7. Teile, und beherrsche den Rest

7.1. Division mit Rest

Nicht alle natürlichen Zahlen sind durch 3 teilbar:

Es lässt	17	den Rest	2	$[17 = 5 \cdot 3 + 2]$
	18	geht auf		
	19	lässt Rest	1	
	20	lässt Rest	2	
	21	geht auf		
	22	lässt Rest	1	
	23	lässt Rest	2	
	24	geht auf		
	25	lässt Rest	1	
	26	lässt Rest	2	
	27	geht auf		
	28	lässt Rest	1	

Offenbar geht das periodisch weiter.

Man kann das mit jeder natürlichen Zahl d statt 3 machen.

Wir haben das alle in der Grundschule als „Teilen mit Rest“ gelernt (und meist danach wieder vergessen, weil wir glauben, mit Brüchen und Dezimal-Entwicklungen „besser“ rechnen zu können):

Zu natürlichen Zahlen a, d gibt es stets eine natürliche Zahl q so, dass der *Rest* $r = a - qd$ nicht negativ wird, aber kleiner als d ausfällt. Formaler ausgedrückt:

Zu natürlichen Zahlen a, d gibt es stets genau eine natürliche Zahl q und einen „Rest“ r mit $0 \leq r < d$ so, dass $\quad a = qd + r \quad$ gilt.

Statt „m und n lassen den gleichen Rest bei Division durch d“ sagt man

„m und n sind kongruent modulo d“

und schreibt

$$m \equiv n \pmod{d}.$$

Es gibt ein nützliches Kriterium:

Zwei natürliche Zahlen a, b lassen genau dann den gleichen Rest bei Division durch d, wenn ihre Differenz durch d teilbar ist.

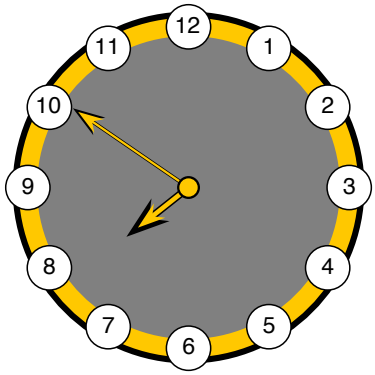
7.2. Ein wohl bekanntes Beispiel

Wie spät ist es in 4 Stunden?

Wie spät in 16 Stunden?

Uhrzeiten werden „modulo 12“
(oder „modulo 24“) angegeben.

Minuten-Angaben scheinen dann „modulo 60“ zu sein ...



Wenn wir zu „6 Uhr“	5	Stunden addieren, erhalten wir	„11 Uhr“,
wenn wir	7	Stunden addieren, erhalten wir	„1 Uhr“.

Was erhalten wir, wenn wir 136 Stunden addieren?

Wir teilen mit Rest: $136 = 11 \cdot 12 + 4$.

Da die Vielfachen von 12 bei Uhrzeiten keine Rolle spielen, ergibt sich:

Wenn wir zu „6 Uhr“	136	Stunden addieren, erhalten wir	„10 Uhr“.

Was erhalten wir, wenn wir 139 Stunden addieren?

Wir teilen wieder mit Rest: $139 = 11 \cdot 12 + 7$.

Mit $6 + 139 \equiv 6 + 7 = 13 \equiv 1 \pmod{12}$ ergibt sich:

Wenn wir zu „6 Uhr“	139	Stunden addieren, erhalten wir	„1 Uhr“.

Die Rollen, die hier (und auch in unserem Kalender, oder bei der Messung von Winkeln) die Zahlen 12 und 60 spielen, scheinen nicht so recht zu unserer ansonsten vom Dezimalsystem geprägten Welt zu passen.

In der Tat sind dies Spuren uralter Zahlsysteme, die bei den Sumerern und Babyloniern im Gebrauch waren. Dass gerade solche Elemente der Kultur — und nicht Schrift oder Musik — über so lange Zeiten überdauern, mag zu denken geben. Es bleibt auf jeden Fall faszinierend, dass sich hier über so große Zeiträume immerhin Kontinuität belegen lässt.

7.3. Abstraktion: Addieren von Resten

Es sei $\{0, 1, 2, \ldots, d-1\}$ die Menge der Reste bei Division durch d. Wir setzen $x \underset{d}{+} y$ fest als den Rest von $x + y$ bei Division durch d. Es gilt also

$$x \underset{d}{+} y \equiv x + y \pmod{d} \qquad \text{und} \qquad 0 \leq x \underset{d}{+} y < d\,.$$

Beispiele: Es ist $2 \underset{3}{+} 2 = 1\,,$ $4 \underset{8}{+} 7 = 3\,,$ $13 \underset{20}{+} 7 = 0\,.$

7.4. Mehr Rechnungen mit Resten

Man kann Reste auch multiplizieren: Wie bei der Addition rechnen wir erst wie gewohnt und reduzieren danach.

