KAPITEL 1

Zahlentheoretische Grundlagen

Die Vorlesung setzt Grundkenntnisse der

- natürlichen Zahlen ($\mathbb{N} = \{1, 2, 3, \dots\}$ $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\} = \mathbb{N} \cup \{0\}$),
- ganzen Zahlen ($\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$),
- rationalen Zahlen ($\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$),
- reellen Zahlen ($\mathbb{R}$),
- komplexen Zahlen ($\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$)

voraus. Für Teilmengen $M \subseteq \mathbb{R}$ und $c \in \mathbb{R}$ sind folgende Schreibweisen nützlich:

$$M_{\geq c} = \{m \in M : m \geq c\},$$

und ganz analog $M_{>c}$, $M_{\leq c}$, $M_{<c}$. Beispielsweise ist dann

$$\mathbb{N} = \mathbb{Z}_{>0} = \mathbb{Z}_{\geq 1} \quad \text{und} \quad \mathbb{N}_0 = \mathbb{Z}_{\geq 0}.$$

Achtung: In der Vorlesung beginnt $\mathbb{N}$ mit 1, es gibt aber auch Bücher, in denen die natürlichen Zahlen mit der 0 beginnen.

Eine wichtige Funktion, die jeder reellen Zahl eine ganze Zahl zuordnet, ist folgende:

Definition (Abrundungsfunktion, floor function). *Für $a \in \mathbb{R}$ sei $\lfloor a \rfloor$ die größte ganze Zahl, die $\leq a$ ist, also*

$$\lfloor a \rfloor = \max\{n \in \mathbb{Z} : n \leq a\}.$$

(Es gilt dann $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$. Im Fall $a \geq 0$ erhält man $\lfloor a \rfloor$ durch Abschneiden des Nachkommaanteils von a.)

Die Funktion wurde von Gauß eingeführt, aber mit der Schreibweise $[x]$, und ist deshalb auch als **Gauß-klammer** bekannt.

Beispiele:

$$\lfloor 3.1 \rfloor = 3, \quad \lfloor 3.99 \rfloor = 3, \quad \lfloor -3.1 \rfloor = -4, \quad \lfloor -3.99 \rfloor = -4.$$

1. Division mit Rest

Ganze Zahlen kann man addieren, subtrahieren, multiplizieren, wobei eine Reihe von Gesetzmäßigkeiten erfüllt sind, wie beispielsweise die Assoziativität und Kommutativität von Addition und Multiplikation und Distributivgesetze.
Außerdem gibt es für natürliche Zahlen die **Division mit Rest (Teilen mit Rest)**: Teilt man $a \in \mathbb{N}_0$ durch $b \in \mathbb{N}$, so erhält man einen Quotienten $q \in \mathbb{N}_0$ und einen Rest $r \in \mathbb{N}_0$, also

$$a : b = q \text{ Rest } r,$$

wobei der Rest kleiner als b ist. Mathematisch kann man dies auch in der Form

$$a = qb + r \quad \text{mit} \quad q, r \in \mathbb{N}_0 \quad \text{und} \quad 0 \leq r < b$$

schreiben.

Beispiel: Wir teilen 12345 durch 987 nach dem in der Schule gelernten Verfahren:

$$\begin{array}{rrrrrcrrrcrr}
1 & 2 & 3 & 4 & 5 & : & 9 & 8 & 7 & = & 1 & 2 \\
- & - & - & - & & & & & & & & \\
1 & 2 & 3 & 4 & & & & & & & & \\
- & 9 & 8 & 7 & & & & & & & & \\
- & - & - & - & & & & & & & & \\
 & 2 & 4 & 7 & 5 & & & & & & & \\
- & 1 & 9 & 7 & 4 & & & & & & & \\
 & - & - & - & - & & & & & & & \\
 & & 5 & 0 & 1 & & & & & & &
\end{array}$$

12345 durch 987 ergibt also 12 Rest 501. Es ist also

$$12345 = 12 \cdot 987 + 501.$$

Das folgende Lemma gibt eine mathematische Charakterisierung der Division mit Rest, wobei wir etwas allgemeiner den Fall $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ betrachten:

LEMMA. *Zu $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = q \cdot b + r \quad \textit{und} \quad 0 \le r < b.$$

Es ist

$$q = \left\lfloor \frac{a}{b} \right\rfloor \quad \textit{und} \quad r = a - \left\lfloor \frac{a}{b} \right\rfloor b.$$

