdot \underline{(18438 - 2 \cdot 7350)} - 30 \cdot 7350 \overset{A}{=} 59 \cdot 18438 - 118 \cdot 7350 - 30 \cdot 3750 \overset{Z}{=}$$

$$59 \cdot 18438 - 148 \cdot 7350$$

$$= 59 \cdot \mathbf{18438} + (-148) \cdot \mathbf{7350}$$

Also: $ggT(18438,7350) = 59 \cdot 18438 + (-148) \cdot 7350$

Man könnte jetzt vermuten, daß sich der ggT zweier natürlicher Zahlen a und b <u>stets</u> derart schreiben läßt, nämlich:

$ggT(a,b) = x \cdot a + y \cdot b$ mit geeigneten $x,y \in \mathbb{Z}$.

Im ersten Beispiel war 5 eine Lösung für x und -12 eine für y;
im zweiten Beispiel war 59 eine Lösung für x und -148 eine für y.

Tatsächlich ist das auch so:

Satz 6.14

Für alle $a,b \in \mathbb{N}$ existieren $x,y \in \mathbb{Z}$, so daß sich der ggT von a und b als Linearkombination von a und b darstellen läßt.

In Zeichen: $\forall a,b \in \mathbb{N}\ \exists x,y \in \mathbb{Z}: (ggT(a,b) = x \cdot a + y \cdot b)$

Beweis:

Ein Rückblick auf den Euklidischen Algorithmus liefert eine Beweisidee. Im Gegensatz zu den Beispielen auf den letzten Seiten sollte man hier bei dem Beweis in der ersten Zeile des E.A. beginnen. Das liegt daran, daß man im allgemeinen Fall nicht weiß, aus wie vielen Schritte der E.A. besteht, und man somit nicht bis zu der Darstellung des Restes durch a und b vordringen kann, wenn man wie bei konkreten Zahlen in der vorletzten Zeile des E.A. beginnt.
Beginnt man aber in der ersten Zeile, so kann man die Zeilen des E.A. sukzessiv nach den Resten auflösen und in die nächste Zeile einsetzen. Da in der ersten Zeile a und b vorkommen, sind sie in den nachfolgenden Einsetzungen immer mit dabei, so daß man den jeweiligen Rest als Linearkombination der beiden ausdrücken kann.

Man löst die 1. Gleichung des E.A. nach r_1 auf:

$a = q_1 \cdot b + r_1$ (1. Zeile des E.A.)

$\Leftrightarrow\ r_1 = a - q_1 \cdot b$

$\Leftrightarrow\ r_1 = 1 \cdot a + (-q_1) \cdot b$

Man erhält für r_1 eine Linearkombination von a und b mit $r_1 = 1 \cdot a + (-q_1) \cdot b$.

Dann wird entsprechend die zweite Gleichung nach r_2 aufgelöst:

$b = q_2 \cdot r_1 + r_2$ (2. Zeile des E.A.)

$\Leftrightarrow\ r_2 = b - q_2 \cdot r_1$

Nun orientiert man sich an der 🕮 EAZ-Regel.
Setzt man hier für r_1 die oben gewonnene Darstellung ein, so ergibt sich:

$\Leftrightarrow\ r_2 = b - q_2 \cdot (1 \cdot a + (-q_1) \cdot b)$ (**E**)

$\Leftrightarrow\ r_2 = b - q_2 \cdot a + q_2 \cdot q_1 \cdot b$ (**A**)

$\Leftrightarrow\ r_2 = (-q_2) \cdot a + (1 + q_2 \cdot q_1) \cdot b$ (**Z**)

Man erhält für r_2 somit auch eine Linearkombination von a und b mit:
$r_2 = (-q_2) \cdot a + (1 + q_2 \cdot q_1) \cdot b$

Dieses Verfahren zieht man bis zur letzten Zeile durch und erhält so eine Darstellung von r_{n+1} , die nur von a und b abhängig ist:

$ggT(a,b) = r_{n+1} = xa + yb$

Entscheidend für diesen Beweis ist, daß laut Satz über Division mit Rest alle Gleichungen existieren und eindeutig sind.

t

Wir wissen nun, daß sich der ggT(a,b) als Linearkombination von a und b darstellen läßt. Man kann diesen Satz jedoch noch weiter verschärfen:

Satz 6.15

Seien $a,b \in \mathbb{N}$, dann ist der ggT von a und b die kleinste natürliche Zahl, die sich als Linearkombination von a und b darstellen läßt.

In Zeichen: $\forall a,b \in \mathbb{N}: (ggT(a,b) = \min(\{c \in \mathbb{N} \mid c = x \cdot a + y \cdot b \text{ mit } x,y \in \mathbb{Z}\}))$

Beweis:
Die Idee des Beweises beruht auf der Identitivität von „≤“, die man häufig zum Beweis von Gleichheitsaussagen benutzt:
$\forall a,b\in\mathbb{N}: (a\le b \wedge b\le a \Rightarrow a=b)$

Zu zeigen: (i) $ggT(a,b) \le \min(\{c\in\mathbb{N} \mid c = x\cdot a + y\cdot b \text{ mit } x,y\in\mathbb{Z}\})$
(ii) $\min(\{c\in\mathbb{N} \mid c = x\cdot a + y\cdot b \text{ mit } x,y\in\mathbb{Z}\}) \le ggT(a,b)$

Seien $a,b\in\mathbb{N}$ beliebig gewählt.

(i) Hilfreich ist hier der Satz 6.4 (i). Wenn man zeigen kann, daß die Teilbarkeitsbeziehung gilt, so kann man auf die ≤-Beziehung schließen.
Klar ist, daß der ggT(a,b) sowohl a als auch b teilt:

$ggT(a,b) \mid a \wedge ggT(a,b) \mid b$ (Satz 6.6 (ii))

Damit teilt der ggT aber auch alle Vielfachen von a und b sowie deren Summen, also alle Linearkombinationen von a und b:

$\Rightarrow \forall x,y\in\mathbb{Z}: (ggT(a,b) \mid x\cdot a + y\cdot b\})$ (Satz 6.3 (iii))

Der ggT(a,b) teilt also jede beliebige Linearkombination („$\forall x,y\in\mathbb{Z}$“) und damit insbesondere auch die kleinstmögliche.

$\Rightarrow ggT(a,b) \mid \min(\{c\in\mathbb{N} \mid c = x\cdot a + y\cdot b \text{ mit } x,y\in\mathbb{Z}\})$

$\Rightarrow ggT(a,b) \le \min(\{c\in\mathbb{N} \mid c = x\cdot a + y\cdot b \text{ mit } x,y\in\mathbb{Z}\})$ (Satz 6.4(i), $\min(...)\neq 0$)

Damit ist (i) gezeigt.

(ii) Da sich nach Satz 6.14 der ggT(a,b) stets als Linearkombination von a und b darstellen läßt, folgt (ii) sehr schnell, denn der ggT(a,b) ist somit ein Element der Menge aller Linearkombinationen aus a und b. Das heißt aber auch, daß er nicht kleiner sein kann, als das kleinste Element dieser Menge.

$\exists x,y\in\mathbb{Z}: (ggT(a,b) = x\cdot a + y\cdot b)$ (Satz 6.14)

$\Rightarrow ggT(a,b) \in \{c\in\mathbb{N} \mid c = x\cdot a + y\cdot b \text{ mit } x,y\in\mathbb{Z}\}$

Der ggT ist also ein Element der Menge aller Linearkombinationen. Also ist er größer oder gleich dem kleinsten Element dieser Menge.

$\Rightarrow \min(\{c\in\mathbb{N} \mid c = x\cdot a+y\cdot b \text{ mit } x,y\in\mathbb{Z}\}) \le ggT(a,b)$ (def. „min“)

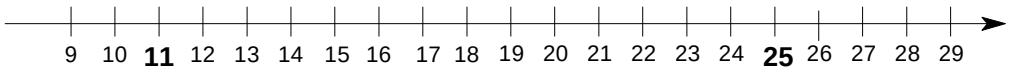
Damit ist (ii) gezeigt.

