# 7 Zahlentheorie

Die Grundmenge in diesem Abschnitt ist $\mathbb{Z}$, die Menge der ganzen Zahlen.

## 7.1 Teilbarkeit

Eine Zahl $n$ ist durch eine Zahl $m > 0$ teilbar, wenn die Division $n/m$ aufgeht, d.h eine ganze Zahl ergibt, sagen wir $t$. Es gilt dann also $n/m = t$. Multiplizieren wir beide Seiten dieser Gleichung mit $m$, so erhalten wir die gleichwertige Beziehung $n = tm$. Dies ist die Grundlage für folgende Definition.

**Definition 7.1** *Für zwei Zahlen* $m, n \in \mathbb{Z}$ *mit* $m > 0$ *ist* $m$ Teiler von $n$, *falls es ein* $t \in \mathbb{Z}$ *gibt, so dass* $n = tm$. *Als Kurzschreibweise verwenden wir* $m \backslash n$, *lies:* $m$ *teilt* $n$. *Die Menge aller Teiler von* $n$ *ist* $T_n = \{k > 0 \mid k \backslash n\}$.

Zum Beispiel gilt $2\backslash 6$, da $6 = 3 \cdot 2$, aber $2 \not\backslash 7$, da $7 \neq t \cdot 2$ für alle $t \in \mathbb{Z}$. Für jedes $n$ gilt $1\backslash n$. Ist $n > 0$, so gilt auch $n\backslash n$.

Ist $m$ kein Teiler von $n$, so bleibt bei der Division ein Rest. Wir können dann schreiben

$$n = tm + r. \tag{7.1}$$

Dabei wählen wir $t$ maximal, so dass $tm \leq n$ ist, also $t = \lfloor n/m \rfloor$. Eingesetzt in Gleichung (7.1) erhalten wir für $r$

$$r = n - \left\lfloor \frac{n}{m} \right\rfloor m$$

Da $\lfloor \frac{n}{m} \rfloor m \leq n$, ist $r \geq 0$. Andererseits ist $r < m$, da $\lfloor \frac{n}{m} \rfloor$ der größte Faktor $t$ ist, so dass $tm \leq n$. Folglich gilt $r \in \{0, 1, \ldots m-1\}$. Diese Menge bezeichnen wir mit $\mathbb{Z}_m$,

$$Z_m = \{0, 1, \ldots m-1\}.$$

Bei der ganzahligen Division von $n$ durch $m$ bezeichnet man $m$ als den *Modul* und den Rest $r$ als $n$ *modulo* $m$. In Kurzschreibweise

$$r = n \bmod m.$$

Der Rest $r$ ist also der Abstand von $n$ zum nächst kleineren Vielfachen von $m$. Zum Beispiel haben wir für $m = 3$ und $n = 5$ den Rest

$$r = 5 \bmod 3 = 5 - \left\lfloor \frac{5}{3} \right\rfloor \cdot 3 = 5 - 1 \cdot 3 = 2.$$

Die Zahl $n - r$ muss dann durch $m$ teilbar sein: $5 - 2 = 3$ und $\frac{3}{3} = 1$. Damit haben wir die Darstellung $5 = 1 \cdot 3 + 2$. Dieselbe Rechnung mit $n = -5$ ergibt

$$r = -5 \bmod 3 = -5 - \left\lfloor \frac{-5}{3} \right\rfloor \cdot 3 = -5 + 2 \cdot 3 = 1.$$

Dann ist wieder $n - r = -6$ durch $m$ teilbar: $\frac{-6}{3} = -2$. Dies ergibt die Darstellung $-5 = -2 \cdot 3 + 1$. Abbildung 1 illustriert die Situation.

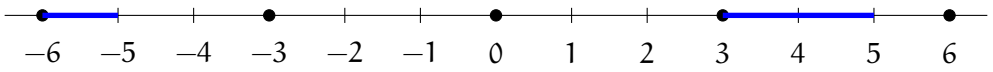


Abbildung 1: *Ein Zahlenstrahl, auf dem die Vielfachen von* $m = 3$ *mit Punkten markiert sind. Der Rest einer Zahl* $n$ *modulo* $m$ *ist der Abstand zum nächst kleineren Vielfachen von* $m$*. Für* $n = 5$ *ist dies durch die blau gezeichnete Strecke von* 5 *nach* 3 *hervor gehoben. Diese hat die Länge* 2*. Für* $n = -5$ *ist dies die Strecke bis* $-6$ *mit der Länge* 1*.*

Eine Zahl $n$ kann, für festes $m$, auf viele Arten in der Form $n = tm + r$ geschrieben werden. Zum Beispiel ist für $n = 11$ und $m = 3$

$$11 = 1 \cdot 3 + 8 = 2 \cdot 3 + 5 = 3 \cdot 3 + 2 = 4 \cdot 3 - 1.$$

Beschränkt man $r$ auf den Bereich $\{0, 1, \ldots, m-1\}$, dann gibt es nur noch eine Darstellung in der Form $n = tm + r$.

**Theorem 7.2** *Sei* $n, m \in \mathbb{Z}$ *und* $m > 0$*. Die Darstellung* $n = tm + r$ *mit* $0 \leq r < m$ *ist eindeutig.*

**Beweis.** Angenommen es gäbe außer der Darstellung $n = tm + r$ noch eine weitere der Form $n = t'm + r'$, mit $0 \leq r, r' < m$. Dann gilt $tm + r = t'm + r'$ und folglich

$$(t - t')\, m = r' - r. \tag{7.2}$$

Nach Gleichung (7.2) ist $r' - r$ ein Vielfaches von $m$. Da $0 \leq r, r' < m$, liegt die Differenz $r' - r$ im Bereich $\{-(m-1), \ldots, -1, 0, 1, \ldots, m-1\}$. Das einzige Vielfache von $m$ im diesem Bereich ist 0. Folglich gilt $t - t' = 0$ und somit $t = t'$. Damit folgt aus Gleichung (7.2) $r' - r = 0$, also $r = r'$. D.h. die beiden Darstellungen von $n$ sind gleich. □

Als nächstes betrachten wir die gemeinsamen Teiler zweier Zahlen $m$ und $n$. Diese fassen wir in der Menge $T_{m,n}$ zusammen, d.h. wir definieren

$$T_{m,n} = T_m \cap T_n.$$

**Definition 7.3** *Der* größte gemeinsame Teiler von $m$ und $n$*, kurz* $\mathrm{ggT}(m, n)$*, ist die größte Zahl in* $T_{m,n}$*, also* $\max T_{m,n}$*. Anders ausgedrückt,*

$$\mathrm{ggT}(m, n) = \max\{\, k \mid k \backslash m \text{ und } k \backslash n \,\}.$$

*Das* kleinste gemeinsame Vielfache von $n, m > 0$ *ist die kleinste Zahl die von* $m$ *und* $n$ *geteilt wird,*

$$\mathrm{kgV}(m, n) = \min\{\, k > 0 \mid m \backslash k \text{ und } n \backslash k \,\}.$$

Beispielsweise ist $T_{12} = \{1, 2, 3, 4, 6, 12\}$ und $T_{18} = \{1, 2, 3, 6, 9, 18\}$. Die gemeinsamen Teiler von 12 und 18 sind in der Menge $T_{12,18} = \{1, 2, 3, 6\}$. Der größte gemeinsame Teiler von 12 und 18 ist der größte Wert in $T_{12,18}$, also 6. Das kleinste gemeinsame Vielfache von 12 und 18 ist 36.

Wir sind an einem möglichst effizienten Verfahren zur Berechnung des größten gemeinsamen Teilers zweier Zahlen interessiert. Dazu zeigen wir zunächst einige Eigenschaften der Teilermengen.

Die gemeinsamen Teiler zweier Zahlen $m$ und $n$ haben die Eigenschaft, dass sie auch alle Linearkombinationen von $m$ und $n$ teilen.

**Lemma 7.4** *Für alle* $a, b \in \mathbb{Z}$ *ist* $T_{m,n} \subseteq T_{am+bn}$.

**Beweis.** Sei $k \in T_{m,n}$ ein beliebiger Teiler von $m$ und $n$. Es gibt also $s, t \in \mathbb{Z}$, so dass $m = sk$ und $n = tk$. Dann gilt

$$am + bn = ask + btk = (as + bt)k,$$

und folglich $k \backslash am + bn$. D.h. $k \in T_{am+bn}$. □

Speziell gilt also für größten gemeinsamen Teiler und für alle $a, b \in \mathbb{Z}$

$$ggT(m, n) \backslash (am + bn).$$

Als Beispiel betrachten wir $m = 12$ und $n = 18$. Für $a = -1$ und $b = 2$ ist $am + bn = -1 \cdot 12 + 2 \cdot 18 = 24$ und es gilt

$$T_{12,18} = \{1, 2, 3, 6\} \subseteq T_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}.$$

Wir sehen, dass die Teilermenge $T_{am+bn}$ im Allgemeinen mehr Zahlen enthält als $T_{m,n}$. In unserem Beispiel ist $4 \in T_{24}$, aber $4 \notin T_{12,18}$.

Unser Ziel ist es, mindestens eine der Zahlen $m$ und $n$ zu verkleinern, und zwar so, dass die gemeinsamen Teiler $T_{m,n}$ unverändert bleiben. Das funktioniert wenn wir nur Linearkombinationen $am + bn$ betrachten bei denen $a = 1$ oder $b = 1$ ist, also Teilermengen der Form $T_{m,am+n}$ wenn wir $b = 1$ setzen. Zum Beispiel für $a = 2$ ist $am + n = 2 \cdot 12 + 18 = 42$ und $T_{12,42} = \{1, 2, 3, 6\} = T_{12,18}$. Wenn wir $a$ positiv wählen, dann vergrößert sich die Zahl. Aber wir können $a$ auch negativ wählen. Dann bekommen wir kleinere Zahlen.

**Folgerung 7.5** *Für alle* $a \in \mathbb{Z}$ *ist* $T_{m,n} = T_{m,n-am}$.

**Beweis.** Wir zeigen zuerst $T_{m,n} \subseteq T_{m,n-am} = T_m \cap T_{n-am}$. Natürlich gilt $T_{m,n} = T_m \cap T_n \subseteq T_m$. Die Inklusion $T_{m,n} \subseteq T_{n-am}$ folgt nach Lemma 7.4, wenn man dort für $b = 1$ einsetzt und $a$ durch $-a$ ersetzt.