Für Reste x, y bei Division durch d setzen wir also $x \underset{d}{\cdot} y$ fest als den Rest von $x \cdot y$ modulo d. Es gilt damit

$$x \underset{d}{\cdot} y \equiv x \cdot y \pmod{d} \qquad \text{und} \qquad 0 \leq x \underset{d}{\cdot} y < d\,.$$

Beispiele: Es ist $2 \underset{3}{\cdot} 2 = 1\,,$ $4 \underset{8}{\cdot} 7 = 4\,,$ $13 \underset{20}{\cdot} 7 = 11\,.$

Entsprechend können wir auch ohne Schwierigkeit Reste potenzieren:

Weil uns die vernünftig lesbaren Symbole langsam ausgehen, schreiben wir aber nur x^y und merken uns im Stillen, dass wir nur den Rest modulo d nehmen wollen ...

Wenn man sicher gehen will, benutzt man die Schreibweise „$x^y \equiv z \pmod{d}$“.

Beispiele: Es ist $2^2 \equiv 1 \pmod{3}\,,$ $3^8 \equiv 6 \pmod{15}\,,$ $4^8 \equiv 1 \pmod{15}\,,$
$3^2 \equiv 1 \pmod{7}\,,$ $4^2 \equiv 0 \pmod{8}\,.$

Anders als bei den natürlichen Zahlen (die man gerade zu diesem Zweck zum Bereich aller ganzen Zahlen erweitern muss) kann man Reste auch hemmungslos und uneingeschränkt subtrahieren:
Es geht hier ja darum, zu gegebenen Resten x, y einen Rest z so zu finden, dass $x \underset{d}{+} z = y$.
Mit anderen Worten: Wir suchen z so, dass

$$x + z \equiv y \pmod{d} \qquad \text{und} \qquad 0 \leq z < d\,.$$

Um uns klar zu machen, dass es diesen Rest z gibt (und auch gleich, dass er eindeutig bestimmt ist), betrachten wir die Folge der Reste

$$x \underset{d}{+} 0\,, \quad x \underset{d}{+} 1\,, \quad x \underset{d}{+} 2\,, \quad \ldots \quad x \underset{d}{+} (d-1)\,.$$

Diese sind paarweise verschieden (weil je zwei von ihnen kleineren Abstand als d von einander haben). Wir erhalten in dieser Folge also d verschiedene Elemente der Menge $\{0, 1, 2, \ldots, d-1\}$ aller Reste modulo d: Das müssen alle sein!

Für den durch Subtraktion erhaltenen Rest werden wir $x \underset{d}{-} y$ schreiben.

7.5. Kompliziertere Rechnungen

Wenn wir nacheinander mehrere Rechenoperationen auf Reste anwenden sollen, ist es manchmal angenehmer, nicht jedesmal zwischendurch zu reduzieren. Allerdings muss man sich klar machen, dass man dann auch am Ende dasselbe Ergebnis erhält.

Beispiel: Für $7 \equiv 1 \pmod 3$ und $14 \equiv 2 \pmod 3$:

$$\begin{aligned} 7 + 14 = 21 &\equiv 0 \equiv 1 + 2 \pmod 3 \\ 7 \cdot 14 = 98 &\equiv 2 \equiv 1 \cdot 2 \pmod 3\,. \end{aligned}$$

Wir können für beliebig große Zahlen aussuchen, ob wir zuerst rechnen und dann modulo d reduzieren, oder umgekehrt. In der Tat:
Aus $a \equiv b \pmod d$ und $x \equiv y \pmod d$ folgt zuerst die Existenz von ganzen (vielleicht negativen) Zahlen m, n mit $b = a + m \cdot d$ und $y = x + n \cdot d$. Jetzt rechnet man

$$\begin{aligned} b + y &= (a + m \cdot d) + (x + n \cdot d) = a + x + (m + n) \cdot d \\ &\equiv a + x \pmod d \\ b \cdot y &= (a + m \cdot d) \cdot (x + n \cdot d) = a \cdot x + (a \cdot n + m \cdot n \cdot d + m \cdot x) \cdot d \\ &\equiv a \cdot x \pmod d\,. \end{aligned}$$