(i) und (ii) $\overset{\text{"≤" identitiv}}{\Rightarrow}$ $\min(\{c\in\mathbb{N} \mid c = x\cdot a+y\cdot b \text{ mit } x,y\in\mathbb{Z}\}) = ggT(a,b)$

t

6.7 Diophantische Gleichungen

Man lasse sich auf folgendes Spiel ein.
Vorgegeben ist ein Zahlenstrahl etwa so:



Eine Spielfigur steht zuerst auf einer bestimmten natürlichen Zahl, zum Beispiel der 11. Dieses ist das Ausgangsfeld. Das Zielfeld für die Figur ist eine weitere natürliche Zahl, zum Beispiel die 25. Dabei kann man für das Ziehen der Figur verschiedene Varianten vereinbaren. Zwei Beispiele:

1. Die Figur darf 3 oder 10 Schritte nach links oder rechts gezogen werden.

2. Die Figur darf 3 oder 9 Schritte nach links oder rechts gezogen werden.

Als Gewinner(in) könnte man beispielsweise denjenigen (diejenige) bestimmen, der (die) die wenigsten Züge benötigt, um von 11 auf 25 zu kommen.

Denkpause

---

1. Hier gibt es verschiedene Möglichkeiten, um zum Ziel zu gelangen. Man kann z.B. zwei Zehnerschritte nach rechts und zwei Dreierschritte nach links ziehen (das wären 4 Spielzüge) oder einen Zehnerschritt nach links und acht Dreierschritte nach rechts (9 Spielzüge).

2. Es scheint so, als ob man auch nach langem Suchen keine Lösung finden könnte.

Nun zur Auflösung:

Start- und Zielpunkt sind für die Lösung des Problems irrelevant. Entscheidend ist, daß die Figur 14 Schritte weiterziehen soll. Diese 14 Schritte sollen mit Zehner- und Dreierschritten vollzogen werden.

Zieht man x-viele Zehnerschritte und y-viele Dreierschritte weiter, so ist man insgesamt $(x \cdot 10 + y \cdot 3)$-viele Schritte weitergezogen.

Das bedeutet, daß wir Lösungen für x und y der folgende Gleichung suchen: $14 = x \cdot 10 + y \cdot 3$. Dabei gibt x die Anzahl der 10-er Schritte und y die Anzahl der 3-er Schritte an. Da die Schritte in beide Richtungen gezogen werden können, können x und y positiv oder negativ sein. Die positiven Zahlen geben die Schritte nach rechts und die negativen die nach links an.

Also werden $x,y \in \mathbb{Z}$ gesucht mit $14 = 10 \cdot x + 3 \cdot y$,

im 2. Spiel werden dementsprechend $x,y \in \mathbb{Z}$ gesucht mit $14 = 9 \cdot x + 3 \cdot y$.

Solche Gleichungen, in denen es mehr als eine Variable gibt, nennt man **Diophantische Gleichungen** (nach Diophantos von Alexandria, um 250 n. Chr.). In der Zahlentheorie werden dabei vor allem diophantischen Gleichungen der Form $a \cdot x + b \cdot y = c$ (mit $a,b \in \mathbb{N}$ und $c \in \mathbb{Z}$ beliebig vorgegeben) auf deren ganzzahlige Lösungen für die Variablen x und y hin untersucht.

Die dem Spiel zugrundeliegende Problemstellung läßt sich nun wie folgt generalisieren:

Wann existieren für x und y der diophantischen Gleichung $a \cdot x + b \cdot y = c$ ganzzahlige Lösungen? Und wie findet man mögliche Lösungen?

Bekannt ist (Satz 6.14), daß die spezielle diophantische Gleichung:
$a \cdot x + b \cdot y = ggT(a,b)$ stets eine Lösung besitzt.

Wählen wir nun $c \in \mathbb{Z}$ beliebig. Dann gilt:

Satz 6.15

Eine diophantische Gleichung $a \cdot x + b \cdot y = c$ ist genau dann lösbar, wenn c ein Vielfaches des ggT(a,b) ist.
In Zeichen: $\exists (x_0,y_0) \in \mathbb{Z} \times \mathbb{Z}: ((a \cdot x_0 + b \cdot y_0 = c) \Leftrightarrow ggT(a,b) \mid c)$

Zur Bildung von $\mathbb{Z} \times \mathbb{Z}$ vgl. 🕮 Kreuzprodukt.

Anmerkung:
Das Paar (x_0,y_0) wird hier bewußt mit anderen Variablen bezeichnet als in der allgemeinen Form $a \cdot x + b \cdot y = c$, da es sich hierbei um eine spezielle Lösung dieser diophantischen Gleichung handelt. Nähme man erneut (x,y) - was in der Literatur durchaus so gemacht wird - , könnte man meinen, es handele sich hierbei um die einzige Lösung.

Beweis:

„$\Leftarrow$“: $ggT(a,b) \mid c$

$\Rightarrow \exists k \in \mathbb{Z}: (ggT(a,b) \cdot k = c)$ ♦ (Definition „$\mid$“)

Den ggT kann man auch als Linearkombination von a und b schreiben:

$\exists x_1,y_1 \in \mathbb{Z}: (a \cdot x_1 + b \cdot y_1 = ggT(a,b))$ (Satz 6.14)

$\Rightarrow \exists x_1,y_1 \in \mathbb{Z}: ((a \cdot x_1 + b \cdot y_1) \cdot k = ggT(a,b) \cdot k)$ (Eigenschaft „=“)

$\Rightarrow \exists x_1,y_1 \in \mathbb{Z}: ((a \cdot x_1) \cdot k + (b \cdot y_1) \cdot k = ggT(a,b) \cdot k)$ (DIST)

$\Rightarrow \exists x_1,y_1 \in \mathbb{Z}: (a \cdot (k \cdot x_1) + b \cdot (k \cdot y_1) = ggT(a,b) \cdot k)$ (ASS, KOM)

$\Rightarrow \exists x_1,y_1 \in \mathbb{Z}: (a \cdot (k \cdot x_1) + b \cdot (k \cdot y_1) = c)$ (wegen ♦)

Insgesamt gilt also: $(k \cdot x_1, k \cdot y_1)$ ist eine Lösung von $a \cdot x + b \cdot y = c$.

Da k, x_1 und y_1 ganze Zahlen sind, gilt dies auch für $k \cdot x_1$ und $k \cdot y_1$.
Wir haben somit ein (spezielles) ganzzahliges Lösungspaar, nämlich $(x_0,y_0) = (k \cdot x_1, k \cdot x_2)$ $(\in \mathbb{Z} \times \mathbb{Z})$ gefunden.

„$\Rightarrow$“: Nun kann man davon ausgehen, daß $a \cdot x + b \cdot y = c$ eine Lösung $(x_0,y_0) \in \mathbb{Z} \times \mathbb{Z}$ hat: $a \cdot x_0 + b \cdot y_0 = c$ ⚹

Weiterhin folgt aus den Eigenschaften des ggT (Satz 6.6):

$ggT(a,b) \mid a \ \wedge \ ggT(a,b) \mid b$ (Satz 6.6)

$\Rightarrow \ ggT(a,b) \mid a \cdot x_0 + b \cdot y_0$ (6.5 (vii))

$\Rightarrow \ ggT(a,b) \mid c$ (✂)

t

Man hat nun ein Kriterium zur Hand, wann eine Diophantische Gleichung lösbar ist. Nämlich genau dann, wenn der ggT von a und b ein Teiler von c ist.

Wie bestimmt man nun die Lösung (bzw. wie untersucht man die Lösbarkeit) einer diophantischen Gleichung, wenn diese konkret vorgegeben ist. Kehren wir zurück zu unseren beiden Beispielen:

1. Beispiel: $10 \cdot x + 3 \cdot y = 14$ ❀

2. Beispiel: $9 \cdot x + 3 \cdot y = 14$ ❁

1. Schritt: Um zu testen, ob eine Diophantische Gleichung überhaupt lösbar ist, muß man folglich den ggT(a,b) bestimmen. Dies geschieht zumeist mittels des Euklidischen Algorithmus (vgl. Unterkapitel 6.6).

Hier erkennt man allerdings sofort: $ggT(10,3) = 1$ und $ggT(9,3) = 3$.

Da $1 \mid 14$ gilt, besitzt ❀ Lösungen in $\mathbb{Z}$ (vgl. Satz 6.15).