Wir betrachten die umgekehrte Inklusion $T_{m,n-am} \subseteq T_{m,n}$. Trivial ist wieder $T_{m,n-am} \subseteq T_m$. Die Inklusion $T_{m,n-am} \subseteq T_n$ folgt ebenfalls nach Lemma 7.4, da sich $n$ wie folgt als eine Linearkombination von $m$ und $n - am$ darstellen lässt: $n = am + (n - am)$. □

Wählt man in Folgerung 7.5 $a \geq 1$, so verkleinert sich das Zahlenpaar $(m, n)$ zu $(m, n - am)$, trotzdem bleiben die gemeinsamen Teiler dieselben. Je kleiner $n-am$ ist, desto einfacher wird es, den größten gemeinsamen Teiler zu bestimmen. Wir wählen folglich $a$ maximal, so dass $n - am \geq 0$ ist. Das gilt offensichtlich für $a = \lfloor \frac{n}{m} \rfloor$. Dann haben wir

$$n - am = n - \left\lfloor \frac{n}{m} \right\rfloor m = n \bmod m.$$

**Folgerung 7.6** *Für* $m > 0$ *gilt* $T_{m,n} = T_{m,n \bmod m}$.

Ein Spezialfall ist, wenn die Division aufgeht und $n \bmod m = 0$ ist. Dann erhalten wir $T_{m,n} = T_{m,0}$. Da jede positive Zahl Teiler von 0 ist, gilt $T_0 = \mathbb{N}$ und somit $T_{m,0} = T_m \cap \mathbb{N} = T_m$.

Das folgende Beispiel zeigt, wie man durch mehrfaches Anwenden von Folgerung 7.6 alle gemeinsamen Teiler zweier Zahlen bestimmen kann.

$$\begin{aligned} T_{12,18} &= T_{12,6}, && \text{da } 18 \bmod 12 = 6 \\ &= T_{0,6}, && \text{da } 12 \bmod 6 = 0 \\ &= T_6. \end{aligned}$$

D.h. die gemeinsamen Teiler von 12 und 18 sind genau die Teiler von 6. Insbesondere ist also der größte gemeinsame Teiler von 12 und 18 der größte Teiler von 6, und somit 6.

Das Ganze funktioniert auch allgemein. Dies ist die Vorgehensweise des *euklidische Algorithmus*: Ausgehend von $m$ und $n$ ersetzt man die jeweils größere der beiden Zahlen, sagen wir $n$, durch $r = n \bmod m$ und wiederholt diesen Schritt mit $r$ und $m$. Nach Folgerung 7.5 bleibt die gemeinsame Teilermenge gleich. Der Prozess stoppt wenn die Division ohne Rest aufgeht. Da die Zahlen immer kleiner werden ist dies spätestens dann der Fall, wenn die kleinere Zahl 1 ist. Sind 0 und $d$ die Zahlen in diesem letzten Schritt, dann ist $T_{m,n} = T_d$ und damit insbesondere $d = \mathrm{ggT}(m, n)$.

Dies ist ein interessantes Ergebnis. Am Anfang war natürlich klar, dass jeder Teiler von $n$ und $m$ kleiner oder gleich $\mathrm{ggT}(m, n)$ ist. Jetzt wissen wir, dass jeder Teiler von $n$ und $m$ sogar ein Teiler von $\mathrm{ggT}(m, n)$ ist.

**Folgerung 7.7** $T_{m,n} = T_{\mathrm{ggT}(m,n)}$. *Jeder gemeinsame Teiler von* $n$ *und* $m$ *teilt folglich* $\mathrm{ggT}(m, n)$.

Der *euklidische Algorithmus* geht genau wie oben beschrieben vor, um den größten gemeinsamen Teiler von $m$ und $n$ zu bestimmen. Die einfachste Formulierung ist als rekursive Prozedur. Sei $0 \leq m < n$.

EUKLID$(m, n)$
1 **if** $m = 0$ **then return** $n$
2 **else return** EUKLID$(n \bmod m, m)$

Um die Laufzeit des euklidischen Algorithmus' zu untersuchen, müssen wir die Anzahl der rekursiven Aufrufe in Zeile 2 bestimmen. Betrachten wir dazu das Zahlenpaar $(m, n)$ mit $m < n$ in einer Rekursionsstufe und das darauf folgende Paar $(r, m)$ in der nächsten Stufe, also mit $r = n \bmod m$. Es gilt $0 \leq r < m$ da $r$ ein Rest modulo $m$ ist. Die Zahl $n$ lässt sich schreiben als $n = tm + r$ für ein $t \in \mathbb{Z}$. Da wir $n > m$ voraussetzen ist $t \geq 1$. Folglich haben wir

$$n = tm + r \geq m + r > r + r = 2r,$$

und damit $r < n/2$. Also ist $r$ weniger als halb so groß wie $n$.

Das wiederholt sich wenn wir nun die gleiche Betrachtung ausgehend vom Paar $(r, m)$ machen. D.h. dass sich die Zahlen die der euklidischen Algorithmus durchläuft alle zwei Schritte mehr als halbieren.

Halbiert man fortgesetzt eine Zahl $n$, so landet man in $\log n$ Schritten bei 1. Dies passiert hier bei jedem 2. Schritt. Wir fassen zusammen.

**Theorem 7.8** *Sei* $0 \leq m < n$. EUKLID$(m, n)$ *macht höchstens* $2\lceil \log n \rceil$ *rekursive Aufrufe.*

Die Laufzeit ist folglich linear in der Länge der Eingabe wenn man den Aufwand für eine modulo-Operation als konstant ansetzt. Wenn die Zahlen allerdings sehr groß sind, sollte man auch den Aufwand für die Arithmetik genauer berücksichtigen. Die Schulmethoden für Multiplikation und Division haben quadratischen Aufwand in der Anzahl der Stellen der Zahlen, d.h. $O(\log^2 n)$. Die Laufzeit von EUKLID$(m, n)$, die sogenannte *Bit-Komplexität*, ist also $O(\log^3 n)$. Damit gehört der euklidische Algorithmus zu den effizientesten zahlentheoretischen Algorithmen.

Der euklidische Algorithmus wird sehr häufig benützt, meistens als Teil in einer anderen Berechnung. Deswegen ist man an einer möglichst effizienten Implementierung interessiert. Eine rekursive Formulierung, wie sie oben angegeben ist, erzeugt auf einem Rechner einen gewissen zusätzlichen Verwaltungsaufwand, der natürlich Zeit kostet. Wenn man also ein Verfahren auch halbwegs elegant iterativ formulieren kann, dann sollte dies in der Regel zu einer effizienteren Implementierung führen. Im Fall des euklidischen Algorithmus ist dies recht einfach:

EUKLID-ITERATIV$(m, n)$

```
1  while m > 0 do
2      r ← n mod m
3      n ← m
4      m ← r
5  return n
```

Das *Lemma von Bézout* beschreibt eine weitere interessante Eigenschaft des größten gemeinsamen Teilers von $m$ und $n$: Er lässt sich als Linearkombination von $m$ und $n$ darstellen.

**Lemma 7.9 (Bézout)** *Es gibt* $m', n' \in \mathbb{Z}$, *so dass* $m'm + n'n = \mathrm{ggT}(m, n)$.

**Beweis.** Wir führen eine Induktion über die Zahlenfolge des euklidischen Algorithmus', und zwar vom Ende her. Der Induktionsanfang ist der Rekursionsabbruch im euklidischen Algorithmus, d.h es ist $n > m = 0$. Wir setzen $m' = 0$ und $n' = 1$. Dann gilt

$$m'm + n'n = 0 \cdot 0 + 1 \cdot n = n = \mathrm{ggT}(0, n) = \mathrm{ggT}(m, n).$$

Für den Induktionsschritt nehmen wir an, die Behauptung gilt für $m$ und $r = n \bmod m$. D.h. es gibt $r'', m'' \in \mathbb{Z}$, so dass

$$r''r + m''m = \mathrm{ggT}(r, m). \tag{7.3}$$

Wir zeigen die Behauptung für $m$ und $n$. Nach Folgerung 7.6 gilt $\mathrm{ggT}(r, m) = \mathrm{ggT}(m, n)$. Für $r$ gilt

$$r = n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor m.$$

Eingesetzt in Gleichung (7.3) erhalten wir

$$r'' \left( n - \left\lfloor \frac{n}{m} \right\rfloor m \right) + m''m = \mathrm{ggT}(m, n).$$

Wenn wir in dieser Gleichung ausmultiplizieren und die Glieder umordnen, bekommen wir

$$\left( m'' - r'' \left\lfloor \frac{n}{m} \right\rfloor \right) m + r''n = \mathrm{ggT}(m, n).$$

D.h. mit

$$\begin{aligned} m' &= m'' - r'' \left\lfloor \frac{n}{m} \right\rfloor \\ n' &= r'' \end{aligned}$$

erhalten wir die gewünschte Darstellung. □

Wir erweitern den euklidischen Algorithmus gemäß den obigen Gleichungen, so dass auch die Werte $m'$ und $n'$ berechnet werden.

ERWEITERTER-EUKLID$(m, n)$
1 **if** $m = 0$ **then return** $(n, 0, 1)$
2 **else**
3 $\quad (d, r'', m'') \leftarrow$ ERWEITERTER-EUKLID$(n \bmod m, m)$
4 $\quad m' \leftarrow m'' - r'' \lfloor \frac{n}{m} \rfloor$
5 $\quad n' \leftarrow r''$
6 $\quad$ **return** $(d, m', n')$

Die Anzahl der rekursiven Aufrufe ist dieselbe wie bei EUKLID da je Rekursionsstufe nur die beiden Anweisungen in Zeile 4 und 5 hinzu kommen.

Der erweiterte euklidische Algorithmus liefert eine schöne Charakterisierung des größten gemeinsamen Teilers: Betrachten wir die Menge aller Linearkombinationen von $m$ und $n$,

$$L_{m,n} = \{ am + bn \mid a, b \in \mathbb{Z} \}.$$

Nach Lemma 7.4 teilt $\mathrm{ggT}(m, n)$ jede Zahl in $L_{m,n}$. D.h. insbesondere, dass $\mathrm{ggT}(m, n)$ kleiner oder gleich jeder positiven Zahl in $L_{m,n}$ ist. Andererseits wissen wir von Lemma 7.9, dass $\mathrm{ggT}(m, n) \in L_{m,n}$. Als Konsequenz erhalten wir, dass $\mathrm{ggT}(m, n)$ die kleinste positive Zahl in $L_{m,n}$ ist. Mit $L^+_{m,n}$ bezeichnen wir die positiven Elemente in $L_{m,n}$, also $L^+_{m,n} = \{ d \in L_{m,n} \mid d \geq 1 \}$.

**Folgerung 7.10** $\mathrm{ggT}(m, n) = \min L^+_{m,n}$.

Da $L^+_{m,n}$ nur positive Zahlen enthält, ist 1 die kleinst mögliche Zahl in $L^+_{m,n}$. Wenn $1 \in L^+_{m,n}$ ist, dann muss also nach Folgerung 7.10 $\mathrm{ggT}(m, n) = 1$ sein.

**Folgerung 7.11** $\mathrm{ggT}(m, n) = 1 \iff \exists m', n' \in \mathbb{Z} \quad m'm + n'n = 1$.

Der größte gemeinsame Teiler ist als Maximum der Menge $T_{m,n}$ definiert. Folgerung 7.10 beinhaltet also eine Extrem-Gleichung der Art: das Maximum einer Menge ist gleich dem Minimum einer anderen Menge.

$$\max T_{m,n} = \min L^+_{m,n}.$$

Folglich ist $\mathrm{ggT}(m,n)$ das einzige Element im Schnitt der beiden Mengen,

$$T_{m,n} \cap L^+_{m,n} = \{\mathrm{ggT}(m,n)\}.$$

Solche Beziehungen erweisen sich oft als sehr nützlich wie beispielsweise folgende Anwendung zeigt.