Beweis:

(1) Wir zeigen zunächst, dass q und r durch die angegebenen Bedingungen eindeutig bestimmt sind. Sei also $a = qb + r$ mit $0 \le r \le b - 1$. Dann folgt $\frac{a}{b} = q + \frac{r}{b}$ und wegen $0 \le r < b$

$$q \le q + \frac{r}{b} < q + \frac{b}{b} = q + 1.$$

Dann ist aber

$$q = \left\lfloor q + \frac{r}{b} \right\rfloor = \left\lfloor \frac{a}{b} \right\rfloor \quad \text{und} \quad r = a - qb = a - \left\lfloor \frac{a}{b} \right\rfloor b,$$

was die Eindeutigkeit der Darstellung beweist.

(2) Nun zeigen wir, dass $q = \left\lfloor \frac{a}{b} \right\rfloor$ und $r = a - \left\lfloor \frac{a}{b} \right\rfloor b$ die angegebenen Bedingungen erfüllen. Die Gleichung $a = qb + r$ ist nach Definition von r erfüllt. Wir müssen noch zeigen, dass $0 \le r < b$ gilt. Aus $q = \left\lfloor \frac{a}{b} \right\rfloor$ folgt

$$q \le \frac{a}{b} < q + 1, \quad \text{und damit} \quad qb \le a < qb + b.$$

Subtrahiert man qb, so ergibt sich

$$0 \le a - qb < b, \quad \text{also} \quad 0 \le r < b,$$

wie behauptet. ■

Bemerkung: Sind $b, r \in \mathbb{Z}$ mit $r < b$, so gilt $b - r > 0$, also $b - r \in \mathbb{Z}_{>0} = \mathbb{Z}_{\ge 1}$ und damit $b - r \ge 1$, was man auch in der Form $r \le b - 1$ schreiben kann. Nochmals:

$$b, r \in \mathbb{Z} \text{ und } r < b \quad \Longrightarrow \quad r \le b - 1.$$

Die Bedingungen

$$a = qb + r \quad \text{und} \quad 0 \le r < b$$

kann man daher auch in der Form

$$a = qb + r \quad \text{und} \quad 0 \le r \le b - 1$$

schreiben.

Für den Divisionsrest r hat sich eine eigene Bezeichnung eingebürgert:

DEFINITION. *Für $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ wird „a modulo b“ definiert als*

$$a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b.$$

Für $a \in \mathbb{Z}$, $b \in \mathbb{N}$ ist also

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + (a \bmod b) \quad \text{und} \quad 0 \leq (a \bmod b) \leq b - 1.$$

Beispiele:

$$17 \bmod 4 = 1, \quad 37 \bmod 5 = 2, \quad 49 \bmod 6 = 1.$$

Bemerkungen:

(1) Leider taucht die Bezeichung „mod“ in der Vorlesung in zwei Bedeutungen auf. In der obigen Definition ist „mod“ eine Funktion

$$\bmod : \mathbb{Z} \times \mathbb{N} \to \mathbb{N}_0, \quad (a, b) \mapsto a - \left\lfloor \frac{a}{b} \right\rfloor b,$$

die aber traditionell in der Form „$a \bmod b$“ geschrieben wird. Um $a \bmod b$ als Funktionswert zu kennzeichnen schreiben wir auch manchmal $(a \bmod b)$.

(2) Statt $a \bmod b$ findet sich auch mitunter die Schreibweise $a\%b$, also

$$a\%b = a \bmod b.$$

für $a \bmod b$.

(3) In Python und SAGE erhält man für $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ den Rest $(a \bmod b)$ als `a%b` und den Quotienten $\left\lfloor \frac{a}{b} \right\rfloor$ als `a//b`. Daneben kennt SAGE auch `mod(a,b)`.

(4) Wir werden später in der Vorlesung sogenannte „euklidische Ringe“ behandeln. Wir werden sehen, dass die Division mit Rest die ganzen Zahlen zu einem euklidischen Ring macht.

Die folgende Regel kann für das Rechnen hilfreich sein:

LEMMA. *Für $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und $k \in \mathbb{Z}$ gilt*

$$a \bmod b = (a + kb) \bmod b.$$

(Man kann bei der Berechnung von $a \bmod b$ die Zahl a um ganzzahlige Vielfache von b abändern ohne den Rest $a \bmod b$ zu ändern.)