Da $3 \nmid 14$ gilt, besitzt ❁ keine Lösung in $\mathbb{Z}$ (vgl. Satz 6.15).

2.Schritt: Wie in Unterkap. 6.6 erläutert, entwickelt man nun eine Linearkombination des ggT(a,b), indem man im Euklidischen Algorithmus „rückwärts rechnet".
Man erhält eine spezielle Lösung (x_0,y_0) mit $a \cdot x_0 + b \cdot y_0 = ggT(a,b)$.

Für das erste Beispiel gilt: $10 \cdot 1 + 3 \cdot (-3) \ = \ 1 \ (= ggT(10,3))$.

3. Schritt: Man multipliziert die entwickelte Linearkombination mit derjenigen Zahl k, für die gilt $k \cdot ggT(a,b) = c$:

$$\begin{aligned} & a \cdot x_0 + b \cdot y_0 && = && ggT(a,b) && \\ \Rightarrow \quad & k \cdot (a \cdot x_0 + b \cdot y_0) && = && k \cdot ggT(a,b) && \text{(Eigenschaft „=")} \\ \Rightarrow \quad & a \cdot (x_0 \cdot k) + b \cdot (y_0 \cdot k) && = && k \cdot ggT(a,b) && \text{(DIST, ASS, KOM)} \\ \Rightarrow \quad & a \cdot (x_0 \cdot k) + b \cdot (y_0 \cdot k) && = && c && \end{aligned}$$

Dieser Schritt liefert für 14 eine Linearkombination von 10 und 3 und damit eine Lösung der Gleichung ❀.

$$\begin{aligned} & 10 \cdot 1 + 3 \cdot (-3) \ = \ 1 \\ \Rightarrow \quad & (10 \cdot 1) \cdot 14 + (3 \cdot (-3)) \cdot 14) \ = 1 \cdot 14 \\ \Rightarrow \quad & 10 \cdot 14 + 3 \cdot (-42) \ = 14 \end{aligned}$$

4. Schritt: Man erhält mit $(k \cdot x_0, k \cdot y_0)$ ein (spezielles) Lösungspaar der Gleichung $a \cdot x_0 + b \cdot y_0 = c$.

Für unsere Beispielsgleichung ❀ ergibt sich das spezielle Lösungspaar (14,–42).

Wichtig ist an dieser Stelle, aufzupassen, welche der beiden Lösungszahlen zu a und welche zu b gehört. Hier steht beispielsweise 14 bei 10 und ist daher eine spezielle Lösung für x und – 42 ist dementsprechend eine spezielle Lösung für y. Um Verwechslungen zu vermeiden, bietet es sich an, am Ende des dritten Schrittes, die Gleichung so umzuformen, daß die Zahlen a und b in derselben Reihenfolge auftauchen wie in der diophantischen Gleichung, so daß die speziellen Lösungen für x und y direkt abgelesen werden können.

Weiterhin darf man im vierten Schritt auf keinen Fall schreiben: $x = 14$ und $y = -42$, da es für x und y nicht nur eine, sondern unendlich viele Lösungen gibt. Entweder man bezeichnet die Lösung gar nicht mit Variablen (wie wir), oder man wählt noch nicht verwendete Variablen zur Bezeichnung (z.B. x_1 und y_1).

Für unser Spiel am Zahlenstrahl haben wir nun folgende Ergebnisse:

2. Es gibt tatsächlich keine Möglichkeit mit Dreier- und Neunerschritten zum Ziel zu kommen (es liegt nicht daran, daß wir nicht lange genug gesucht haben).

1. Wir kommen auf das gewünschte Feld, indem wir 14 Zehnerschritte nach rechts und 42 Dreierschritte nach links ziehen. Wenn wir so vorgehen müssen wir allerdings 56 Schritte ziehen. Dies ist zwar eine Lösung unseres Problems, aber sicherlich nicht diejenige, mit den wenigsten Zügen (... und wir wollen ja gewinnen). Wie erhält man alle Lösungen (und wie findet man dann heraus, welches die mit den wenigsten Zügen ist)?

Um alle Lösungen zu erhalten, benötigen wir folgenden Satz (ohne Beweis), mit dessen Hilfe man alle Lösungen einer diophantischen Gleichung bestimmen kann, falls man eine spezielle Lösung (und zwar irgendeine) schon kennt:

Satz 6.16

Ist $(x_0,y_0) \in \mathbb{Z} \times \mathbb{Z}$ Lösung der diophantischen Gleichung, dann gilt:

Die Menge $B = \{(x,y) \mid x = x_0 + \frac{b}{ggT(a,b)} \cdot t \quad \wedge \quad y = y_0 - \frac{a}{ggT(a,b)} \cdot t \quad \text{mit } t \in \mathbb{Z}\}$

umfaßt alle Lösungen der diophantischen Gleichung .

Für unser Beispiel bedeutet dies:

$$B = \{ (x,y) \mid x = 14 + \tfrac{3}{1} \cdot t \quad \wedge \quad y = -42 - \tfrac{10}{1} \cdot t \quad \text{mit } t \in \mathbb{Z} \}$$
$$= \{ (x,y) \mid x = 14 + 3 \cdot t \quad \wedge \quad y = -42 - 10 \cdot t \quad \text{mit } t \in \mathbb{Z} \}$$

Man vergewissere sich, daß die drei bereits gefundenen Paare (2,–2), (–1,8) und (14,–42) tatsächlich in der Menge B enthalten sind. (**A6**)

Schauen wir uns die Menge B nun etwas genauer an, indem wir einige konkrete Werte für (x,y) ausrechnen. Wir setzen dabei für t die Zahlen von –2 bis +2 ein:

$B = \{ ..., (8,-22), (11,-32), (14,-42), (17,-52), (20,-62) ... \}$

Betrachtet man die Lösungen für x und y getrennt, so erkennt man, daß sich die Werte von x von Lösungspaar zu Lösungspaar jeweils um 3 ändern, die Werte für y jeweils um 10. Weiterhin fällt auf, daß sich die Werte für y verringern, wenn sich die entsprechenden für x erhöhen und umgekehrt: Von Lösungspaar (8,–22) zu Paar (11,–32) erhöht sich der x-Wert um 3 und gleichzeitig verringert sich der y-Wert um 10.

Warum ist das so?

Der Term für x läßt sich wie folgt umformen:

$x = 14 + 3 \cdot t = 2 + 12 + 3 \cdot t = 2 + 3(4+t) = 3(4+t) + 2$ ♣

Hier erkennt man, daß x bei Division durch 3 immer den Rest 2 läßt (vgl. 🕮 Division mit Rest).

In der Kongruenzschreibweise läßt sich das wie folgt festhalten:

$$\begin{aligned} & 3(4+t) + 2 \equiv 2 \ (3) \\ \Rightarrow \quad & x \equiv 2 \ (3) \qquad (\clubsuit) \end{aligned}$$

Die Menge aller Lösungen dieser Kongruenz kann man nun wie folgt festhalten:

$$\mathbb{L}_x = \{x \mid x \in \mathbb{Z} \ \wedge \ x \equiv 2 \ (3)\}$$

$\mathbb{L}_x$ enthält alle Zahlen, die kongruent 2 modulo 3 sind (das sind unendlich viele). Sie bilden eine sogenannte R e s t k l a s s e bezüglich des Moduls 3:

Definition Restklasse

R e s t k l a s s e n sind Mengen von Zahlen, die bei Division durch eine bestimmte Zahl, denselben Rest lassen.

In Zeichen: $[a]_b := \{x \mid x \in \mathbb{Z} \ \wedge \ x \equiv a \ (b)\}$
$:= \{x \mid x \in \mathbb{Z} \ \wedge \ x = a + k \cdot b\}$

Die Restklassen sind nichts anderes als die Äquivalenzklassen bezüglich der Kongruenzrelation.
Da die „≡"-Relation eine 🕮 Äquivalenzrelation ist, zerlegt sie $\mathbb{Z}$ vollständig in 🕮 Äquivalenzklassen.
Für den Modul 3 sieht das beispielsweise so aus: $[0]_3 \cup [1]_3 \cup [2]_3 = \mathbb{Z}$, d.h. wenn man die Menge aller Zahlen, die den Rest 0 bei Division durch 3 lassen, mit der Menge aller Zahlen, die den Rest 1 lassen, und mit der Menge aller Zahlen, die den Rest 2 lassen, vereinigt, erhält man die Menge aller ganzen Zahlen.