Der erweiterte euklidische Algorithmus hat den großen Vorteil, dass er *selbstbestätigend* ist, da er seinen eigenen Korrektheitsbeweis mitliefert. Misstraut man nämlich der Ausgabe $(d,m',n')$ einer Implementierung von ERWEITERTER-EUKLID$(m,n)$, da einem vielleicht der Wert $d$ zu klein vorkommt, dann genügt es, die folgenden beiden Bedingungen nachzuprüfen:

(i) $d \backslash m$ und $d \backslash n$,

(ii) $m'm + n'n = d$.

Aus Bedingung (i) folgt nämlich $d \in T_{m,n}$, und aus Bedingung (ii) folgt $d \in L^+_{m,n}$. Nach unserer obigen Überlegung kann dies nur für $d = \mathrm{ggT}(m,n)$ gelten. Nur das richtige Ergebnis besteht also diesen Test.

## 7.2 Primzahlen

Jede natürliche Zahl $n$ hat mindestens die Teiler 1 und $n$. Dies sind die *trivialen Teiler*. Hat eine Zahl keine weiteren Teiler, so nennen wir sie Primzahl.

**Definition 7.12** *Eine natürliche Zahl* $p$ *heißt* Primzahl, *wenn sie genau zwei Teiler hat.*

Die kleinste Zahl, die diese Bedingung erfüllt ist 2. Weitere Primzahlen sind 3, 5, 7, 11, 13, 17, 19, ....

Unter einem *Primzahltest* versteht man einen Algorithmus, der für eine gegebene Zahl $n$ herausfindet, ob $n$ prim ist. Dazu kann man der Reihe nach die Zahlen $k = 2,3,4,\ldots$ durchgehen, und jeweils prüfen, ob $k$ ein Teiler von $n$ ist. Sicherlich genügt es dabei Zahlen $k \leq n$ zu betrachten. Allerdings ist $k = n$ ein trivialer Teiler, der für die Primzahleigenschaft uninteressant ist. Der nächst kleinere mögliche Teiler ist dann $n/2$. Es genügt also, Werte $k$ mit $k \leq n/2$ zu betrachten. Wenn $n/2$ Teiler ist, heißt das, das $n$ gerade ist:

$$n = 2 \cdot \frac{n}{2}.$$

In diesem Fall hätten wir aber bereits am Anfang, für $k = 2$ gemerkt, dass 2 ein Teiler von $n$ ist. Von daher brauchen wir auch nicht bis $n/2$ zu gehen. Der nächst kleinere mögliche Teiler nach $n/2$ ist $n/3$. Aber hier gilt das Gleiche: Wenn $n/3$ Teiler von $n$ ist, dann auch 3,

$$n = 3 \cdot \frac{n}{3},$$

und das hätten wir ebenfalls früher gemerkt, für $k = 3$. Allgemein gilt: Ist $n/k$ Teiler von $n$, dann auch $k$,

$$n = k \cdot \frac{n}{k}.$$

Solange $k \leq \frac{n}{k}$ gilt, stoßen wir zuerst auf $k$ und müssen folglich $n/k$ nicht mehr betrachten. Es gilt

$$k \leq \frac{n}{k} \iff k^2 \leq n \iff k \leq \sqrt{n}.$$

Es genügt folglich, die Teiler von $n$ im Bereich $2, 3, \ldots, \lfloor\sqrt{n}\rfloor$ zu suchen.

Das *Sieb des Eratosthenes* geht nach dieser Methode vor, spart sich dabei aber noch weitere Divisionen ein. Am Anfang testen wir, ob $n$ gerade ist, also ob 2 ein Teiler von $n$ ist. Wenn wir dabei feststellen, dass $n$ ungerade ist, dann kann keine gerade Zahl Teiler von $n$ sein. Der Test für alle Vielfachen von 2 erübrigt sich also, die Zahlen $4, 6, 8, \ldots$ müssen wir gar nicht mehr testen sondern können sie direkt *aussieben*. Das Gleiche gilt für den nächsten Wert, $k = 3$. Ist $n$ nicht durch 3 teilbar, dann sind auch alle Vielfachen von 3 keine Teiler von $n$. Wir können also $6, 9, 12, \ldots$ aussieben. Als nächstes käme eigentlich $k = 4$. Aber 4 ist schon ausgesiebt worden. Die nächste Zahl, die noch nicht ausgesiebt wurde ist 5. Wir fahren also analog mit 5 fort, usw.

Wir formulieren den Algorithmus als Pseudocode. Die Eingabe ist eine Zahl $n$ und die Ausgabe eine Zahl $k$. Ist $k \geq 2$, dann ist $k$ ein Teiler von $n$. Andernfalls ist $k = 0$. In diesem Fall ist $n$ Primzahl. Der Algorithmus benützt für den Siebmechanismus ein boolesches Array prim$[2..\lfloor\sqrt{n}\rfloor]$. Anfangs ist prim[k] true für alle $k$. Für die ausgesiebten Zahlen $k$ wird dann prim[k] auf false gesetzt. Am Ende ist prim[k] true $\iff$ $k$ prim.

```
SIEB-DES-ERATOSTHENES (n)
 1  if 2\n then return 2
 2  prim[2] ← true
 3  for k ← 3 to ⌊√n⌋ do prim[k] ← [k ungerade]
 4  for k ← 3 to ⌊√n⌋ step 2 do
 5      if prim[k] then
 6          if k\n then return k   (* k ist Fakor von n *)
 7          j ← k²
 8          while j ≤ ⌊√n⌋ do
 9              prim[j] ← false
10              j ← j + 2k
11  return 0   (* n ist Primzahl *)
```

Zeile 1 bis 3 in SIEB-DES-ERATOSTHENES testen, ob $n$ ungerade ist und initialisieren das array prim. In Zeile 3 wird dabei prim[k] für alle ungeraden k's auf true gesetzt, und für alle geraden k's auf false. Damit sind alle geraden Zahlen bereits ausgesiebt, mit Ausnahme der Primzahl 2. Die for-Schleife von Zeile 4 bis 10 betrachtet die restlichen Zahlen ab $k = 3$. Die Schleife erhöht $k$ in 2er-Schritten, so dass $k$ nur noch die ungeraden Werte durchläuft. Wenn prim[k] true ist, wurde $k$ noch nicht ausgesiebt. Da die Vielfachen aller Zahlen $< k$ bereits ausgesiebt sind ist $k$ folglich prim. In Zeile 6 wird getestet, ob $k$ Teiler von $n$ ist. Andernfalls werden die Vielfachen von $k$ ausgesiebt. Es genügt dabei mit $k^2$ zu beginnen,

da die Werte $ik$ für $i < k$ bereits früher als die Vielfachen von $i$ ausgesiebt wurden. Die while-Schleife von Zeile 8 bis 10 setzt die Vielfachen prim[j] auf false und erhöht j. Dabei wird das nächste Vielfache $j + k$ übersprungen da es eine bereits ausgesiebte gerade Zahl ist: $k$ ist immer ungerade. In Zeile 7 ist dann $j = k^2$ ebenfalls ungerade. Die Summe $j + k$ zweier ungeraden Zahlen ergibt eine gerade Zahl. Dagegen ist $2k$ gerade und die Summe $j + 2k$ einer ungeraden und einer geraden Zahl ergibt eine ungerade Zahl. Damit bleibt $j$ ungerade. Wenn die for-Schleife nie durch die Rückgabe eines Faktors in Zeile 6 verlassen wurde, dann hat $n$ keinen nichttrivialen Teiler und ist folglich prim. In diesem Fall wird in Zeile 11 der Wert 0 ausgegegeben.

Primzahlen sind gewissermaßen die Atome der Zahlen: Man kann sie nicht weiter in Faktoren zerlegen und jede natürliche Zahl $n$ lässt sich als Produkt von Primzahlen darstellen. Das gilt für $n = 1$, wenn man das Produkt über 0 Primzahlen als 1 definiert. Es gilt aber auch für $n = 2$ oder $n = 3$, da dies selbst Primzahlen sind. Nehmen wir induktiv an, dass sich alle Zahlen $< n$ in Primfaktoren zerlegen lassen und zeigen nun die Behauptung für $n$. Ist $n$ selbst Primzahl, dann ist nichts weiter zu zeigen. Ist $n$ keine Primzahl, dann hat $n$ zwei echte Teiler, $n = km$, mit $1 < k, m < n$. Nach Voraussetzung lassen sich $k$ und $m$ zerlegen in $k = p_1 \cdots p_s$ und $m = q_1 \cdots q_t$, für Primzahlen $p_1, \ldots, p_s$ und $q_1, \ldots, q_t$. Damit erhalten wir für $n$ die Darstellung $n = km = p_1 \cdots p_s q_1 \cdots q_t$.

Zerlegen wir $n = 60$, so erhalten wir

$$60 = 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5.$$

Meisten schreibt man die Primfaktoren so wie hier in aufsteigender Reihenfolge und fasst gleiche Primzahlen mittels Potenzen zusammen. Wir schreiben also

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

mit $p_1 < \cdots < p_k$ prim und Potenzen $e_i \geq 1$, für $i = 1, \ldots, k$. Als nächstes zeigen wir, dass diese Darstellung von $n$ eindeutig ist.

**Theorem 7.13** *Die Darstellung* $n = p_1 \cdots p_t$ *mit* $p_1 \leq \cdots \leq p_t$ *prim ist eindeutig.*

**Beweis.** Die Behauptung gilt offenbar für $n = 1$ und 2. Sei also $n > 2$ und gelte die Behauptung für alle Zahlen $< n$. Nehmen wir an, es gäbe zwei verschiedene Darstellungen für $n$,

$$n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_s,$$

mit $q_1 \leq q_2 \leq \cdots \leq q_s$. Es muss $p_1 \neq q_1$ gelten, da sonst $p_2 \cdots p_t = q_2 \cdots q_s$ verschiedene Primfaktor Zerlegungen einer Zahl $< n$ wären. Nach der Induktionsvoraussetzung ist das aber nicht möglich. Wir können also o.B.d.A. annehmen, dass $p_1 < q_1$ ist und somit $\mathrm{ggT}(p_1, q_1) = 1$. Nach Lemma 7.9 gibt es ganze Zahle $a$ und $b$, so dass gilt $ap_1 + bq_1 = 1$. Damit können wir folgende Aussagen über die Teilbarkeit durch $p_1$ machen:

(i) $p_1 \backslash aq_1 q_2 \cdots q_s$, und

(ii) $p_1 \backslash bq_1 \cdots q_s$.

Die Teilbarkeit (i) ist offensichtlich, da $p_1$ als Faktor auftaucht. Die Teilbarkeit (ii) gilt, da $q_1 \cdots q_s = n$, und nach Voraussetzung gilt $p_1 \backslash n$.