Beweis: Für $q = \left\lfloor \frac{a}{b} \right\rfloor$ gilt

$$a = q \cdot b + (a \bmod b).$$

Daraus ergibt sich

$$a + kb = (q + k) \cdot b + (a \bmod b).$$

Da $0 \leq (a \bmod b) < b$ gilt, folgt aus der Eindeutigkeitsaussage des vorangegangenen Lemmas sofort

$$(a + kb) \bmod b = a \bmod b,$$

wie behauptet. ■

Beispiele:

$$\begin{aligned} 2021 \bmod 7 &= (2021 - 2100) \bmod 7 = (-79) \bmod 7 = (84 - 79) \bmod 7 = 5 \bmod 7 = 5, \\ (-123) \bmod 7 &= (140 - 123) \bmod 7 = 17 \bmod 7 = (17 - 14) \bmod 7 = 3 \bmod 7 = 3. \end{aligned}$$

2. Teilbarkeit

DEFINITION. *Für $a, b \in \mathbb{Z}$ sagt man „a **teilt** b“ (oder „a ist ein **Teiler** von b“ oder „b ist ein **Vielfaches** von a“) und schreibt $a \mid b$, falls ein $c \in \mathbb{Z}$ existiert mit $b = ca$. Teilt a die Zahl b nicht, so schreibt man $a \nmid b$.*

Beispiele:

$$3|12, \quad -4 \mid 12, \quad 2 \nmid 3, \quad 77 \mid 0, \quad 1 \mid -1.$$

Der folgende Satz stellt einige Regeln für die Teilbarkeit zusammen:

SATZ. *Für $a, b, c \in \mathbb{Z}$ gilt:*

(1) *Teilbarkeit ist „bis aufs Vorzeichen“ eine Ordnungsrelation.*
   (a) $a \mid b \iff \pm a \mid \pm b \iff |a| \mid |b|$ *(Teilbarkeit hängt nicht vom Vorzeichen ab).*
   (b) $a \mid a$ *(Reflexivität).*
   (c) $a \mid b$ *und* $b \mid a \Longrightarrow b = \pm a$ *(Teilbarkeit ist bis aufs Vorzeichen antisymmetrisch).*
   (d) $a \mid b$ *und* $b \mid c \Longrightarrow a \mid c$ *(Transitivität).*

(2) *Eigenschaften der Zahl* 1.
   (a) $1 \mid a$.
   (b) $a \mid 1 \Longrightarrow a = \pm 1$.

(3) *Eigenschaften der Zahl* 0.
   (a) $a \mid 0$.
   (b) $0 \mid a \Longrightarrow a = 0$.

(4) *Allgemeine Eigenschaften*
   (a) $a \mid b$ *und* $a \mid c \Longrightarrow a \mid mb + nc$ *für alle* $m, n \in \mathbb{Z}$.
   (b) *Für* $a \neq 0$*:* $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$ *(Theoretischer Teilbarkeitstest).*
   (c) *Für* $a \neq 0$*:* $a \mid b \iff (b \mod a) = 0$ *(Praktischer Teilbarkeitstest).*
   (d) *Für* $a \neq 0$*:* $a \mid b \Longrightarrow \frac{b}{a} \in \mathbb{Z}$ *und* $\frac{b}{a} \mid b$.
   (e) *Für* $a \neq 0$*:* $b \mid c \iff ab \mid ac$.
   (f) *Für* $a \neq 0$*:* $a \mid b$ *und* $b \mid c \Longrightarrow \frac{b}{a}, \frac{c}{a} \in \mathbb{Z}$ *und* $\frac{b}{a} \mid \frac{c}{a}$.
   (g) *Für* $b \neq 0$*:* $a \mid b \Longrightarrow 1 \leq |a| \leq |b|$ *(Wichtig um nach den Teilern einer Zahl zu suchen).*

Beweis: Wir beweisen nur einige ausgewählte Eigenschaften.

(4b) Gilt $a \mid b$, so gibt es ein $c \in \mathbb{Z}$ mit $ac = b$. Wegen $a \neq 0$ ist $c = \frac{b}{a}$, also $\frac{b}{a} \in \mathbb{Z}$. Ist umgekehrt $\frac{b}{a} \in \mathbb{Z}$, so folgt aus $a \cdot \frac{b}{a} = b$ sofort $a \mid b$.