Was kann man für die Lösungen für y folgern? (**A7**)

Nun kann man die Lösungen für x und y problemlos errechnen. Doch wie finden wir nun die Lösung mit den wenigsten Zügen?

Halten wir nun erstmal einige Lösungen in einer Tabelle fest:

t	…	–6	–5	–4	–3	–2	–1	0	1	2	…
x	…	–4	–1	2	5	8	11	14	17	20	…
y	…	18	8	–2	–12	–22	–32	–42	–52	–62	…
$\lvert x \rvert + \lvert y \rvert$	…	22	9	4	17	30	43	56	69	82	…

In der letzten Zeile ist jeweils die Anzahl der Züge angegeben. Man erkennt, daß diese für $t = -4$ am kleinsten ist.
Für $t < -6$ wachsen sowohl die Werte für $\lvert x \rvert$, als auch die Werte für $\lvert y \rvert$, so daß die Anzahl der Spielzüge immer größer wird. Dasselbe gilt auch für $t > 2$.

Ergebnis: Mit 2 Zehnerschritten nach rechts und 2 Dreierschritten nach links gewinnt man auf jeden Fall!

LÖSUNGEN der Arbeitsaufgaben dieses Unterkapitels:

A6 $2 = 14+3\cdot t \;\wedge\; -2 = -42-10\cdot t \;\Rightarrow\; t = (-12):3 \;\wedge\; t = 40:(-10) \;\Rightarrow\; t = -4$

Für $t = -4$ erhält man somit das Lösungspaar $(2,-2)$. Da $-4 \in \mathbb{Z}$, gilt $(2,-2) \in B$.

Analog ergibt sich:

Für $t = -5$ erhält man das Lösungspaar $(-1,8)$. Da $-5 \in \mathbb{Z}$, gilt $(-1,8) \in B$.

Für $t = 0$ (vgl. auch Tabelle) erhält man das Lösungspaar $(14,-42)$. Da $0 \in \mathbb{Z}$, gilt $(14,-42) \in B$.

A7 Der Term für y läßt sich wie folgt umformen:

$y = -42 - 10\cdot t = -2 - 40 - 10\cdot t = -2 + 10\cdot(-4-t) = 10\cdot(-4-t) - 2$ ♣

Hier erkennt man, daß y kongruent 8 modulo 10 ist:

$10 \mid 10\cdot(-4-t)$

$\Rightarrow \quad 10\cdot(-4-t) \equiv 0 \quad (10)$ (Satz 6.11)

$\Rightarrow \quad 10\cdot(-4-t) - 2 \equiv -2 \quad (10)$ ($2 \equiv 2$ (10), Subtr. v. Kongr.)

$\Rightarrow \quad y \equiv 8 \quad (10)$ (♣, $-2 \equiv 8$ (10), TRANS „≡“)

Die Menge aller Lösungen dieser Kongruenz kann man nun wie folgt festhalten:

$\mathbb{L}_y = \{ y \mid y \in \mathbb{Z} \;\wedge\; y \equiv 8 \quad (10) \}$

6.8 Teilbarkeitsregeln und Rechenproben

— Zahlentheorie in der Grundschule

Als kleiner Ausblick erfolgen nun stellvertretend für eine Vielzahl von Anwendungen zwei Bereiche aus dem Mathematikunterricht der Grundschule, in denen die Zahlentheorie eine wichtige Rolle spielt:

- Teilbarkeitsregeln
- Rechenproben

6.8.1 Teilbarkeitsregeln

Teilbarkeitsregeln haben zum Ziel, die Untersuchung von vorgelegten Zahlen bezüglich ihrer Teilbarkeit zu vereinfachen, indem statt diesen kleinere Zahlen untersucht werden, die es aufgrund der Regel gestatten, auf die Teilbarkeit der größeren Zahl zu schließen.

Als einführendes Beispiel soll die sogenannte Neunerregel dienen. Dabei wollen wir keinen streng formalen Beweis (dieser ist in Ü8 von Kap.5 gefordert) durchführen, sondern die Regel mit grundschultypischen Mitteln herleiten. Dazu argumentieren wir im folgenden an der 🕮 Stellentafel.

Bei der Herleitung einer Teilbarkeitsregel an der Stellentafel versucht man, die Zahl zu verkleinern, indem man Plättchen wegnimmt oder nach rechts verschiebt, wo ihnen ein kleinerer Stellenwert zugeordnet wird. Entscheidend ist dabei jeweils, sicherzustellen, daß der Divisionsrest der vorgelegten Zahl trotz der Veränderung gleichbleibt.

Hier wird die Methode des Verschiebens angewandt:

Eine beliebige Zahl n sei durch Plättchen in der Stellentafel dargestellt.
Was passiert nun, wenn man ein beliebiges Plättchen um eine Spalte nach rechts verschiebt?
Nun, offensichtlich wird die Zahl kleiner (das freut uns), da das Plättchen in einer weiter rechts stehenden Spalte einen kleineren Stellenwert hat.

Aber: Ändert sich dabei die Teilbarkeit der Zahl durch 9?

Das müssen wir unbedingt ausschließen, denn sonst haben wir die Zahl zwar verkleinert, aber die kleinere Zahl hat nicht denselben Neunerrest wie unsere Ausgangszahl. Wenn sich der Neunerrest beim Verschieben nämlich nicht ändern würde, könnte man von den Zahlen, die man durch das Verschieben erhält, nicht auf die Ausgangszahl rückschließen. D.h. dann erhalten wir so mit Sicherheit keine Teilbarkeitsregel.

Betrachten wir dazu ein konkretes Beispiel:

Die Zahl 3537 soll auf Teilbarkeit durch 9 untersucht werden.

Darstellung in der Stellentafel:

T	H	Z	E
○○○	○○○○○	○○○	○○○○○ ○○

Als mögliche Verschiebungen kommen in Frage:

Von der Tausender- in die Hunderterspalte (T $\rightarrow$ H), von der Hunderter- in die Zehnerspalte (H $\rightarrow$ Z), und von der Zehner- in die Einerspalte (Z $\rightarrow$ E).

Beginnen wir mit Z $\rightarrow$ E: Bei einer Verschiebung eines Plättchens von der Zehner- in die Einerspalte, wird die Zahl um 10 verringert (in der Zehnerspalte ist ja nun ein Plättchen weniger) und gleichzeitig um 1 erhöht (in der Einerspalte befindet sich jetzt ein Plättchen mehr), d.h. die in der Stellentafel dargestellte Zahl wurde um 9 verkleinert. Werden mehrere Plättchen von der Zehner- in die Einerspalte verschoben, verringert sich die Zahl demnach um eine Vielfaches von 9.

Bei der Verschiebung H $\rightarrow$ Z wird die Zahl um 100 verringert und um 10 erhöht, d.h. die Zahl verringert sich um 90, bei der Verschiebung mehrerer Plättchen um ein Vielfaches von 90.

Entsprechend den beiden anderen Verschiebungen wird die Zahl bei T $\rightarrow$ H um ein Vielfaches von 900 vermindert.

Was fällt auf?

Die Zahl wird bei jeder Verschiebung von Plättchen nach rechts um ein Vielfaches von 9 verringert. Da ein Vielfaches von 9 den Neuner-Rest 0 läßt, ändert sich bei keiner der Verschiebungen der Neuner-Rest, d.h. die nach der Verschiebung erhaltene Zahl hat denselben Neuner-Rest wie die zu untersuchende Zahl (hier: 3537). Ist die nach der Verschiebung erhaltene Zahl durch 9 teilbar, dann ist demnach auch 3537 durch 9 teilbar.