Damit teilt $p_1$ auch die Summe der beiden Zahlen

$$\begin{aligned} ap_1q_2 \cdots q_s + bq_1 \cdots q_s &= (ap_1 + bq_1)q_2 \cdots q_s \\ &= q_2 \cdots q_s, \end{aligned}$$

da $ap_1 + bq_1 = 1$. Nun ist $q_2 \cdots q_s < n$ und nach Induktionsvoraussetzung die Primfaktor Zerlegung eindeutig. Da $p_1 \backslash q_2 \cdots q_s$ und $p_1$ prim ist, muss also $p_1$ selbst bei den $q_i$'s dabei sein. Das kann aber nicht sein, da $p_1$ nach Voraussetzung kleiner als $q_1$, und damit kleiner als alle $q_i$'s ist. Wir erhalten also einen Widerspruch zu der Annahme, dass es mehr als eine Zerlegung in Primfaktoren für $n$ gibt. □

Schon Carl Friedrich Gauß hat sich mit der Frage beschäftigt wieviele Primzahlen es gibt. Eine erste Antwort ist: unendlich viele. Gäbe es nämlich nur endlich viele, könnten wir sie alle angeben. Nehmen wir also an, dass $p_1, p_2, \ldots, p_k$ alle Primzahlen sind. Wir definieren die Zahl

$$N = p_1p_2 \cdots p_k + 1.$$

Keine der Primzahlen $p_1, p_2, \ldots, p_k$ teilt N, da N gerade so definiert ist, dass N mod $p_i = 1$ für alle $i$. Andererseits haben wir bereits gezeigt, dass sich jede natürliche Zahl in Primfaktoren zerlegen lässt. Die Primfaktoren von N kommen aber nicht in $p_1, p_2, \ldots, p_k$ vor. Folglich können dies nicht alle Primzahlen gewesen sein.

Insbesondere in der Kryptographie werden große Primzahlen benötigt und es ist wichtig, dass es viele Primzahlen gibt. Von daher ist man an der Verteilung der Primzahlen innerhalb natürlichen Zahlen interessiert. Die ist nach wie vor ziemlich undurchsichtig. Beispielsweise gibt es bis heute keine einfache Formel, die ausschließlich Primzahlen produziert. Man weiß allerdings, dass die Primzahlen sehr dicht gestreut sind. Dies ist die Aussage des **Primzahlsatzes**. Definieren wir die Funktion $\pi(n)$ als die Anzahl der Primzahlen $\leq n$, also

$$\pi(n) = |\{\, p \mid p \leq n \text{ prim} \,\}|,$$

dann gilt

$$\pi(n) \sim \frac{n}{\ln n}.$$

Dabei kann man das Symbol $\sim$ als 'ungefähr gleich' lesen. Formal ist es definiert als *assymptotisch proportional*, d.h. dass der Quotient von $\pi(n)$ und $n/\ln n$ gegen 1 konvergiert wenn $n$ gegen unendlich geht. Aus den Primzahlsatz folgt, dass es sehr viele Primzahlen gibt, da die Funktion $\ln n$ nur sehr langsam wächst.

Die eindeutige Primfaktor Zerlegung jeder Zahl erlaubt eine andere Art der Zahlendarstellung, indem man für $n$ angibt, wie oft jede Primzahl in $n$ vorkommt. Zum Beispiel für $n = 84$ haben wir $84 = 2^2 \cdot 3 \cdot 7$. Wir betrachten die Primzahlen in aufsteigender Reihenfolge $2, 3, 5, 7, 11, \ldots$. In 84 kommt die 2 zweimal vor, die 3 einmal, 5 nullmal, 7 einmal, und alle anderen Primzahlen nullmal. Wir schreiben 84 also als Sequenz $(2, 1, 0, 1, 0, 0, \ldots)$. Wegen der Eindeutigkeit der Primfaktor Zerlegung ist auch diese Darstellung eindeutig. Allgemein sei

$$n = 2^{n_2} \cdot 3^{n_3} \cdots p_t^{n_{p_t}},$$

mit $n_p \geq 0$ für alle $p$. Dann schreiben wir für $n$

$$n \to (n_2, n_3, \dots, n_{p_t}, 0, 0, \dots).$$

Diese Zahlendarstellung hat einige Vorteile wie wir im Folgenden sehen werden.

Sei $m$ einen weitere Zahl mit der Darstellung

$$m \to (m_2, m_3, \dots).$$

Das Produkt $mn$ kann mit dieser Darstellung sehr einfach berechnet werden: Es genügt die Potenzen der Primzahlen zu addieren,

$$mn \to (m_2 + n_2, m_3 + n_3, \dots). \tag{7.4}$$

Damit $m$ Teiler von $n$ ist, darf keine Primzahl-Potenz von $m$ größer sein als die entsprechende Primzahl-Potenz von $n$.

$$m \backslash n \iff m_p \leq n_p \quad \forall p.$$

Für den Quotient $n/m$ erhalten wir in diesem Fall die Darstellung

$$n/m \to (n_2 - m_2, n_3 - m_3, \dots).$$

Nun erhalten wir auch eine Beschreibung des größten gemeinsamen Teilers von $m$ und $n$. Für jedes $p$ nehmen wir die größte Potenz die $\leq m_p$ und $\leq n_p$ ist. D.h.

$$\mathrm{ggT}(m, n) \to (\min\{m_2, n_2\}, \min\{m_3 + n_3\}, \dots).$$

Für das kleinste gemeinsame Vielfache von $m$ und $n$ erhalten wir eine entsprechende Beschreibung. Für jedes $p$ nehmen wir die kleinste Potenz die $\geq m_p$ und $\geq n_p$ ist. D.h.

$$\mathrm{kgV}(m, n) \to (\max\{m_2, n_2\}, \max\{m_3 + n_3\}, \dots).$$

Bilden wir nun das Produkt $\mathrm{ggT}(m, n)\mathrm{kgV}(m, n)$ dann müssen wir die einzelnen Potenzen addieren. D.h. für jedes $p$ bilden wir die Summe $\min\{m_p, n_p\} + \max\{m_p, n_p\}$. Ist nun $m_p \leq n_p$, dann wird die Summe zu $m_p + n_p$. Ist dagegegen $m_p \geq n_p$, dann erhalten wir $n_p + m_p$. Da die Addition kommutativ ist, gilt also

$$\min\{m_p, n_p\} + \max\{m_p, n_p\} = m_p + n_p.$$

Dies ist die Potenz, die wir in (7.4) für das Produkt $mn$ haben. Damit haben wir folgende Gleichung gezeigt

$$\mathrm{ggT}(m, n)\mathrm{kgV}(m, n) = mn.$$

Für das kleinste gemeinsame Vielfache erhalten wir daraus die Beziehung

$$\mathrm{kgV}(m, n) = \frac{mn}{\mathrm{ggT}(m, n)}.$$

Weil wir mit dem euklidischen Algorithmus ein effizientes Verfahren zur Berechnung des größten gemeinsamen Teilers haben, können wir mittels dieser Formel daraus auch das kleinste gemeinsame Vielfache effizient berechnen.

Hat man die Primfaktor-Zerlegungen zweier Zahlen gegeben, so ist die ggT- und kgV-Bestimmung mit den obigen Überlegungen noch einfacher als mit dem euklidischen Algorithmus. Das Problem dabei ist, dass man zuerst die Primfaktor-Zerlegungen berechnen muss.

Bis heute kennt man kein *effizientes* Verfahren zur Bestimmung der Primfaktoren einer gegebenen Zahl!

Wie man sieht hat es sich aber trotzdem gelohnt, die Eigenschaften von Primfaktor-Zerlegungen zu betrachten. So konnten wir elegant obige Formel für das kgV herleiten, in der die Primfaktoren wieder verschwunden sind und nur noch der ggT auftaucht. Erst dadurch erhielten wir ein effizientes Verfahren für das kgV.

Eine Anwendung des kleinsten gemeinsamen Vielfachen ist die Addition von Brüchen. Die Summe $\frac{a}{b} + \frac{c}{d}$ ist definiert als $\frac{ad+bc}{bd}$. Dabei ist $bd$ der sogenannte *Hauptnenner* der beiden Brüche. Dieser Hauptnenner kann jedoch unnötig groß sein und somit zu einem erhöhten Rechenaufwand führen. Der kleinst-mögliche Hauptnenner ist $\mathrm{kgV}(b, d)$. Es gilt

$$\frac{a}{b} + \frac{c}{d} = \frac{a\frac{\mathrm{kgV}(b,d)}{b} + c\frac{\mathrm{kgV}(b,d)}{d}}{\mathrm{kgV}(b, d)}.$$

Führt man dabei alle beteiligten Divisionen so früh wie möglich aus, so bleiben alle Zwischen-Ergebnisse möglichst klein. Zum Schluss kann man den Bruch eventuell noch kürzen. D.h. man sucht nach gemeinsamen Faktoren von Zähler und Nenner. Zum Beispiel

$$\frac{12}{18} = \frac{2 \cdot 6}{3 \cdot 6} = \frac{2}{3}.$$

Da 2 und 3 keine gemeinsamen Faktoren mehr haben, ist der Bruch nun so weit gekürzt wie möglich. Dies motiviert die folgende Definition.

**Definition 7.14** *Zwei Zahlen* $m$ *und* $n$ *heißen* teilerfremd *oder* relativ prim*, falls* $\mathrm{ggT}(m, n) = 1$. *Als Kurzform schreiben wir* $m \perp n$.

Mit anderen Worten, $m$ und $n$ sind teilerfremd wenn sie keine gemeinsamen Primfaktoren haben.

In obiger Zahlen-Darstellung mittels Primzahl-Potenzen hat 1 die Darstellung $1 \to (0, 0, \dots)$. D.h. für die Primzahl-Potenzen von $n$ und $m$ gilt $\min\{m_p, n_p\} = 0$ für alle Primzahlen $p$, oder, gleichwertig dazu, $m_p n_p = 0$. Die Ähnlichkeit zu einem inneren Vektorprodukt ist die Motivation für die Kurzschreibweise $m \perp n$.

Hat eine Zahl $k$ keine gemeinsamen Primfaktoren mit $m$ und mit $n$, dann auch nicht mit dem Produkt $mn$, da im Produkt genau die Primfaktoren von $n$ und $m$ sind. Es gilt also

$$k \perp m \text{ und } k \perp n \iff k \perp mn.$$

Ist $p$ Primzahl und teilt das Produkt $mn$, dann hat mindestens eine der beiden Zahlen $p$ als Primfaktor und somit gilt:

$$p \text{ prim und } p \backslash mn \implies p \backslash m \text{ oder } p \backslash n. \tag{7.5}$$

Nehmen wir statt $p$ eine zusammen gesetzte Zahl $k$, so können wir nicht mehr so schließen. Z.B. ist 4 ein Teiler von $60 = 6 \cdot 10$, aber weder Teiler von 6 noch von 10. Der Grund ist, dass die Primfaktoren von 4 auf die beiden Faktoren 6 und 10 verteilt sind. Dagegen ist in

der Zerlegung $60 = 5 \cdot 12$ die 5 teilerfremd zu 4 und entprechend 4 ein Teiler des anderen Faktors 12. Es gilt allgemein

$$k \backslash mn \text{ und } k \perp m \implies k \backslash n.$$

Kommen wir zurück zum Kürzen von Brüchen. Der größte Faktor in einem Bruch $\frac{a}{b}$ ist der größte gemeinsame Teiler von $a$ und $b$. Kürzt man also mit $ggT(a, b)$, so ist sind Zähler und Nenner teilerfremd,

$$\frac{a}{b} = \frac{a/ggT(a, b)}{b/ggT(a, b)},$$

und es gilt $a/ggT(a, b) \perp b/ggT(a, b)$. Der Bruch ist damit soweit wie möglich gekürzt.