Man kann diese Erkenntnis in expliziten Rechnungen nutzen, aber auch allgemeine Aussagen damit herleiten:

Es gelten die Assoziativ-Gesetze für Addition und Multiplikation von Resten modulo d:
Für alle natürlichen Zahlen x, y, z gilt

$$\left(x \underset{d}{+} y\right) \underset{d}{+} z = x \underset{d}{+} \left(y \underset{d}{+} z\right) \quad \text{und} \quad \left(x \underset{d}{\cdot} y\right) \underset{d}{\cdot} z = x \underset{d}{\cdot} \left(y \underset{d}{\cdot} z\right) .$$

Beispiel: Es gilt $\left(3 \underset{4}{\cdot} 2\right) \underset{4}{\cdot} 2 = 3 \underset{4}{\cdot} \left(2 \underset{4}{\cdot} 2\right) = 3 \underset{4}{\cdot} 0 = 0.$

Es gilt das Distributiv-Gesetz für Reste modulo d:
Für alle natürlichen Zahlen x, y, z gilt

$$\left(x \underset{d}{+} y\right) \underset{d}{\cdot} z = \left(x \underset{d}{\cdot} z\right) \underset{d}{+} \left(y \underset{d}{\cdot} z\right) .$$

Beispiele:

$$\begin{aligned} 3 \underset{9}{\cdot} \left(3 \underset{9}{+} 4\right) &= \left(3 \underset{9}{\cdot} 3\right) \underset{9}{+} \left(3 \underset{9}{\cdot} 4\right) = 0 \underset{9}{+} 3 = 3 \\ \left(3 \underset{9}{\cdot} 2\right) \underset{9}{+} \left(6 \underset{9}{\cdot} 4\right) &= 3 \underset{9}{\cdot} \left(2 \underset{9}{+} \left(2 \underset{9}{\cdot} 4\right)\right) = 3 \underset{9}{\cdot} 10 = 3 \end{aligned}$$

Beispiel: Aus dem Distributiv-Gesetz folgt die „Neunerprobe“:
Eine Zahl ist genau dann durch 9 teilbar, wenn ihre Quersumme (also die Summe ihrer Ziffern) durch 9 teilbar ist.

Sind $z_n, z_{n-1}, z_{n-2}, \ldots, z_2, z_1, z_0$ die Ziffern von z, so gilt ja

$$z = z_0 + z_1 \cdot 10 + z_2 \cdot 10^2 + \cdots + z_{n-2} \cdot 10^{n-2} + z_{n-1} \cdot 10^{n-1} + z_n \cdot 10^n .$$

Wegen $10 \equiv 1 \pmod 9$ gilt auch $10^2 = 10 \cdot 10 \equiv 1 \cdot = 1 \pmod 9$, und man erhält weiter $10^k \equiv 1 \pmod 9$ für jeden Exponenten k. Aus dem Distributiv-Gesetz ergibt sich

$$z \equiv z_0 + z_1 \cdot 1 + z_2 \cdot 1 + \cdots + z_{n-2} \cdot 1 + z_{n-1} \cdot 1 + z_n \cdot 1 \pmod 9 ,$$

also

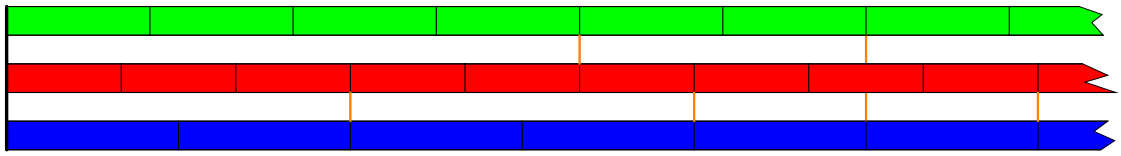
$$z \equiv z_0 + z_1 + z_2 + \cdots + z_{n-2} + z_{n-1} + z_n \pmod 9 .$$

Es ist damit z genau dann durch 9 teilbar (d.h. $z \equiv 0 \pmod 9$), wenn die Summe der Ziffern von z durch 9 teilbar ist.

7.6. Gemeinsame Vielfache und gemeinsame Teiler

Für zwei natürliche Zahlen a, b wird mit $\mathrm{kgV}(a,b)$ das kleinste gemeinsame Vielfache, mit $\mathrm{ggT}(a,b)$ der größte gemeinsame Teiler bezeichnet.