Dann mal fröhlich ans Verschieben:

3T $\rightarrow$ 3H : $-3000 + 300 = -2700$, d.h. die Zahl wird um 2700 verringert und wir erhalten in der Hunderterspalte zu den 5 Plättchen 3 hinzu:

T	H	Z	E
	○○○○○ ○○○	○○○	○○○○○ ○○

8H $\rightarrow$ 8Z : $-800 + 80 = -720$, d.h. die Zahl wird um 720 verringert und wir erhalten in der Zehnerspalte 8 Plättchen hinzu:

T	H	Z	E
		○○○○○ ○○○○○ ○	○○○○○ ○○

11Z $\rightarrow$ 11E : $-110 + 11 = -99$, d.h. die Zahl wird um 99 verringert und wir erhalten in der Einerspalte 11 Plättchen hinzu:

T	H	Z	E
			○○○○○ ○○○○○ ○○○○○ ○○○

Nachdem alle möglichen Verschiebungen durchgeführt worden sind, liegen 7 + 11 = 18 Plättchen in der Einer-Spalte - und (das ist das Tolle!) der Neuner-Rest der erhaltenen Zahl (18 eben) ist derselbe wie der von 3537.

Da 9 ein Teiler von 18 ist, ist demzufolge auch 3537 durch 9 teilbar.

Was bedeutet das allgemein?

Nachdem alle möglichen Verschiebungen durchgeführt worden sind, liegen alle Plättchen in der Einer-Spalte. Die Anzahl dieser Plättchen entspricht der Summe der Plättchenanzahlen der zuvor dargestellten Zahl, d.h. der Summe der Ziffern. In unserem Beispiel liegen am Schluß $3 + 5 + 3 + 7 = 18$ Plättchen in der letzten Spalte. Die Summe der Ziffern einer Zahl nennt man auch die Q u e r s u m m e der Zahl (da „quer", d.h. beispielsweise von rechts nach links, addiert wird):

Definition Quersumme

Die Quersumme einer natürlichen Zahl ist die Summe ihrer Ziffern.
Für die Quersumme von n wird abkürzend **Q(n)** geschrieben.
In Zeichen:
Sei $n \in \mathbb{N}$ in ihrer dekadischen Darstellung[45] wie folgt angegeben:
$n = a_k \cdot 10^k + \ldots + a_1 \cdot 10 + a_0$ mit $0 \leq a_i < 10$ für $i \in \{0,1,2,\ldots,k\}$
Dann gilt: $Q(n) = a_0 + a_1 + a_2 + \ldots + a_k$

Obige Überlegungen münden in folgendem Satz:

Teilbarkeitsregel für 9 (Neunerregel)

Eine (natürliche) Zahl n ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.
In Zeichen: $9 \mid n \Leftrightarrow 9 \mid Q(n)$

Die an der Stellentafel durchgeführten Betrachtungen liefern noch mehr als eine Teilbarkeitsregel:
Wir haben herausgefunden, daß eine natürliche Zahl denselben Neuner-Rest läßt wie ihre Quersumme. Damit haben wir einen Zusammenhang entdeckt, der über die aufgestellte Teilbarkeitsregel hinausgeht und wir können eine „Reste-Regel" für die Division durch 9 formulieren[46]:

Eine natürliche Zahl n läßt bei Division durch 9 denselben Rest wie die Quersumme von n.
In Zeichen: $n \equiv Q(n) \ (9)$

An der Stellentafel läßt sich also die Gültigkeit von Teilbarkeitsregeln und von Reste-Regeln begründen und veranschaulichen. Dieses Verfahren läßt sich so aufbereiten, daß auch Grundschüler Einsicht in die Gültigkeit von Teilbarkeitsregeln gewinnen können.
Eine mathematisch „wasserdichte" Begründung der Allgemeingültigkeit derartiger Regeln über die Stellentafel ist wesentlich aufwendiger, da man zeigen muß, daß die Regeln für beliebige Zahlen zutreffen. Der/die Leser(in) versuche sich an Ü8 und Ü9 aus Kapitel 5. Bei den Aufgaben sollte eine allgemeingültige Herleitung im Vordergrund stehen, während in diesem Unterkapitel der Schwerpunkt auf der Idee und die Einsicht in die Gültigkeit von Teilbarkeitsregeln liegt.

[45] vgl. Satz 5.1
[46] Natürlich könnte man diese Regel auch mit Hilfe der Division mit Rest notieren. Kürzer und besser zu handhaben ist jedoch eine Formulierung in der Kongruenzschreibweise (vgl. Satz 6.11).

Die Herleitung von Teilbarkeitsregeln (und Reste-Regeln) anhand Betrachtungen an der Stellentafel sind zwar anschaulich, aber eine korrekte Begründung ihrer Allgemeingültigkeit ist recht aufwendig. Mit Hilfe der Kongruenzschreibweise lassen sich Teilbarkeitsregeln für jede beliebige Zahl entwikkeln und beweisen.

Dazu geht man von einer beliebigen Zahl n aus und stellt diese in ihrer 🕮 Dezimaldarstellung dar:

$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0$

mit $a_i \in \mathbb{N}_0$ und $0 \le a_i < 10$ für $i \in \{0,1,2,...,k\}$ und $a_k \neq 0$ (vgl. Satz 5.1)

Für eine derart dargestellte Zahl kann nun eine Teilbarkeitsregel aufgestellt werden. Wir werden im folgenden die Teilbarkeitsregel für 9 auch auf diesem Weg entwickeln:

Dazu versuchen wir, die 10er-Potenzen, die in der Dezimaldarstellung von n auftreten, durch kleinere Zahlen, die denselben Neuner-Rest haben zu ersetzen (dies entspricht einem Verschieben der Plättchen).

Es gilt:

$10 \equiv 1 \ (9)$ $\quad (10 = 1 \cdot 9 + 1)$

$\Rightarrow \ 10^1 \equiv 1^k \ (9) \ \wedge \ 10^2 \equiv 1^k \ (9) \ \wedge \ ... \ \wedge \ 10^k \equiv 1^k \ (9)$ $\quad$ (Potenz. b. Kongr.)

$\Rightarrow \ 10^1 \equiv 1 \ (9) \ \wedge \ 10^2 \equiv 1 \ (9) \ \wedge \ ... \ \wedge \ 10^k \equiv 1 \ (9)$ [47]

Nun lassen sich nach Satz 6.10 (iii) diese Kongruenzen mit den (wegen REFL „≡“ geltenden) Kongruenzen $a_1 \equiv a_1 \ (9) \ \wedge \ a_2 \equiv a_2 \ (9) \ \wedge \ ... \ \wedge \ a_k \equiv a_k \ (9)$ multiplizieren:

$\Rightarrow \ a_1 \cdot 10^1 \equiv a_1 \ (9) \ \wedge \ a_2 \cdot 10^2 \equiv a_2 \ (9) \ \wedge \ ... \ \wedge \ a_k \cdot 10^k \equiv a_k \ (9)$ [48]

Wegen REFL „≡“ gilt außerdem: $a_0 \equiv a_0 \ (9)$ [49].

Nun können wir nach Satz 6.10 (i) alle aufgestellten Kongruenzen addieren:

$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0 \equiv a_k + a_{k-1} + ... + a_1 + a_0 \ (9)$ [50]

$\Rightarrow \quad n \equiv Q(n) \ (9)$

aus dieser Reste-Regel ergibt sich: $9 \mid n \ \Leftrightarrow \ 9 \mid Q(n)$

Damit haben wir die oben an der Stellentafel hergeleitete Teilbarkeitsregel auch über Kongruenzen bewiesen.

Neben der Quersumme gibt es auch die sogenannte alternierende Quersumme (alternieren bedeutet abwechseln), bei der die Ziffern abwechselnd addiert und subtrahiert werden:

Definition alternierende Quersumme

Sei $n \in \mathbb{N}$ in ihrer dekadischen Darstellung wie folgt angegeben:
$n = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0$ mit $0 \le a_i < 10$ für $i \in \{0,1,2,...,k\}$

Dann heißt **Q'(n)** $= a_0 + (-a_1) + a_2 + (-a_3) + ... + (-1)^k a_k$
die alternierende Quersumme dieser Zahl.

[47] Diese Zeile gibt die Verschiebungen Z → E, H → E usf. wieder.
[48] Wenn man ein Plättchen verschiebt, kann man auch mehrere verschieben ...
[49] Die Plättchen in der Einerspalte werden nicht verschoben (aber berücksichtigt).
[50] Die Summe auf der rechten Seite der Kongruenz gibt die Anzahl aller Plättchen wieder.