(4c) Gilt $a \mid b$, so gibt es ein $c \in \mathbb{Z}$ mit $ac = b$. Schreibt man $b = c \cdot a + 0$, so liefert die Eindeutigkeit der Division mit Rest sofort $(b \mod a) = 0$. Gilt umgekehrt $(b \mod a) = 0$, so folgt aus $b = \lfloor \frac{b}{a} \rfloor \cdot a + 0$ natürlich $a \mid b$.

(4d) Gilt $a \mid b$, so gibt es ein $c \in \mathbb{Z}$ mit $ac = b$. Dann ist $c = \frac{b}{a}$. Natürlich gilt dann $\frac{b}{a} = c \in \mathbb{Z}$ und $\frac{b}{a} \mid b$.

(4g) Es gelte $a \mid b$ mit $b \neq 0$. Dann gibt es ein $c \in \mathbb{Z}$ mit $ac = b$. Wegen $b \neq 0$ gilt auch $a, c \neq 0$, also $|a| \geq 1$, $|c| \geq 1$. Es folgt $|a| = \frac{|b|}{|c|} \leq \frac{|b|}{1} = |b|$.

Die andern Eigenschaften beweise man zur Übung. ■

3. Teilermengen, ggT und euklidischer Algorithmus

Da es bei der Teilbarkeit nicht auf das Vorzeichen ankommt, betrachten wir hier für eine ganze Zahl $n \in \mathbb{Z}$ nur die Menge der positiven Teiler:

$$T(n) = \{d \in \mathbb{N} : d \mid n\}.$$

Ein paar einfache Beobachtungen:

(1) Für $n \in \mathbb{Z}$ ist $T(n) = T(-n) = T(|n|)$.
(2) Für $d \in \mathbb{Z}$ und $n \neq 0$ gilt: $d \mid n \iff |d| \in T(n)$.

(3) $0 \mid n \iff n = 0$. Die einzige Zahl, die 0 als Teiler hat, ist 0 selbst, aber alle Zahlen teilen die 0, weswegen $T(0) = \mathbb{N}$ gilt.
(4) Für $n \geq 1$ gilt
$$\{1, n\} \subseteq T(n) \subseteq \{1, 2, 3, \ldots, n\}.$$
(5) Ist $n \geq 1$ und $d \in T(n)$, so gibt es ein $d' \in \mathbb{N}$ mit $n = dd'$. Dann ist auch $d' \in T(n)$. Also:
$$d \in T(n) \quad \Longrightarrow \quad \frac{n}{d} \in T(n).$$
(Man nennt d' auch manchmal den zu d **komplementären Teiler** von n.)

Beispiele:

a	$T(a)$
1	$\{1\}$
2	$\{1, 2\}$
3	$\{1, 3\}$
4	$\{1, 2, 4\}$
5	$\{1, 5\}$
6	$\{1, 2, 3, 6\}$
7	$\{1, 7\}$
8	$\{1, 2, 4, 8\}$
9	$\{1, 3, 9\}$
10	$\{1, 2, 5, 10\}$
11	$\{1, 11\}$
12	$\{1, 2, 3, 4, 6, 12\}$
13	$\{1, 13\}$
14	$\{1, 2, 7, 14\}$
15	$\{1, 3, 5, 15\}$

a	$T(a)$
16	$\{1, 2, 4, 8, 16\}$
17	$\{1, 17\}$
18	$\{1, 2, 3, 6, 9, 18\}$
19	$\{1, 19\}$
20	$\{1, 2, 4, 5, 10, 20\}$
21	$\{1, 3, 7, 21\}$
22	$\{1, 2, 11, 22\}$
23	$\{1, 23\}$
24	$\{1, 2, 3, 4, 6, 8, 12, 24\}$
25	$\{1, 5, 25\}$
26	$\{1, 2, 13, 26\}$
27	$\{1, 3, 9, 27\}$
28	$\{1, 2, 4, 7, 14, 28\}$
29	$\{1, 29\}$
30	$\{1, 2, 3, 5, 6, 10, 15, 30\}$

Wir wollen gemeinsame Teiler von Zahlen betrachten. Für $a, b \in \mathbb{Z}$ definieren wir den **größten gemeinsamen Teiler** von a und b durch
$$\mathrm{ggT}(a, b) = \begin{cases} \max(T(a) \cap T(b)) = \max\{d \in \mathbb{N} : d \mid a \text{ und } d \mid b\}, & \text{falls } (a, b) \neq (0, 0), \\ 0, & \text{falls } a = b = 0 \end{cases}$$
und für $a_1, \ldots, a_n \in \mathbb{Z}$
$$\mathrm{ggT}(a_1, a_2, \ldots, a_n) = \begin{cases} \max(T(a_1) \cap T(a_2) \cap \cdots \cap T(a_n)), & \text{falls } (a_1, a_2, \ldots, a_n) \neq (0, 0, \ldots, 0), \\ 0, & \text{falls } a_1 = a_2 = \cdots = a_n = 0. \end{cases}$$