Manche ganze Zahlen haben ganzzahlige Wurzeln, wie zum Beispiel $\sqrt{9} = 3$. Ist $\sqrt{n} = q$, dann ist $q$ auch Faktor von $n$, da nach Definition $q^2 = n$ gilt. Da eine Primzahl keine nichttrivialen Faktoren hat, kann auch keine Primzahl eine ganzzahlige Wurzel haben. Wir zeigen, dass $\sqrt{p}$ für Primzahlen $p$ nicht einmal rational ist. Nehmen wir an, es gäbe einen Bruch mit $\sqrt{p} = \frac{a}{b}$. Der Bruch sei soweit wie möglich gekürzt, d.h. es gelte $a \perp b$. Aus $\sqrt{p} = \frac{a}{b}$ folgt

$$b^2 p = a^2. \tag{7.6}$$

Folglich gilt $p \backslash a^2$. Da $p$ prim ist folgt nach (7.5), dass gilt $p \backslash a$. Wir können also $a$ zerlegen in $a = tp$ für eine Zahl $t$. Eingesetzt in Gleichung (7.6) erhalten wir $b^2 p = t^2 p^2$. Wir kürzen $p$ auf beiden Seiten der Gleichung und erhalten $b^2 = t^2 p$. Folglich gilt $p \backslash b^2$ und somit $p \backslash b$, da $p$ prim ist. Damit haben $a$ und $b$ den gemeinsamen Faktor $p$. Dies steht aber im Widerspruch zu unserer Voraussetzung, dass $a$ und $b$ teilerfremd sind. Folglich lässt sich $\sqrt{p}$ nicht als Bruch schreiben.

## 7.3 Kongruenz

Die *Kongruenz-Relation* $\equiv_m$ setzt ganze Zahlen miteinander in Beziehung, die den gleichen Rest haben bei Division durch eine Zahl $m \geq 1$: für ganze Zahlen $a, b$ definieren wir

$$a \equiv_m b, \text{ falls } a \bmod m \;=\; b \bmod m.$$

Wir sagen $a$ *ist kongruent zu* $b$ *modulo* $m$.

Obige Schreibweise $a \equiv_m b$ ist die, die bei zweistelligen Relation üblich ist: das Relationssymbol steht zwischen den beiden Elementen. Bei der Kongruenz-Relation hat sich jedoch eine andere Schreibweise durchgesetzt, die auf Gauß zurückgeht. Statt $a \equiv_m b$ schreibt man

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

Zum Beispiel ist

$$1 \equiv 4 \equiv 7 \equiv -2 \equiv -5 \pmod 3,$$
$$2 \equiv 7 \equiv 12 \equiv -3 \equiv -8 \pmod 5.$$

Da die Kongruenz-Relation mittels einer Gleichheit definiert ist, sieht man leicht, dass es sich um eine Äquivalenz-Relation handelt. Zum Beispiel die Äquivalenzklasse von 2 modulo 5 ist

$$\begin{aligned}[2]_{\equiv_5} &= \{\ldots,\ -8,\ -3,\ 2,\ 7,\ 12,\ \ldots\} \\ &= \{5t+2 \mid t \in \mathbb{Z}\}.\end{aligned}$$

Allgemein gibt es $m$ Äquivalenzklassen modulo $m$. Für jedes $r \in \mathbb{Z}_m = \{0,\ 1,\ \ldots,\ m-1\}$ gibt es eine Äquivalenzklasse

$$[r]_{\equiv_m} = \{tm + r \mid t \in \mathbb{Z}\}.$$

Diese sind paarweise disjunkt und ihre Vereinigung ergibt $\mathbb{Z}$.

## 7.4 Rechenregeln von Kongruenzen

Offensichtlich gilt

$$a \equiv 0 \pmod{m} \iff m \backslash a.$$

Allgemeiner sieht man an obigen Beispielen, dass die Differenz zweier kongruenter Zahlen $a$ und $b$ immer Vielfaches des Moduls $m$ ist.

**Theorem 7.15** $a \equiv b \pmod{m} \iff m \backslash (a-b)$.

**Beweis.** Sei $a = k_a m + r_a$ und $b = k_b m + r_b$ mit $0 \leq r_a, r_b \leq m-1$. Dann ist $r_a = a \bmod m$ und $r_b = b \bmod m$. Die Bedingung $a \equiv b \pmod{m}$ heißt also, dass $r_a = r_b$ ist. Es gilt

$$\begin{aligned}a - b &= (k_a m + r_a) - (k_b m + r_b) \\ &= (k_a - k_b)m + (r_a - r_b).\end{aligned}$$

Folglich gilt

$$m \backslash (a-b) \iff m \backslash (r_a - r_b)\,.$$

Da die Reste $r_a, r_b \in \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ liegen, gilt für die Differenz $r_a - r_b \in \{-(m-1), \ldots, -1, 0, 1, \ldots, m-1\}$. Das einzige Vielfache von $m$ in diesem Bereich ist 0. Deshalb gilt

$$m \backslash (r_a - r_b) \iff r_a - r_b = 0\,.$$

Zusammengefasst erhalten wir

$$m \backslash (a-b) \iff r_a = r_b\,.$$

Das war zu zeigen. □

Da $m \backslash (a-b)$ äquivalent ist zu $a - b \equiv 0 \pmod{m}$, kann man also in Kongruenzen der Form $a \equiv b \pmod{m}$ z.B. das $b$ auf die andere Seite des Kongruenz-Zeichens bringen, so wie man es bei Gleichungen über ganzen Zahlen gewohnt ist.

**Folgerung 7.16** $a \equiv b \pmod{m} \iff a - b \equiv 0 \pmod{m}$.

Wir wollen einen arithmetischen Ausdruck modulo $m$ berechnen. Als Beispiel betrachten wir $a = 109$ und $c = 54$. Für $m = 7$ ergibt sich

$$a + c = 109 + 54 = 164 \equiv 2 \pmod 7.$$

Wir haben dabei zuerst die Summe von $a$ und $c$ berechnet und dann das Ergebnis modulo 7 reduziert. Um mit möglichst kleinen Zahlen zu rechnen ist es geschickter, die Summanden bereits *vor* der Addition modulo 7 zu reduzieren: sei $b = a \bmod 7 = 4$ und $d = c \bmod 7 = 5$, dann gilt

$$b + d = 4 + 5 = 9 \equiv 2 \pmod 7.$$

Wir bekommen also dasselbe Ergebnis, rechnen dabei aber mit Zahlen die kleiner als der Modul sind. Das folgende Lemma zeigt, dass diese Vorgehensweise zulässig ist, also immer das gleiche Ergebnis liefert, und analog auch für Subtraktion und Multiplikation funktioniert.

**Lemma 7.17** *Seien* $a \equiv b \pmod m$ *und* $c \equiv d \pmod m$. *Dann gilt*

(1) $a + c \equiv b + d \pmod m$,

(2) $a - c \equiv b - d \pmod m$,

(3) $ac \equiv bd \pmod m$.

**Beweis.** Wir wenden Theorem 7.15 an.

$$\begin{aligned} a + c \equiv b + d \pmod m &\iff (a + c) - (b + d) \equiv 0 \pmod m \\ &\iff (a - b) + (c - d) \equiv 0 \pmod m. \end{aligned}$$

Die letzte Zeile gilt, da nach Voraussetzung $m \backslash (a - b)$ und $m \backslash (c - d)$, und folglich $m \backslash ((a - b) + (c - d))$.

Der Beweis von (2) verläuft analog. Wir zeigen noch Teil (3). Es gilt

$$\begin{aligned} ac \equiv bd \pmod m &\iff ac - bd \equiv 0 \pmod m \\ &\iff ac - bc + bc - bd \equiv 0 \pmod m \\ &\iff (a - b)c + (c - d)b \equiv 0 \pmod m. \end{aligned}$$

Die letzte Zeile ist nach Voraussetzung richtig. □

Durch Induktion folgt, dass man diese Regeln analog auch auf größere Ausdrücke anwenden kann. Zum Beispiel um $98 \cdot 292 + 191 \pmod 3$ zu berechnen, nehmen wir die beteiligten Zahlen zuerst modulo 3: es ist $98 \equiv 2 \pmod 3$, $292 \equiv 1 \pmod 3$ und $191 \equiv 2 \pmod 3$. Nach Lemma 7.17 (3) und (1) ist dann

$$98 \cdot 292 + 191 \equiv 2 \cdot 1 + 2 \equiv 1 \pmod 3.$$

Die eigentlich Rechung erfolgt also auf deutlich kleineren Zahlen als wenn wir den gegebenen Ausdruck zuerst berechnen und erst zum Schluss modulo 3 reduzieren.

Aus den Rechenregeln folgt außerdem, dass man Kongruenzen wie gewöhnliche Gleichungen umformen kann, so wie man es beispielsweise von den ganzen Zahlen her kennt. Betrachten wir die Kongruenz

$$x - 3 \equiv 5 \pmod 7. \tag{7.7}$$

Da trivialerweise $3 \equiv 3 \pmod 7$ gilt, können wir nach Lemma 7.17 (1) eine Zahl auf beiden Seiten der Kongruenz (7.7) hinzu addieren. Dies ergibt

$$(x - 3) + 3 \equiv 5 + 3 \pmod 7,$$

und folglich gilt auch

$$x \equiv 8 \pmod 7. \tag{7.8}$$

Da man nach Lemma 7.17 (2) analog auch eine Zahl auf beiden Seiten der Kongruenz (7.8) abziehen kann, folgt aus $x \equiv 8 \pmod 7$ auch $x - 3 \equiv 5 \pmod 7$. D.h. die beiden Kongruenzen (7.7) und (7.8) haben die gleiche Lösungsmenge. Da $8 \equiv 1 \pmod 7$, sind folglich alle $x$ mit $x \equiv 1 \pmod 7$ Lösung obiger Gleichung. Analog erhält man für die Gleichung $x + 3 \equiv 5 \pmod 7$ die Lösung $x \equiv 2 \pmod 7$.