Die alternierende Quersumme bildet die Grundlage weiterer Teilbarkeitsregeln. Beispielsweise die Teilbarkeitsregel für 11 läßt sich mit Hilfe der alternierenden Quersumme formulieren:

Teilbarkeitsregel für 11 (Elferregel)

Eine (natürliche) Zahl n ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

In Zeichen: $11 \mid n \Leftrightarrow 11 \mid Q'(n)$

Entsprechend zur Neunerregel läßt sich auch eine Reste-Regel für die Division durch 11 formulieren:

Eine natürliche Zahl n läßt bei Division durch 11 denselben Rest wie die Quersumme von n.

In Zeichen: $n \equiv Q'(n)\ (11)$

Den Beweis führe der/die Leser(in) selbst (Ü20).

Bemerkung: Meist wird mit Hilfe von Kongruenzen die Reste-Regel gezeigt. Aus der Reste-Regel folgt dann sofort die Teilbarkeitsregel.

Auf der Suche nach einer Teilbarkeitsregel für 4 stoßen wir auf diese Äußerung eines (Schulbuch-)Schülers.

Max Schlaumeier behauptet:

„Wenn Du 'ne große Zahl hast und Du weißt nicht, ob da die 4 reinpaßt, dann brauchste nur die letzten beiden Ziffern anzugucken - und schon weißt Du's."

Wie kann man nachprüfen, ob Max Schlaumeier seinen Namen zu recht trägt?

Untersuchen wir (wiederum) eine beliebige natürliche Zahl n.

$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0$

mit $a_i \in \mathbb{N}_0$ und $0 \le a_i < 10$ für $i \in \{0,1,2,...,k\}$ und $a_k \neq 0$ (vgl. Satz 5.1)

Man betrachtet die Reste der Zehnerpotenzen bei Division durch 4:

$$10 \equiv 2\ (4)$$

Das bedeutet, jede 10 in der obigen Darstellung von n läßt sich durch 2 ersetzen (genauer: 10^2 durch 2^2 usw.). Das macht die Zahl ganz schön viel kleiner, aber es gibt noch bessere Ersetzungen der Zehnerpotenzen:

$$10^2 \equiv 0\ (4) \qquad (\text{denn } 4 \mid 100 \text{ bzw. } 100 = 25 \cdot 4 + 0)$$

Jetzt können wir unsere Suche abbrechen, denn etwas Besseres kann uns gar nicht passieren: Wenn sich (wie wir gleich zeigen werden) auch die nächsten Zehnerpotenzen durch Nullen ersetzen lassen, wird unsere Ausgangszahl stark verkleinert.

$$10^2 \equiv 0\ (4)$$

$\Rightarrow \quad 10^i \equiv 0\ (4)$ für alle $i \ge 2$ (Mult. mit $10 \equiv 10\ (4)$, Satz 6.10 (iii))

$\Rightarrow \quad a_i \cdot 10^i \equiv a_i \cdot 0\ (4)$ für alle $i \ge 2$ (Mult. mit $a_i \equiv a_i\ (4)$, Satz 6.10 (iii))

$\Rightarrow \quad a_2 \cdot 10^2 \equiv 0\ (4) \wedge a_3 \cdot 10^3 \equiv 0\ (4) \wedge ... \wedge a_k \cdot 10^k \equiv 0\ (4)$ für $k \ge 2$

Weiterhin gilt wegen REFL „≡": $a_0 \equiv a_0\ (4)$ und $a_1 \cdot 10^1 \equiv a_1 \cdot 10^1\ (4)$

Nun können wir nach Satz 6.10 (i) alle aufgestellten Kongruenzen addieren:

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + ... + a_1 \cdot 10^1 + a_0 \equiv a_1 \cdot 10^1 + a_0 \quad (4)$$

$$\Rightarrow \qquad n \equiv a_1 \cdot 10^1 + a_0 \quad (4)$$

Was für eine Zahl wird durch $a_1 \cdot 10^1 + a_0$ dargestellt?

$a_1 \cdot 10^1 + a_0 = a_1 \cdot 10^1 + a_0 \cdot 10^0$ entspricht $(a_1\, a_0)_{10}$, d.h. der Zahl $a_1 a_0$ im uns vertrauten Zehnersystem (vgl. Unterkap. 5.3).

Folglich hängt der Rest einer natürlichen Zahl bei Division durch 4 ausschließlich von den letzten beiden Ziffern der Zahl ab, genauergesagt von der Zahl, die durch die beiden letzten Ziffern dargestellt wird.

Wir haben somit eine Teilbarkeitsregel für 4 hergeleitet:

Teilbarkeitsregel für 4

Eine (natürliche) Zahl n ist genau dann durch 4 teilbar, wenn die durch ihre letzten beiden Ziffern dargestellte Zahl durch 4 teilbar ist.

In Zeichen:
Sei $n \in \mathbb{N}$ in ihrer dekadischen Darstellung wie folgt angegeben:
$n = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0$ mit $0 \le a_i < 10$ für $i \in \{0,1,2,...,k\}$
Dann gilt: $4 \mid n \Leftrightarrow 4 \mid a_1 a_0$

Dies ist eine sogenannte E n d s t e l l e n r e g e l, da die Teilbarkeit der Zahl von ihren letzten Stellen abhängt. Es gibt auch Endstellenregeln, bei der es ausschließlich auf die letzte Zahl ankommt, bei anderen muß die Zahl, die durch die letzten drei Ziffern dargestellt wird, untersucht werden usw.

Entsprechend zur Neunerregel läßt sich auch eine „Reste-Regel“ für die Division durch 4 formulieren:

Eine natürliche Zahl n läßt bei Division durch 4 denselben Rest wie die Zahl, die durch ihre letzten beiden Ziffern dargestellt wird.

In Zeichen: $n \equiv a_1 a_0 \quad (4)$

Tatsächlich trägt Max Schlaumeier seinen Namen nicht ohne Grund.

Wie findet man, wenn kein Max Schlaumeier als Muse zur Verfügung steht, den Ansatz zu der Herleitung einer Teilbarkeitsregel?

Wir suchen eine Teilbarkeitsregel für t. Gegeben ist die Zahl n (gähn!) in ihrer Dezimaldarstellung:

Die Größe von n hängt entscheidend von den 10er-Potenzen ab. Schön wäre, man könnte statt der 10er-Potenzen jeweils eine **1** oder eine **–1** schreiben und die Teilbarkeit durch t würde dadurch nicht beeinflußt - die nun zu betrachtende Zahl wäre viel kleiner, da nur noch die Ziffern addiert, bzw. subtrahiert würden (man erhielte eine Quersummenregel oder eine alternierende Quersummenregel).
Als besonders fein erweist es sich, wenn man für alle oder zumindest einige der 10er-Potenzen eine **0** schreiben kann, ohne die Teilbarkeit durch t zu beeinflussen: Dann ist ein großer Teil der Summe Null, und die noch auf Teilbarkeit durch t zu betrachtende Zahl ist wesentlich kleiner.

Die 10er-Potenzen lassen sich nur ersetzen, ohne daß sich die Teilbarkeit der Zahl durch t verändert, wenn sie denselben Rest lassen wie die sie ersetzenden Nullen oder Einsen (oder auch anderer Zahlen). Um herauszufinden, ob eine der Möglichkeiten in Betracht kommt, wird untersucht, zu welchen Zahlen die 10er-Potenzen kongruent (restgleich) modulo t sind.

Wir wissen nicht, was Max Schlaumeier empfiehlt.
Wir empfehlen Ü20.

6.8.2 Rechenproben

Aus den Teilbarkeitsregeln für 9 und für 11 lassen sich Rechenproben ableiten, mit denen man die Richtigkeit bestimmter Rechnungen überprüfen kann. Dies könnte man im vierten Schuljahr thematisieren - leider wird das allzuselten gemacht.