Man sieht hier drei periodische Vorgänge auf parallelen Skalen eingezeichnet, die Perioden sind 5, 4 bzw. 6 Zeiteinheiten. Die Perioden treffen immer bei gemeinsamen Vielfachen zusammen.



Es gilt $a \cdot b = \mathrm{kgV}(a,b) \cdot \mathrm{ggT}(a,b)$, wie man leicht durch Zerlegung in Primfaktoren sieht.

Man nennt a, b teilerfremd, wenn $\mathrm{ggT}(a,b) = 1$; dann gilt natürlich $\mathrm{kgV}(a,b) = a \cdot b$.

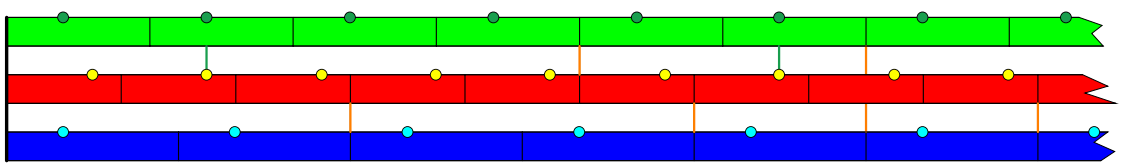
Beispiele: $\mathrm{ggT}(2,3) = 1$, $\mathrm{ggT}(2,6) = 2$, $\mathrm{ggT}(9,12) = 3$,
$\mathrm{kgV}(2,3) = 6$, $\mathrm{kgV}(2,6) = 6$, $\mathrm{kgV}(9,12) = 36$.

Wir betrachten zwei periodische Vorgänge, mit Perioden a bzw. b.
Der Einfachheit bezeichnen wir die periodisch durchlaufenen Zustände mit Zahlen, also etwa $0, 1, 2, \ldots, a-2, a-1, 0, 1, 2, \ldots$
Mit anderen Worten: Nach der Zeit t ist der erste Vorgang in dem Zustand, der sich als Rest von t modulo a ergibt, der zweite Vorgang ist dann in dem Zustand, den man als Rest von t modulo b erhält.

Die beiden Vorgänge erreichen nach $\mathrm{kgV}(a,b)$ Zeiteinheiten wieder das gleichen Paar von Zuständen.

7.7. Der Chinesische Restsatz

Wir wählen jetzt für beide Systeme je einen Zustand aus und fragen uns, ob jemals beide Zustände simultan angenommen werden.



Beispiel: Eine Mensa wechselt täglich einerseits zwischen 5 Fleischgerichten, andererseits zwischen 4 vegetarischen Gerichten.
Der Student F.R. Wöhnt mag weder das Fleischgericht 2 noch das vegetarische Gericht 3. Kommt es vor, dass er auf den Schnell-Imbiss ausweichen muss?

Offenbar kommt das immer wieder vor.

? Was passiert dagegen, wenn die Mensa durch eine Reihe von 6 (statt 5) Fleischgerichten wechselt? **?**

In der obigen Darstellung heißt das, die grüne durch die blaue Zeit-Leiste zu ersetzen.

Es ist im dargestellten Bereich noch nicht zu sehen, ob irgendwann einmal gleichzeitig das rote System im Zustand 3 und das blaue im Zustand 2 sein wird.

Eine Betrachtung geeigneter Reste zeigt uns aber die Wahrheit:

Das rote System ist im Zustand 3 genau zu den Zeiten der Form $3 + n \cdot 4$.
Das sind auf jeden Fall ungerade Zeiten.
Dagegen ist das blaue System im Zustand 2 zu den Zeiten der Form $2 + m \cdot 6$
— und die sind alle gerade.

Es kommt also nie vor, dass die Systeme gleichzeitig in den fraglichen Zuständen sind!

Analoge Fragestellungen ergeben sich, wenn man die (näherungsweise periodischen) Umlaufbahnen von Planeten um die Sonne (oder von Monden um Planeten) betrachtet und nach bestimmten, interssanten Konstellationen fragt — besonders spektakulär sind hier Sonnen- oder Mondfinsternisse, aber auch die Tatsache, dass sich Mars und Erde im Jahr 2003 besonders nahe kamen (und dass dies so schnell nicht wieder geschieht, weil die Bahn-Perioden ein großes kleinstes gemeinsames Vielfaches haben).