Setzen wir in Lemma 7.17 speziell $a = c$ und $b = d$, so folgt aus (3)

$$a^2 \equiv b^2 \pmod m.$$

Induktiv erhalten wir für jede Potenz $n$

**Folgerung 7.18** *Ist* $a \equiv b \pmod m$, *dann ist* $a^n \equiv b^n \pmod m$, *für alle* $n \geq 0$.

Zum Beispiel ist $2 \equiv -1 \pmod 3$. Also ist auch $2^n \equiv (-1)^n \pmod 3$. Nach Lemma 7.17 (2) ist dann auch $2^n - 1 \equiv (-1)^n - 1 \pmod 3$. Da

$$(-1)^n - 1 = \begin{cases} 0, & \text{falls } n \text{ gerade,} \\ -2, & \text{falls } n \text{ ungerade,} \end{cases}$$

erhalten wir das Ergebnis

$$3 \backslash (2^n - 1) \iff n \text{ gerade.}$$

Ob eine Dezimalzahl durch 3 teilbar ist kann man mittels der Quersumme einfach erkennen. Sei $a = a_{n-1} \cdots a_1 a_0$ eine $n$-stellige Dezimalzahl, d.h. die $a_i$'s sind die Ziffern von $a$ mit $a_i \in \{0, \ldots, 9\}$. Der Zahlenwert von $a$ berechnet sich nach der Formel

$$a = \sum_{k=0}^{n-1} a_k 10^k.$$

Wir betrachten zunächst die Zehner-Potenzen. Es gilt offensichtlich $10 \equiv 1 \pmod 3$. Mit Folgerung 7.18 erhalten wir damit $10^k \equiv 1 \pmod 3$ für alle $k \geq 0$. Dann gilt nach Lemma 7.17 (3) auch $a_k 10^k \equiv a_k \pmod 3$ für alle $k \geq 0$. Nun wenden wir $(n-1)$-mal Lemma 7.17 (1) an und erhalten

$$a = \sum_{k=0}^{n-1} a_k 10^k \equiv \sum_{k=0}^{n-1} a_k \pmod 3.$$

Den Summe auf der rechten Seite nennt man die *Quersumme von* $a$. Sie ist also modulo 3 kongruent zu $a$. Folglich ist $a$ genau dann durch 3 teilbar, wenn dies für die Quersumme zutrifft.

In Lemma 7.17 wird keine Division behandelt. Der Grund ist, dass man hier vorsichtig sein muss, wie folgendes Beispiel zeigt. Es gilt zwar $3 \cdot 2 \equiv 5 \cdot 2 \pmod 4$, aber man kann die 2 nicht kürzen: Es gilt $3 \not\equiv 5 \pmod 4$. Was geht hier schief? Betrachten wir allgemein die Kongruenz $ad \equiv bd \pmod m$. Es gilt

$$\begin{aligned} ad \equiv bd \pmod m &\iff m \backslash ad - bd \\ &\iff m \backslash (a-b)d. \end{aligned}$$

Daraus können wir aber nicht folgern, dass $m$ Teiler von $a-b$ ist, da sich die Prim-Faktoren von $m$ auf beide Faktoren, $a-b$ und $d$ verteilen können. Wir verhindern dies, indem wir zusätzlich verlangen, dass $m$ und $d$ keine gemeinsamen Prim-Faktoren haben. Dann können wie schließen, dass $m$ Teiler von $a-b$ ist, und folglich $a \equiv b \pmod m$ gilt.

**Lemma 7.19** *Sei* $d \perp m$ *und* $ad \equiv bd \pmod m$, *dann gilt* $a \equiv b \pmod m$.

## 7.5 Lineare Kongruenzen

Mit Hilfe von Lemma 7.19 können wir lineare Gleichungen lösen. Betrachten wir die Kongruenz

$$2x \equiv 5 \pmod 7. \tag{7.9}$$

Im Unterschied zur Kongruenz (7.7) ist hier noch der Faktor 2 bei $x$. Nach Lemma 7.17 (3) können wir beide Seiten der Kongruenz (7.9) mit einer Zahl multiplizieren. Wir multiplizieren mit 4 und erhalten

$$4 \cdot 2x \equiv 4 \cdot 5 \pmod 7. \tag{7.10}$$

Jede Lösung $x$ für Kongruenz (7.9) löst also auch Kongruenz (7.10). Da $4 \perp 7$ können wir nach Lemma 7.19 die 4 auch wieder kürzen. D.h. die beiden Kongruenzen (7.9) und (7.10) haben die gleichen Lösungen. Kongruenz (7.10) können wir noch etwas vereinfachen. Da $8 \equiv 1 \pmod 7$ und $20 \equiv 6 \pmod 7$ ist Kongruenz (7.10) äquivalent zu

$$x \equiv 6 \pmod 7.$$

Damit haben wir unser Ziel erreicht und Kongruenz (7.9) nach $x$ aufgelöst.

Versuchen wir allgemein die Kongruenz

$$ax \equiv b \pmod m. \tag{7.11}$$

zu lösen. Der Trick in obigem Beispiel bestand darin, eine Zahl $a'$ zu finden, die zu $m$ teilerfremd ist, so dass $a'a \equiv 1 \pmod m$. Dann hat nämlich die Kongruenz (7.11) diesselben Lösungen wie

$$a'ax \equiv x \equiv a'b \pmod m.$$

Wie kommt man zu $a'$? Es gilt

$$a'a \equiv 1 \pmod m \iff a'a = km + 1, \text{ für ein } k \in \mathbb{Z}.$$

Setzen wir $m' = -k$ , so können wir die Gleichung umschreiben zu $a'a + m'm = 1$. D.h. es gibt eine Linearkombination von $a$ und $m$, die den Wert 1 ergibt. Das ist nach Folgerung 7.11 auf Seite 6 gleichwertig dazu, dass der größte gemeinsame Teiler von $a$ und $m$ gleich 1 ist. Außerdem sind $a'$ und $m'$ die Koeffizienten, die der erweiterte euklidische Algorithmus auf Eingabe von $a$ und $m$ berechnet.

Wir fassen unsere Beobachtungen zusammen: Ist $a$ teilerfremd zu $m$, dann liefert der erweiterte euklidische Algorithmus eine Zahl $a' \in \mathbb{Z}$ mit der Eigenschaft $a'a \equiv 1 \pmod{m}$. Die zu $a'$ kongruente Zahl in $Z_m$, also $a' \bmod m$, wird als das *Inverse zu* $a$ *modulo* $m$ bezeichnet. Man schreibt dafür auch $a^{-1}$. Die Kongruenz $ax \equiv b \pmod{m}$ hat dann die Lösungen $x \equiv a^{-1}b \pmod{m}$.

**Theorem 7.20** *Ist* $a \perp m$*, dann hat die Kongruenz* $ax \equiv b \pmod{m}$ *die in* $\mathbb{Z}_m$ *eindeutige Lösung* $x = a^{-1}b \bmod m$.

**Beweis.** Die Existenz einer Lösung haben wir schon gezeigt. Es bleibt noch die Eindeutigkeit. Seien $x, x' \in \mathbb{Z}_m$ zwei Lösungen. D.h. es gilt

$$ax \equiv b \equiv ax' \pmod{m}.$$

Multiplizieren wir die Kongruenz mit dem Inversen $a^{-1}$ von $a$, so erhalten wir $a^{-1}ax \equiv a^{-1}ax' \pmod{m}$ und folglich $x \equiv x' \pmod{m}$. Es gibt also nur eine Lösung in $\mathbb{Z}_m$. □

Die Menge der zu $m$ teilerfremden Zahlen in $\mathbb{Z}_m$ bezeichnen wir mit $\mathbb{Z}_m^*$,

$$\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m \mid k \perp m\}.$$

Zum Beispiel ist

$$\begin{aligned}
\mathbb{Z}_2^* &= \{1\},\\
\mathbb{Z}_3^* &= \{1,2\},\\
\mathbb{Z}_4^* &= \{1,3\},\\
\mathbb{Z}_5^* &= \{1,2,3,4\},\\
\mathbb{Z}_6^* &= \{1,5\}.
\end{aligned}$$

Betrachten wir lineare Kongruenzen über dem Grundbereich $\mathbb{Z}_m^*$, d.h. Kongruenzen $ax \equiv b \pmod{m}$ wobei $a$ und $b$ aus $\mathbb{Z}_m^*$ sind. Aus Theorem 7.20 folgt, dass diese Kongruenzen immer eindeutig lösbar in $\mathbb{Z}_m$ sind. Zusätzlich liegt die Lösung sogar in $\mathbb{Z}_m^*$: Die Lösung $x$ hat die Form $x = a^{-1}b \bmod m$. Nach Voraussetzung ist $b$ teilerfremd zu $m$. Wir zeigen, dass auch $a^{-1}$ teilerfremd zu $m$ ist. Daraus folgt, dass $x$ ebenfalls teilerfremd zu $m$ ist.

Nach Voraussetzung ist $a$ teilerfremd zu $m$. Es gibt also eine Zahl $m'$ mit

$$a^{-1}a + m'm = 1.$$

In dieser Gleichung können wir die Rollen von $a^{-1}$ und $a$ auch vertauschen. D.h. $a$ und $m'$ sind die Koeffizienten die zeigen, dass $\mathrm{ggT}(a^{-1}, m) = 1$ ist.

**Folgerung 7.21** *Für* $a, b \in \mathbb{Z}_m^*$ *hat die Kongruenz* $ax \equiv b \pmod{m}$ *genau eine Lösung in* $\mathbb{Z}_m^*$.

Betrachten wir für $a \in \mathbb{Z}_m^*$ die Funktion $f(x) = ax \mod m$ auf $\mathbb{Z}_m^*$. Folgerung 7.21 ist gleichwertig zu der Aussage, dass $f$ bijektiv auf $\mathbb{Z}_m^*$ ist:

- $f$ ist surjektiv, da für beliebiges $b \in \mathbb{Z}_m^*$ die Kongruenz $ax \equiv b \pmod m$ eine Lösung $x \in \mathbb{Z}_m^*$ hat,
- $f$ ist injektive, da diese Lösung eindeutig ist.

**Folgerung 7.22** *Für $a \in Z_m^*$ ist $f(x) = ax \mod m$ eine Bijektion auf $\mathbb{Z}_m^*$.*

In Übungsaufgabe 1 soll man zeigen, dass für $a, b \in Z_m^*$ auch die Funktion $f(x) = ax + b \mod m$ eine Bijektion auf $\mathbb{Z}_m^*$ ist.

## 7.6 Mehrere lineare Kongruenzen

Wir betrachten den Fall, dass wir zwei lineare Kongruenzen gegeben haben,

$$\begin{aligned} a_1 x &\equiv b_1 \pmod m \\ a_2 x &\equiv b_2 \pmod n. \end{aligned}$$

Wir suchen eine Lösung $x$ die beide Gleichungen erfüllt. Nehmen wir an, dass $a_1 \perp m$ und $a_2 \perp n$, dann können wir die Kongruenzen mit Hilfe von Theorem 7.20 vereinfachen zu

$$\begin{aligned} x &\equiv a \pmod m \\ x &\equiv b \pmod n \end{aligned}$$

mit $a = a_1^{-1} b_1$ und $b = a_2^{-1} b_2$.