Für die Summe und das Produkt von Quersummen gilt:

„N e u n e r p r o b e “

Für $a,b \in \mathbb{N}$ gilt:	(i) $Q(a+b) \equiv Q(a)+Q(b)$ (9)
	(ii) $Q(a \cdot b) \equiv Q(a) \cdot Q(b)$ (9)

Beweis:

zu (i):

Es gilt: $a+b \equiv Q(a+b)$ (9) ◆ (Neunerregel, $a+b \in \mathbb{N}$)

Aus $a \equiv Q(a)$ (9)

und $b \equiv Q(b)$ (9) (Neunerregel)

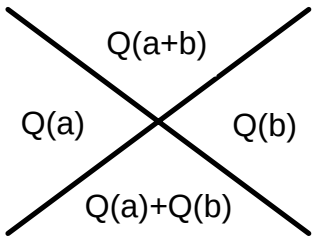
folgt $a+b \equiv Q(a) + Q(b)$ (9) ◆◆ (Satz 6.10 (i))

Aus ◆ und ◆◆ folgt mit TRANS „≡“: $Q(a+b) \equiv Q(a) + Q(b)$ (9)

t

Der Beweis von (ii) läuft völlig analog, da hier nur das „+“ Zeichen durch das „·“ Zeichen ersetzt werden muß, und statt Satz 6.10 (i) wird Satz 6.10 (iii) zur Begründung herangezogen.

Wenn die Neunerprobe in der Grundschule behandelt wird, dann wird den Schüler(innen) meist nebenstehendes Diagramm (bzw. ein entsprechendes für (ii)) an die Hand gegeben, in das sie beim Erstellen der einzelnen Quersummen ihre Zwischenergebnisse eintragen können.



Beispiele zu Rechenprobe (i):

Stimmt folgende Rechnung? $1731 + 2436 = 3167$

Um die Rechnung zu prüfen, bildet man die Quersummen von 1731, 2436 und 3167:

$Q(1731) = 12$, $Q(2436) = 15$ und $Q(3167) = 17$

Gilt nun $Q(1731) + Q(2436) \equiv Q(3167)$ (9) ?

$12 + 15 \equiv 17$ (9) gilt nicht, da $27 = 3 \cdot 9 + 0$, aber $17 = 1 \cdot 9 + 8$

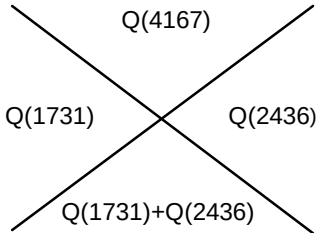
Da die Quersummen nicht kongruent modulo 9 sind, ist das Ergebnis der Addition mit Sicherheit falsch.

Stimmt folgende Rechnung?

$1731 + 2436 = 4167$

Gilt $Q(1731) + Q(2436) \equiv Q(4167)$ (9) ?

$12 + 15 \equiv 18$ (9) $\Leftrightarrow$ $27 \equiv 18$ (9) gilt,
da $9 \mid 27 - 18$



Das Ergebnis der Addition ist damit wahrscheinlich richtig.

Daraus, daß die Quersummen kongruent sind, läßt sich leider nicht folgern, daß die Rechnung auf jeden Fall richtig sein muß. Es ist lediglich wahrscheinlicher, daß sie richtig ist, als daß sie falsch ist.[51]

Ein weiteres Beispiel: $1731 + 2436 = 4176$

Die Rechnung stimmt offensichtlich nicht, dennoch gilt:
$Q(1731) + Q(2436) \equiv Q(4176)$ (9)
Die Vertauschung der Ziffern in der Ergebniszahl verändert zwar die Zahl, nicht aber deren Quersumme.

Das richtige Ergebnis der Addition unterscheidet sich von dem falschen um 9. Hier liegt der Grund dafür, warum der Fehler nicht von der Neunerprobe aufgedeckt wird:

Immer dann, wenn sich das falsche Ergebnis um ein Vielfaches von 9 von dem richtigen Ergebnis unterscheidet, kann die Neunerprobe den Fehler nicht finden.

Eine größere Sicherheit bei der Überprüfung von Rechnungen erhält man, wenn zusätzlich noch eine zweite Rechenprobe angewandt wird:

Die sogenannte Elferprobe läßt sich aus der Elferregel herleiten und ihre Anwendung funktioniert ganz genauso wie die Neunerregel:

„E l f e r p r o b e“

Für $a,b \in \mathbb{N}$ gilt:	(i) $Q(a+b) \equiv Q(a)+Q(b)$ (11)
	(ii) $Q(a \cdot b) \equiv Q(a) \cdot Q(b)$ (11)

Der Beweis verläuft wie bei der Neunerprobe, so daß hier auf ihn verzichtet werden kann.

Auch wenn beide Proben stimmen, kann nicht auf die Gültigkeit der jeweiligen Addition oder Multiplikation geschlossen werden. Wenn jedoch auch nur eine von ihnen nicht stimmt, ist das Ergebnis auf jeden Fall falsch.

[51] „Alles, was lediglich wahrscheinlich ist, ist wahrscheinlich falsch.“ (Descartes)

6.9 Übungsaufgaben

Ü1

a) Bestimme die folgenden Teilermengen:
(i) T(48) (ii) T(90) (iii) T(36)

b) Gibt es eine Zahl n, für die gilt: $T(48) \cap T(36) = T(n)$?

Ü2

Man betrachte die Aussage $a|b \wedge a|c \Rightarrow a|b-c$

a) Ist diese Aussage in $\mathbb{Z}$ gültig? (mit Beweis!)

b) Wann gilt die Aussage in $\mathbb{N}_0$?

Ü3

Beweise oder widerlege (durch ein konkretes Gegenbeispiel) die folgenden Aussagen. Hierbei seien $a,b,c \in \mathbb{N}$.

a) $a|b+c \Rightarrow a|b \vee a|c$

b) $a|b \vee a|c \Rightarrow a|b+c$

c) $a|b+c \wedge a|b \Rightarrow a|c$

d) $a|b \wedge c|d \Rightarrow ac|bd$

e) $a|b \vee a|c \Rightarrow a|bc$

f) $a|bc \Rightarrow a|b \vee a|c$

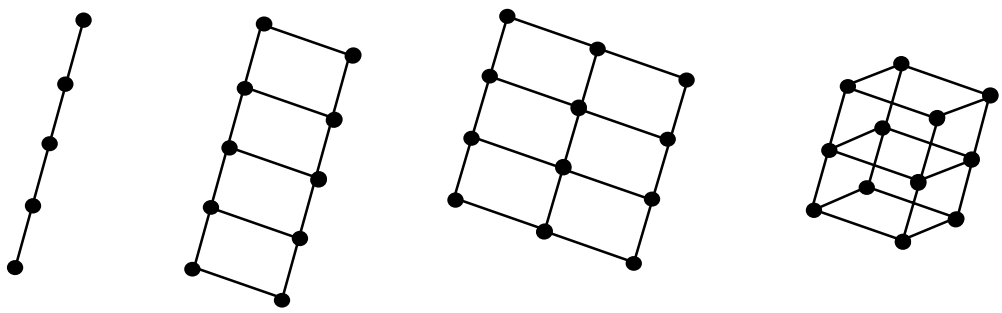
Ü4

Beweise die Aussage von Satz 6.3 (iii): $a|b \wedge a|c \Rightarrow a|m \cdot b + n \cdot c$
durch Verwendung der Definition Teilbarkeit

Ü5

a) Erstelle die Hasse-Teiler-Diagramme für (i) T(48) (ii) T(56) (iii) T(225). [Tip: Die Primfaktorzerlegung der jeweiligen Zahlen leistet sowohl bei der Bestimmung der Teilermengen, als auch bei der Erstellung der Diagramme gute Dienste.]

b) Gib für die folgenden Hasse-Teiler-Diagramme jeweils zwei verschiedene Beschriftungen an:



(i) (ii) (iii) (iv)

c) Warum sind solche Diagramme für die Darstellung von Teilermengen nur bedingt geeignet?

d) Bestimme den ggT(45,75), indem Du die Hasse-Diagramme von T(45) und T(75) übereinanderzeichnest.
Wie läßt sich dementsprechend der ggT(48,56) bestimmen? Versuche, das Verfahren anschaulich zu beschreiben.
Wie kann man bei der kgV-Bestimmung vorgehen? Bestimme kgV(9,25).

Ü6

Beweise mit Vollständiger Induktion über n: $2 \mid 3^n - 1$

(Weitere Beweise von Teilbarkeitsaussagen über Vollständige Induktion findet man in Ü9 und Ü11 von Kap. 5)

Ü7

Zeige, daß folgende Aussage für alle $a,b,c \in \mathbb{N}$ gilt:

$a \mid b \cdot c \ \wedge \ ggT(a,b) = 1 \ \Rightarrow \ a \mid c$

Ü8

Zeige, daß folgende Aussage für alle $a,b,n \in \mathbb{N}$ gilt:

$a \equiv b \ (n) \ \Rightarrow \ ggT(a,n) = ggT(b,n)$

Gilt auch die Umkehrung?