Wir können diese Betrachtungen abstrahieren:

? Gegeben seien natürliche Zahlen a, b, r, s.
Gibt es dann eine natürliche Zahl t derart, dass sowohl $t \equiv r \pmod{a}$ als auch $t \equiv s \pmod{b}$ gilt? **?**

Eine positive Antwort gibt das folgende Ergebnis:

Chinesischer Restsatz:
Wenn a und b teilerfremd sind, gibt es zu jedem beliebigen Paar (r, s) natürlicher Zahlen auch (wenigstens) eine natürliche Zahl t derart, dass sowohl

$$t \equiv r \pmod{a} \quad \text{als auch} \quad t \equiv s \pmod{b} \quad \text{gilt.}$$

Zum Beweis macht man sich zuerst klar, dass es genügt, unter den Zahlen zwischen 0 und $\mathrm{kgV}(a,b)$ zu suchen: Danach wiederholt sich ohnehin alles immer wieder.

Jetzt wollen wir begründen, dass in diesem Bereich (also für $0 \leq t < \mathrm{kgV}(a,b)$) immer wieder verschiedene Konstellationen eintreten: Wenn für t und s sowohl $s \equiv t \pmod{a}$ als auch $s \equiv t \pmod{b}$ gilt, gibt es ganze Zahlen m, n mit $t = s+m\cdot a$ und $t = s+n\cdot b$.

Das bedeutet, dass der Abstand $|t-s| = |m| \cdot a = |n| \cdot b$ ein gemeinsames Vielfaches von a und b und damit ein Vielfaches von $\mathrm{kgV}(a,b)$ ist. Wenn der Abstand kleiner als $\mathrm{kgV}(a,b)$ sein soll, geht das nur mit $|t-s| = 0$ und damit $s = t$.

Diese Argumentation zeigt, dass sich $\mathrm{kgV}(a,b)$ viele verschiedene Paare von Resten modulo a bzw. modulo b ergeben. Unsere Annahme, dass a und b teilerfremd seien, impliziert aber $\mathrm{kgV}(a,b) = a \cdot b$, und wir erhalten alle Paare von Resten.

Man macht sich leicht durch eine Teilbarkeits-Überlegung klar, dass es für nicht teilerfremde a, b auch stets wenigstens ein Paar von Zuständen (r, s) gibt, das nicht gleichzeitig angenommen wird.

7.8. Dividieren?

Für Reste gehen Divisionen öfter auf als für natürliche Zahlen.

Beispiel: Gesucht ist ein Rest x modulo 10 so, dass $7 \underset{10}{\cdot} x = 3$.

Lösung: $x = 9$ [wegen $7 \cdot 9 = 63 \equiv 3 \pmod{10}$].

Wenn a und n teilerfremd sind, kann man modulo n durch a dividieren. In der Tat entnimmt man dem Chinesischen Restsatz, dass es ein e mit $a \underset{n}{\cdot} e = 1$ gibt:
Man suche t so, dass $t \equiv 1 \pmod{n}$ und $t \equiv 0 \pmod{a}$. Jetzt setzt man $e := t/a$.

Vorsicht: manche Divisions-Aufgaben für Reste haben mehrere Lösungen!

Beispiel: Gesucht ist ein Rest x modulo 10 so, dass $6 \underset{10}{\cdot} x = 2$.

1. Lösung: $x = 2$ [wegen $6 \cdot 2 = 12 \equiv 2 \pmod{10}$].

2. Lösung: $x = 7$ [wegen $6 \cdot 7 = 42 \equiv 2 \pmod{10}$].

Genauso schlimm: Aus $x \underset{d}{\cdot} y = 0$ folgt nicht unbedingt, dass einer der Faktoren x, y gleich 0 sein muss:

Beispiele: $2 \underset{10}{\cdot} 5 = 0$, $4 \underset{10}{\cdot} 5 = 0$, $3 \underset{6}{\cdot} 4 = 0$.

Zu einem Rest a modulo d gibt es genau dann einen von 0 verschiedenen Rest b mit $a \underset{d}{\cdot} b = 0$, wenn a und d nicht teilerfremd sind.

In der Tat: Wenn es so einen Rest gibt, muss $a \cdot b$ durch d teilbar sein. Dann ist $\mathrm{kgV}(a, d)$ ein Teiler von $a \cdot b$, und damit sicher kleiner als $a \cdot d$. Dies liefert $\mathrm{ggT}(a, d) = \frac{a \cdot d}{\mathrm{kgV}(a,d)} > 1$, womit a und d als nicht teilerfremd erkannt sind.

Umgekehrt: Sind a und d nicht teilerfremd, so wählen wir einen gemeinsamen Teiler t mit $1 < t < a$, setzen $b := \frac{d}{t}$ und erhalten $\quad a \cdot b \equiv 0 \pmod{d}$.