Betrachten wir das Beispiel $m = 2$ und $n = 3$:

| $x$ | $x \bmod 2$ | $x \bmod 3$ |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| 2 | 0 | 2 |
| 3 | 1 | 0 |
| 4 | 0 | 1 |
| 5 | 1 | 2 |
| 6 | 0 | 0 |

Wir können die Tabelle als Funktion $f$ lesen, die jedem $x \in Z_{mn} = \mathbb{Z}_6$ wird das Paar $(x \bmod 2, x \bmod 3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ zugeordnet:

$$f : \ x \in \mathbb{Z}_6 \mapsto (x \bmod 2, x \bmod 3) \in \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Da die Funktionswerte in der Tabelle alle verschieden sind, ist $f$ injektiv. Da $\mathbb{Z}_2 \times \mathbb{Z}_3$ 6 Elemente hat, $|\mathbb{Z}_2 \times \mathbb{Z}_3| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_3| = 6$, kommt jedes Paar aus $\mathbb{Z}_2 \times \mathbb{Z}_3$ genau einmal vor. Also ist $f$ auch surjektiv und damit bijektiv. D.h. jedes Paar $(a, b)$ mit $a \in \mathbb{Z}_2$ und $b \in \mathbb{Z}_3$

beschreibt eindeutig ein $x \in \mathbb{Z}_6$ und umgekehrt. Für unsere zwei linearen Kongruenzen heißt das, dass es immer ein Lösung gibt, für jedes $a \in \mathbb{Z}_2$ und jedes $b \in \mathbb{Z}_3$. Außerdem ist die Lösung eindeutig in $\mathbb{Z}_6$.

Wir zeigen als nächstes, dass die Beobachtungen in unserem Beispiel allgemein gelten, wenn $m$ und $n$ teilerfremd sind. Eine Frage dabei ist, wie wir von einem gegebenen Paar $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ möglichst einfach das zugehörige $x$ finden. Für größere Werte von $m$ und $n$ ist es nicht mehr praktikabel obige Tabelle aufzustellen um darin den Wert $x$ zu suchen.

Wir lösen die Kongruenzen zunächst für zwei Spezialfälle, nämlich für $(a, b) = (1, 0)$ und $(a, b) = (0, 1)$. Wir setzen voraus, dass $m \perp n$. Dann gibt es Zahlen $m'$ und $n'$, so dass

$$m'm + n'n = 1.$$

Wir betrachten die Gleichung modulo $m$:

$$1 = m'm + n'n \equiv n'n \pmod{m}.$$

Definieren wir $x_1 = n'n$. Dann gilt also

$$\begin{aligned} x_1 &\equiv 1 \pmod{m} \\ x_1 &\equiv 0 \pmod{n}. \end{aligned}$$

$x_1$ ist also die Lösung für den Fall $(a, b) = (1, 0)$. Multiplizieren wir beide Kongruenzen mit einer Zahl $a$, so erhalten wir

$$\begin{aligned} ax_1 &\equiv a \pmod{m} \\ ax_1 &\equiv 0 \pmod{n}. \end{aligned}$$

$ax_1 = an'n$ ist also die Lösung für Paare der Form $(a, 0)$.

Betrachten wir obige Gleichung nun modulo $n$, so erhalten wir analog für $x_2 = m'm$:

$$\begin{aligned} x_2 &\equiv 0 \pmod{m} \\ x_2 &\equiv 1 \pmod{n}. \end{aligned}$$

$x_2$ ist also die Lösung für den Fall $(a, b) = (0, 1)$. Wir multiplizieren beide Kongruenzen mit einer Zahl $b$ und erhalten

$$\begin{aligned} bx_2 &\equiv 0 \pmod{m} \\ bx_2 &\equiv b \pmod{n}. \end{aligned}$$

$bx_2 = bm'm$ ist also die Lösung für Paare der Form $(0, b)$.

Nun ist es einfach den allgemeinen Fall

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

zu lösen: wir setzen $x_0 = an'n + bm'm$. Dann gilt

$$\begin{aligned} x_0 = an'n + bm'm &\equiv a + 0 \equiv a \pmod{m} \\ x_0 = an'n + bm'm &\equiv 0 + b \equiv b \pmod{n}. \end{aligned}$$

Damit habe wir auch eine Lösung in $\mathbb{Z}_{mn}$, indem wir $x = x_0 \bmod mn$ setzen: es gilt

$$x \bmod m = (x_0 \bmod mn) \bmod m = x_0 \bmod m = a,$$

und analog $x \bmod n = b$.

Diese Lösung ist außerdem eindeutig auf $\mathbb{Z}_{mn}$. Dazu betrachten wir wie oben im Beispiel die Funktion $f$ mit

$$f: \ x \in Z_{mn} \mapsto (x \bmod m, x \bmod n) \in \mathbb{Z}_m \times \mathbb{Z}_n$$

Wie wir gerade gesehen haben gibt es zu jedem Paar $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ eine Lösung $x \in \mathbb{Z}_{mn}$. D.h. die Funktion $f$ ist surjektiv. $f$ ist auch injektiv und damit bijektiv, da der Definitionsbereich $\mathbb{Z}_{mn}$ genau so viele Elemente hat wie der Wertebereich: $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$. Zu jedem Paar $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ gibt es also *genau eine* Lösung $x \in \mathbb{Z}_{mn}$. Wir fassen zusammen:

**Theorem 7.23** (Chinesischer Restsatz) *Sei $m \perp n$. Für $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$ haben die beiden Konguenzen*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

*die eindeutige gemeinsame Lösung $x = (an'n + bm'm) \bmod mn \in \mathbb{Z}_{mn}$. Folglich ist die Funktion*

$$f: \ x \in Z_{mn} \mapsto (x \bmod m, x \bmod n) \in \mathbb{Z}_m \times \mathbb{Z}_n$$

*bijektiv.*

Eine Anwendung des chinesischen Restsatzes ist, dass man eine Rechnung mit großen Zahlen auf mehrere Rechnungen auf kleinen Zahlen ausführen kann. Soll ein Produkt $xy$ in $\mathbb{Z}_{mn}$ berechnet werden, so kann man stattdessen die Komponenten von $f(x)$ und $f(y)$ multiplizieren, und erhält

$$((x \bmod m) \cdot (y \bmod m), (x \bmod n) \cdot (y \bmod n)).$$

D.h. man berechnet zwei Produkte, dafür aber auf kleineren Zahlen. Aus dem berechneten Paar bekommt man dann das eigentlich Ergebnis. Betrachten wir nochmal das Beispiel mit $m = 2$ und $n = 3$. Um zum Beispiel 2 mit 5 zu multiplizieren, nehmen wir die Zerlegung in Komponenten $f(2) = (0, 2)$ und $f(5) = (1, 2)$. Dann multiplizieren wir komponentenweise $0 \cdot 1 \bmod 2 = 0$ und $2 \cdot 2 \bmod 3 = 1$. Das Paar $(0, 1)$ entspricht dem Ergebnis $4 = 2 \cdot 5 \bmod 6$.

Wir betrachten noch den Fall, dass $a$ und $b$ teilerfremd zu $m$ bzw. $n$ ist, also $a \in \mathbb{Z}_m^*$ und $b \in \mathbb{Z}_n^*$. Da $x \equiv a \bmod m$, ist nach Folgerung 7.21 auch die Lösung $x \in \mathbb{Z}_m^*$. Analog folgt folgt aus $x \equiv b \bmod m$, dass $x \in \mathbb{Z}_n^*$. Aus $x \perp m$ und $x \perp n$ folgt $x \perp mn$, also $x \in \mathbb{Z}_{mn}^*$. Analog gilt die Umkehrung: ist $x \in \mathbb{Z}_{mn}^*$, dann gilt für das zugehörige Paar $(a, b)$, dass $a \in \mathbb{Z}_m^*$ und $b \in \mathbb{Z}_n^*$ ist. Nach Theorem 7.23 ist die Lösung eindeutig.

**Theorem 7.24** *Sei $m \perp n$. Für $a \in \mathbb{Z}_m^*$ und $b \in \mathbb{Z}_n^*$ haben die beiden Konguenzen*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

*die eindeutige gemeinsame Lösung $x = (an'n + bm'm) \bmod mn \in \mathbb{Z}_{mn}^*$.*

Da die Lösung eindeutig ist, muss folglich die Abbildung

$$x \in \mathbb{Z}_{mn}^* \mapsto (x \bmod m, x \bmod n) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$

bijektiv sein. Insbesondere haben also $Z_{mn}^*$ und $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ gleichviele Elemente,

$$|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*|.$$

**Folgerung 7.25** *Für* $m \perp n$ *ist* $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*|$.

## 7.7 Die eulersche $\varphi$-Funktion

Die Anzahl der zu einer Zahl $m$ teilerfremden Zahlen in $\mathbb{Z}_m$ wird als die *eulersche* $\varphi$*-Funktion* bezeichnet,

$$\varphi(n) = |\mathbb{Z}_m^*|.$$

Anhand der Beispiele auf Seite 18 haben wir

| $n$ | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| $\varphi(n)$ | 1 | 2 | 2 | 4 | 2 |

Ist $p$ eine Primzahl, dann ist $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ und folglich $\varphi(p) = p - 1$. Für alle zusammen gesetzten Zahlen $m$ ist $\varphi(m) < m - 1$.

Wir betrachten zuerst den Fall, dass $m$ eine Primzahl-Potenz ist, $m = p^k$, für $p$ prim und $k \geq 1$. Die Zahlen, die *nicht* teilerfremd zu $m$ sind, sind genau die Vielfachen von $p$, da $p$ der einzige Primfaktor von $m = p^k$ ist. Das größte Vielfache von $p$ das kleiner $m$ ist, ist $p^k - p = (p^{k-1} - 1)p$. Es gilt also

$$\mathbb{Z}_m - \mathbb{Z}_m^* = \{0, p, 2p, 3p, \ldots, (p^{k-1} - 1)p\}.$$

Dies sind $p^{k-1}$ Zahlen. Folglich erhalten wir

$$\varphi(m) = |\mathbb{Z}_m^*| = |\mathbb{Z}_m| - p^{k-1} = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Im Allgemeinen ist $m$ ein Produkt mehrerer Primzahl-Potenzen, $m = p_1^{k_1} \cdots p_t^{k_t}$, für paarweise verschiedene Primzahlen $p_1, \cdots, p_t$. Da verschiedene Primzahlen zueinander teilerfremd sind, können wir nun Folgerung 7.25 mehrfach anwenden:

$$\begin{aligned}
\varphi(m) &= \left|\mathbb{Z}^*_{p_1^{k_1} \cdots p_t^{k_t}}\right| \\
&= \left|\mathbb{Z}^*_{p_1^{k_1}}\right| \cdots \left|\mathbb{Z}^*_{p_t^{k_t}}\right| \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdots\ p_t^{k_t}\left(1 - \frac{1}{p_t}\right) \\
&= p_1^{k_1} \cdots p_t^{k_t} \quad \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right) \\
&= m \prod_{p \setminus m} \left(1 - \frac{1}{p}\right)
\end{aligned}$$

Damit können wir $\varphi(m)$ berechnen, wenn wir die Primfaktor-Zerlegung von $m$ kennen. Z.B. für $m = 1000 = 2^3 \cdot 5^3$ erhalten wir

$$\varphi(1000) = 1000 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400.$$

Es gibt also 400 Zahlen $< 1000$ die zu 1000 teilerfremd sind.