Ü9

a) Sei a Teiler von b. Zeige, daß es dann auch eine Zahl gibt, die sich mit a multiplikativ zu b „ergänzt“. Begründe, warum diese Zahl der Komplementärteiler von a bzgl. b genannt wird.

b) Sei $n \in \mathbb{N}$ eine natürliche Zahl, bei der die Summe ihrer Teiler 2n beträgt.
Die Teiler von n seien wie folgt bezeichnet:
$1, t_1, ..., t_k, n$ mit $1 \le t_1 \le t_2 \le ... \le t_k \le n$
Zeige mit Hilfe von a): $1 + \frac{1}{t_1} + ... + \frac{1}{t_k} + \frac{1}{n} = 2$

Ü10

a) Bestimme mit Hilfe des Euklidischen Algorithmus:
i) ggT(360, 945) ii) ggT(6765, 4181)

b) Löse folgende diophantische Gleichung mittels des Euklidischen Algorithmus: $364x + 442y = 52$

Ü11

Zeige auf zwei verschiedene Arten, daß für alle $a \in \mathbb{N}$ gilt: $5 \mid a^5 - a$

Ü12

Hat $b \in \mathbb{N}$ den Sechserrest r, so hat auch b^3 den Sechserrest r.

Ü13

a) Warum kann es keine Quadratzahl geben, die bei Division durch 3 den Rest 2 läßt? Betrachte dazu die möglichen Reste einer Zahl $a \in \mathbb{N}$ bei Division durch 3 sowie die entsprechenden Reste der dazugehörigen Quadratzahl.

b) Welche Reste können Quadratzahlen bei Division durch 8 lassen?

Ü14

Beweise oder widerlege die beiden folgenden Aussagen:

a) $5 \mid a^2 + b^2 \;\Rightarrow\; 5 \mid a \;\wedge\; 5 \mid b$

b) $7 \mid a^2 + b^2 \;\Rightarrow\; 7 \mid a \;\wedge\; 7 \mid b$

Ü15

Beweise mit Hilfe der Division mit Rest, daß für alle $n \in \mathbb{N}$ gilt: $3 \mid n(n+1)(n+2)$

Ü16

Zeige: Bei zwei beliebigen natürlichen Zahlen a und b ist (wenigstens) eine der Zahlen a, b, a+b oder a–b durch 3 teilbar.

Ü17

a) Welchen Rest läßt 5^{671} bei Division durch 12?

[Tip: Hierbei kann man ausnutzen, daß gilt: $25 \equiv 1\ (12)$ sowie $1^n = 1$ für alle $n \in \mathbb{N}$.]

b) Welchen Rest läßt 17^{5678} bei Division durch 16?

c) Welchen Rest läßt $38^{38} + 3 \cdot 14^{14}$ bei Division durch 12?

d) Auf welche beiden Ziffern endet 7^{325} im Zehnersystem?

e) Wie lautet die Endziffer der Zahl 2^{3454} im Sechsersystem?

Ü18

a) Bestimme die Lösungsmenge folgender linearer Kongruenzen:

(i) $11x \equiv 31\ (7)$ (ii) $4x + 7 \equiv 6x + 3\ (9)$

b) Bei einer Kontrollkamera muß der Filmwechsel alle 7 Stunden vorgenommen werden. An einem Montag wird um 9 Uhr morgens eine Film eingelegt. Wann wird zum ersten Mal danach der Filmwechsel mittags um 12 Uhr erfolgen?

[Löse mit Hilfe einer linearen Kongruenz.]

c) Eine Bankräuberbande braucht zum Graben eines Tunnels mit allen Pausen etc. 174 Stunden. Nach ausreichenden Beobachtungen haben sie festgestellt, daß man zum Ausplündern der Bank 4 Stunden braucht. Um 6 Uhr wollen sie die Bank verlassen.

Wann müssen sie mit dem Graben beginnen?

Ü19

a) Beweise oder widerlege: $a^2 \equiv b^2\ (m) \;\Rightarrow\; a \equiv b\ (m)$

b) Gilt die Rückrichtung?

Ü20

a) Beweise die in Unterkapitel 6.8 aufgestellte Teilbarkeitsregel für 11.

b) Überprüfe 93 645 255 und 563 200 223 auf Teilbarkeit durch 11 mit Hilfe der unter a) aufgestellten Regel.

Ü21

a) Überprüfe die Richtigkeit der folgender Rechnungen unter Zuhilfenahme der Neunerprobe (mit Begründung):

(i) $237 \cdot 428 = 992724$ (ii) $265524 : 812 = 317$

b) Bestimme die fehlende Ziffer in der Gleichung $4123 \cdot 326 = 1\,34?\,098$.

Ü22
Beweise die Aussage (iv) des Satzes 6.10 mittels Vollständiger Induktion über n.

Zusatzaufgabe 1
Vor langer Zeit gab es einmal einen König, der jedes Jahr an seinem Geburtstag mit einer edlen Geste einigen seiner Gefangenen die Freiheit schenkte. Um jedoch nicht willkürlich diese Gefangenen auswählen zu müssen, fand an jenen Tagen folgendes Ritual statt:
Seine n-vielen Wärter gingen nacheinander und der Reihe nach an den Zellen vorbei. Dabei öffnete der erste Wärter jede Zellentür, der zweite verschloß jede zweite Tür, der dritte änderte den Zustand jeder dritten Zellentür (d.h. offene Türen wurden verschlossen, verschlossene wieder geöffnet) und so fort, bis der n-te Wärter sich schließlich jede n-te Zellentür vornahm.
Denjenigen Gefangenen, deren Zellentür am Ende nicht verschlossen war, erließ der König den Rest ihrer Strafe. Um allen Gefangenen eine gleiche Chance zu bieten, durften diese sich **vor** der ganzen Prozedur eine Zelle aussuchen. Die Frage, die alle Gefangenen also während eines ganzen Jahres beschäftigte, war: Gibt es Zellen, die die Freiheit garantieren?

Versetze Dich einmal in folgende Situation: Du sitzt in der Zelle mit der Nummer a. Im Moment ist der Wärter mit der Nummer b unterwegs. In welchem Fall wird dieser Wärter sich an Deiner Türe zu schaffen machen?

Und weiter: Alle Wärter sind durch. Falls Du frei bist, wie viele Wärter waren dann an Deiner Tür, wie viele, wenn Du ein weiteres Jahr „sitzt“?
Spiele die Prozedur beispielhaft für die ersten zehn Zellen durch (Spezialisieren). Welche Zellen haben die „Tür zur Freiheit“?
Fällt Dir irgend etwas auf?

Versuche nun, ein Kriterium zu formulieren, das die Zelle Nr. a zu einer der begehrten Zellen macht (Generalisieren). Kannst Du nachvollziehbar begründen, warum ausgerechnet diese Zellen am Ende geöffnet sind?

Zusatzaufgabe 2
Eine Bäuerin wird auf dem Weg zum Markt von einem vorbeifahrenden hupenden Lkw derart erschreckt, daß sie ihren Korb mit Eiern fallen läßt. Da kommt Herr König von der Homberg-Monheimer vorbei und beruhigt die völlig aufgelöste Frau: „Den Schaden übernimmt doch die Eiertransportversicherung, die ich ihnen erst gestern verkauft habe! Ich muß lediglich wissen, wie viele Eier zu Bruch gegangen sind.“
„Ich weiß nicht mehr, wie viele Eier ich dabei hatte,“ erwidert die Frau, „ich weiß nur noch, daß beim Zählen zu zweien, zu dreien, zu vieren, zu fünfen und zu sechsen jeweils genau ein Ei übrig blieb und daß ich weniger als hundert Eier bei mir trug.“ „Das reicht leider nicht,“ meint Herr König, „ich muß es genau wissen!“ Darauf die Frau: „Aber Herr König! Das werden Sie sich doch überlegen können?!“
Ist es möglich, die Anzahl der zu Bruch gegangenen Eier eindeutig zu bestimmen?