Beispiele: Sei $a \in \mathbb{Z}$.
$$\begin{aligned} \mathrm{ggT}(6, 10) &= \max(T(6) \cap T(10)) = \max(\{1, 2, 3, 6\} \cap \{1, 2, 5, 10\}) = \max(\{1, 2\}) = 2, \\ \mathrm{ggT}(-6, 15) &= \max(T(-6), T(15)) = \max(\{1, 2, 3, 6\} \cap \{1, 3, 5, 15\}) = \max(\{1, 3\}) = 3, \\ \mathrm{ggT}(a, 1) &= \max(T(a) \cap T(1)) = \max(T(a) \cap \{1\}) = 1, \\ \mathrm{ggT}(a, 0) &= \max(T(a) \cap \mathbb{N}) = \max(\{1, \ldots, |a|\}) = |a|. \end{aligned}$$
(Die Beweisführung der letzten Formel gilt zunächst nur für $a \neq 0$. Das Ergebnis gilt aber auch für $a = 0$.)

Satz (Eigenschaften des ggT - I). *Seien $a, b, a_1, \ldots, a_n \in \mathbb{Z}$. Dann gilt:*
(1) $\mathrm{ggT}(a, b) = \mathrm{ggT}(\pm a, \pm b) = \mathrm{ggT}(|a|, |b|)$.
(2) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$.
(3) $\mathrm{ggT}(a, 1) = 1$.
(4) $\mathrm{ggT}(a, 0) = |a|$.
(5) $\mathrm{ggT}(a_1, a_2, \ldots, a_n) = \mathrm{ggT}(a_1, \mathrm{ggT}(a_2, \ldots, a_n))$ *(Man kann den ggT von mehr als zwei Elementen also rekursiv berechnen).*
(6) $\mathrm{ggT}(a, b) = \mathrm{ggT}(a + kb, b)$ *für alle $k \in \mathbb{Z}$ (Man kann a um ganzzahlige Vielfache von b abändern ohne den ggT zu ändern).*

(7) $T(a) \cap T(b) = T(a+kb) \cap T(b)$ *für alle* $k \in \mathbb{Z}$.

Beweis: Die Eigenschaften (1) bis (5) ergeben sich unmittelbar aus der Definition. Wir beweisen zunächst (7): Für $d \in \mathbb{N}$ gilt:

$$\begin{aligned} d \in T(a) \cap T(b) &\iff d \mid a, d \mid b \iff d \mid a, d \mid b, d \mid a+kb \iff d \mid b, d \mid a+kb \iff \\ &\iff d \in T(a+kb) \cap T(b). \end{aligned}$$

Daher gilt

$$T(a) \cap T(b) = T(a+kb) \cap T(b),$$

woraus natürlich auch

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(a+kb,b)$$

folgt. Damit sind auch die Eigenschaften (7) und (6) bewiesen. ■

Beispiel: Wir verwenden insbesondere die Regel (6) aus dem letzten Satz:

$$\begin{aligned} \mathrm{ggT}(27,20) &= \mathrm{ggT}(27-20,20) = \mathrm{ggT}(7,20) = \mathrm{ggT}(7,20-3\cdot 7) = \mathrm{ggT}(7,-1) = \\ &= \mathrm{ggT}(7+7\cdot(-1),-1) = \mathrm{ggT}(0,-1) = |-1| = 1. \end{aligned}$$

Bemerkung: Sind $a,b,q,r \in \mathbb{Z}$ mit $a = qb+r$, so erhält man mit der Eigenschaft (7) des vorangegangenen Satzes:

$$T(a) \cap T(b) = T(qb+r) \cap T(b) = T(r) \cap T(b) = T(b) \cap T(r).$$

Diese Eigenschaft führt zum euklidischen Algorithmus:

Satz (Euklidischer Algorithmus (Variante I)). *Seien $a,b \in \mathbb{N}_0$ gegeben. Rekursiv werden Zahlen $a_i \in \mathbb{N}_0$ definiert, wobei man mit $a_0 = a$ und $a_1 = b$ beginnt. Sind für einen Index $i \geq 0$ die Zahlen a_i und a_{i+1} bereits definiert, so unterscheidet man:*