$\varphi(m)$ gibt die Anzahl der Zahlen in $\mathbb{Z}_m$ an, deren größter gemeinsamer Teiler mit $m$ gleich 1 ist. Etwas allgemeiner fragen wir, wieviele Zahlen in $\mathbb{Z}_m$ den größten gemeinsamen Teiler $d$ mit $m$ haben. Wir definieren also die Menge

$$\mathbb{Z}_m^d = \{\, a \in \mathbb{Z}_m \mid \mathrm{ggT}(a, m) = d \,\}$$

und fragen nach deren Mächtigkeit. Für $d = 1$ erhalten wir $\mathbb{Z}_m^1 = \mathbb{Z}_m^*$. Wir können uns auf die Mengen $\mathbb{Z}_m^d$ beschränken, bei denen $d$ Teiler von $m$ ist, andernfalls ist $\mathbb{Z}_m^d$ leer. Offensichtlich sind die Mengen $\mathbb{Z}_m^d$ für verschiedene Werte von $d$ disjunkt, $\mathbb{Z}_m^d \cap \mathbb{Z}_m^{d'} = \emptyset$ für $d \neq d'$. Wenn wir die Mengen $\mathbb{Z}_m^d$ vereinigen erhalten wir $\mathbb{Z}_m$,

$$\bigcup_{d \backslash m} \mathbb{Z}_m^d = \mathbb{Z}_m.$$

Die Mengen $\mathbb{Z}_m^d$, für $d \backslash m$, bilden also eine Partition von $\mathbb{Z}_m$.

Sei nun $a \in \mathbb{Z}_m^d$, also $\mathrm{ggT}(a, m) = d$. Dann können wir $a$ und $m$ schreiben als $a = bd$ und $m = nd$. Außerdem müssen $b$ und $n$ teilerfremd sein, da sonst $d$ nicht der ggT von $a$ und $m$ wäre, und es ist $b < n$, da $a < m$ ist. Folglich ist $b \in \mathbb{Z}_n^*$. Umgekehrt ist für jedes $c \in \mathbb{Z}_n^*$ die Zahl $cd \in \mathbb{Z}_m^d$. Damit ist die Abbildung $x \mapsto dx$ eine Bijektion von $\mathbb{Z}_n^*$ auf $\mathbb{Z}_m^d$. Da $n = m/d$ ist, erhalten wir

$$\left|\mathbb{Z}_m^d\right| = \varphi\left(\frac{m}{d}\right).$$

Mit Hilfe der eulerschen $\varphi$-Funktion können wir also auch die Mächtigkeit der Mengen $\mathbb{Z}_m^d$ angeben. Da diese eine Partition von $\mathbb{Z}_m$ bilden, erhalten wir damit die Gleichung

$$m = |\mathbb{Z}_m| = \left|\bigcup_{d \backslash m} \mathbb{Z}_m^d\right| = \sum_{d \backslash m} \left|\mathbb{Z}_m^d\right| = \sum_{d \backslash m} \varphi\left(\frac{m}{d}\right).$$

In der letzten Summe durchläuft $d$ alle Teiler von $m$. Dabei durchlaufen die Werte $m/d$ ebenfalls alle Teiler von $m$, lediglich in umgekehrter Reihenfolge. Damit erhalten wir die Gleichung

$$\sum_{d \backslash m} \varphi(d) = m.$$

Wir testen die Gleichung für $m = 6$.

| $d$ | 1 | 2 | 3 | 6 |
|---|---|---|---|---|
| $\varphi(d)$ | 1 | 1 | 2 | 2 |

In der Tat ergibt die Summe der $\varphi$-Werte in der unteren Zeile 6.

## 7.8 Public-Key Kryptographie

Ronald Rivest, Adi Shamir und Leonard Adleman entwickelten 1977 das erste *public-key* Verschlüsselungsverfahren vor, das *RSA-Kryptosystem*. Im Gegensatz zu klassischen Kryptosystemen konnte hier der Schlüssel öffentlicht bekannt gemacht werden, mit dem Nachrichten verschlüsselt wurden. Eine Revolution in der Kryptographie. Wir wollen das Verfahren beschreiben.

### Die Vorbereitung

Eine Person, *Alice*, die das RSA-System benützten will, geht wie folgt vor:

1. Wähle zwei große Primzahlen $p$ und $q$ (typischerweise etwa 100-stellig in Dezimaldarstellung), und setze $n = pq$. Dann ist $\varphi(n) = (p-1)(q-1)$.

2. Wähle eine große Zufallszahl $d$, so dass $d \perp \varphi(n)$. Berechne das Inverse $e$ von $d$ modulo $\varphi(n)$. Es gilt also
$$ed \equiv 1 \pmod{\varphi(n)}.$$

Anders geschrieben gilt also für ein $k \in \mathbb{Z}$

$$ed = k\varphi(n) + 1 = k(p-1)(q-1) + 1\,. \tag{7.12}$$

Die Zahlen $e$ und $n$ sind der *öffentliche Schlüssel* von Alice, d.h. $e$ und $n$ kommen wie die Telefonnummer in ein öffentliches Schlüsselverzeichnis. Mit $e$ und $n$ kann man Nachrichten an Alice verschlüsseln (*encrypt*).

Die Zahl $d$ ist der *private Schlüssel* von Alice, d.h., $d$ ist nur Alice bekannt. Mit $d$ kann Alice Nachrichten entschlüsseln (*decrypt*), die mit $e$ verschlüsselt wurden.

### Das Protokoll

Will Bob eine geheime Nachricht $m \in Z_n$ (*message*) an Alice schicken, so schlägt er im Schlüsselverzeichnis den öffentlichen Schlüssel $(e, n)$ von Alice nach. Dann geht er wie folgt vor:

1. Bob berechnet den Geheimtext $c$ (*cyphertext*) $c = m^e \bmod n$, und schickt $c$ über einen öffentlichen Kanal an Alice.

2. Alice berechnet $c^d \bmod n$.

### Die Korrektheit

Alice erhält also $c^d \equiv m^{ed} \bmod n$. Wir zeigen, dass dies der Orginaltext $m$ ist, also dass gilt

$$m^{ed} \equiv m \pmod{n}\,.$$

Im Exponent $ed$ steckt gemäß Gleichung (7.12) die eulersche $\varphi$-Funktion $\varphi(n)$. Nach der eulerschen Formel ist $m^{\varphi(n)} \equiv 1 \pmod{n}$. Mit der erhalten wir

$$\begin{aligned} m^{ed} &= m^{k\varphi(n)+1} \\ &= \left(m^{\varphi(n)}\right)^k m \\ &\equiv m \pmod{n}. \end{aligned}$$

An dieser Rechnung sieht man sehr schön die Idee, die dem Verfahren zu Grunde liegt. Allerdings hat sie den Nachteil, dass sie nicht für alle $m \in \mathbb{Z}_n$ gilt, da die eulersche Formel nur für $m \perp n$ anwendbar ist.

Das Verfahren ist aber in der Tat für alle $m$ korrekt. Um dies zu sehen machen wir im Prinzip die gleiche Rechnung wie oben, aber nicht modulo $n$, sondern einmal modulo $p$ und einmal modulo $q$.

Nach der fermatschen Formel ist $m^{p-1} \equiv 1 \pmod{p}$. Damit erhalten wir nach Gleichung (7.12)

$$\begin{aligned} m^{ed} &= m^{k(p-1)(q-1)+1} \\ &= (m^{p-1})^{k(q-1)} m \\ &\equiv m \pmod{p}. \end{aligned}$$

Allerdings haben wir auch hier eine Einschränkung, da die fermatsche Formel nur für $m \not\equiv 0 \pmod{p}$ gilt. Aber der Fall $m \equiv 0 \pmod{p}$ ist trivial:

$$m^{ed} \equiv 0 \equiv m \pmod{p}.$$

Analog zeigt man, dass $m^{ed} \equiv m \pmod{q}$.

Es gilt also $p \backslash (m^{ed} - m)$ und $q \backslash (m^{ed} - m)$. Folglich gilt auch $n \backslash (m^{ed} - m)$, und damit $m^{ed} \equiv m \pmod{n}$. D.h. Alice erhält in der Tat die Nachricht $m$, für alle $m \in \mathbb{Z}_n$.

### Die Sicherheit

Das System kann gebrochen werden, wenn man es schafft aus $e$ und $n$ den geheimen Schlüssel $d$ auszurechnen. Der einzige bekannte Weg ist der oben benützte: berechne $d$ als das Inverse von $e$ modulo $\varphi(n)$. Dazu braucht man also $\varphi(n) = (p-1)(q-1)$ .

Es sieht so aus, als ob kein Weg daran vorbeiführt, zunächst die Primfaktoren $p$ und $q$ von $n$ zu berechnen. Für dieses sog. *Faktorisierungsproblem* kennt man bis heute keine effizienten Algorithmen! Auch die nach momentanem Stand schnellsten Algorithmen auf den schnellsten Rechnern brauchen Jahre um eine 200-stellige Zahl zu faktorisieren.

Das bedeutet aber auch: wenn jemand einen effizienten Faktorisierungs-Algorithmus entwickelt, kann er das RSA-System brechen. Außerdem konnte bis heute niemand nachweisen, dass der gerade beschriebene Weg wirklich die einzige Möglichkeit ist das RSA-System zu brechen. Es wäre also immer noch denkbar, dass man über andere Wege als Faktorisierung die Nachricht berechnen kann.

Ein Beweis dafür, dass RSA-System sicher ist, oder ein Beweis dafür, dass es keine effizienten Faktorisierungs-Algorithmus gibt, das sind extrem harte Nüsse deren Lösung momentan nicht in unserer Reichweite zu sein scheinen. Was aber evtl. machbar ist, ist ein Nachweis,

dass die beiden Problem *gleich schwer* sind. Wir haben bereits gesehen, dass man das RSA-System brechen kann, wenn man effizient Faktorisieren kann. Das kann man interpretieren als: RSA ist leichter als Faktorisieren, oder zumindest nicht schwieriger. Die Umkehrung davon ist:

**Offenes Problem:**
Wenn man das RSA-System brechen kann, kann man dann effizient Faktorisieren?

Das kann man dann interpretieren als: Faktorisieren ist leichter als RSA, oder zumindest nicht schwieriger. Zusammengenommen wären die beiden Probleme dann gleich schwer zu lösen. Damit könnte man dann sicher sein, dass es keine „Hintertür“ für das RSA-System gibt: wer RSA brechen will *muss* faktorisieren! Eine positive Lösung von obigem Problem wäre daher ein wichtiger Schritt zur Einschätzung der Sicherheit des RSA-Systems.