- *Ist $a_{i+1} = 0$, so bricht man ab. (Es sei n der größte Index mit $a_{n+1} = 0$.)*
- *Ist $a_{i+1} > 0$, so dividiert man a_i durch a_{i+1} und erhält den Quotienten q_i und den Rest a_{i+2}. Dabei ist $a_{i+2} = a_i \bmod a_{i+1}$ und $0 \leq a_{i+2} < a_{i+1}$. (Wegen $0 \leq a_{i+2} < a_{i+1}$ hört das Verfahren nach endlich vielen Schritten auf.)*

Explizit ergibt sich das Schema (im Fall $a_1 > 0$):

$$\begin{aligned} a_0 &= q_0 a_1 + a_2 \quad \textit{mit} \quad 0 < a_2 < a_1, \\ a_1 &= q_1 a_2 + a_3 \quad \textit{mit} \quad 0 < a_3 < a_2, \\ &\vdots \\ a_i &= q_i a_{i+1} + a_{i+2} \quad \textit{mit} \quad 0 < a_{i+2} < a_{i+1}, \\ &\vdots \\ a_{n-2} &= q_{n-2} a_{n-1} + a_n \quad \textit{mit} \quad 0 < a_n < a_{n-1}, \\ a_{n-1} &= q_{n-1} a_n + 0. \end{aligned}$$

Dann gilt

$$\mathrm{ggT}(a,b) = a_n \quad \textit{und} \quad T(a) \cap T(b) = T(\mathrm{ggT}(a,b)).$$

(Die Zahl n nennt man auch die Anzahl der Schritte, die der Algorithmus zur Berechnung von $\mathrm{ggT}(a,b)$ braucht.)

Beweis: Aus $a_i = q_i a_{i+1} + a_{i+2}$ folgt mit der Vorbemerkung $T(a_i) \cap T(a_{i+1}) = T(a_{i+1}) \cap T(a_{i+2})$ und damit

$$T(a) \cap T(b) = T(a_0) \cap T(a_1) = T(a_1) \cap T(a_2) = \cdots = T(a_{n-1}) \cap T(a_n) = T(a_n) \cap T(0) = T(a_n).$$

Damit folgt dann $\mathrm{ggT}(a,b) = a_n$ und $T(a) \cap T(b) = T(\mathrm{ggT}(a,b))$. ■

Beispiele:

(1) Wir wollen ggT(12345, 987) berechnen:

$$\begin{aligned} 12345 &= 12 \cdot 987 + 501, \\ 987 &= 1 \cdot 501 + 486, \\ 501 &= 1 \cdot 486 + 15, \\ 486 &= 32 \cdot 15 + 6, \\ 15 &= 2 \cdot 6 + 3, \\ 6 &= 2 \cdot 3 + 0, \end{aligned}$$

also gilt ggT(12345, 987) = 3. Zum Vergleich:

$T(12345) = \{1, 3, 5, 15, 823, 2469, 4115, 12345\}$ und $T(987) = \{1, 3, 7, 21, 47, 141, 329, 987\}$.

(2) Was ist ggT(9264857236, 2453245253)? Mit 23 Divisonen ergibt sich

$$\begin{aligned} 9264857236 &= 3 \cdot 2453245253 + 1905121477 \\ 2453245253 &= 1 \cdot 1905121477 + 548123776 \\ 1905121477 &= 3 \cdot 548123776 + 260750149 \\ 548123776 &= 2 \cdot 260750149 + 26623478 \\ 260750149 &= 9 \cdot 26623478 + 21138847 \\ 26623478 &= 1 \cdot 21138847 + 5484631 \\ 21138847 &= 3 \cdot 5484631 + 4684954 \\ 5484631 &= 1 \cdot 4684954 + 799677 \\ 4684954 &= 5 \cdot 799677 + 686569 \\ 799677 &= 1 \cdot 686569 + 113108 \\ 686569 &= 6 \cdot 113108 + 7921 \\ 113108 &= 14 \cdot 7921 + 2214 \\ 7921 &= 3 \cdot 2214 + 1279 \\ 2214 &= 1 \cdot 1279 + 935 \\ 1279 &= 1 \cdot 935 + 344 \\ 935 &= 2 \cdot 344 + 247 \\ 344 &= 1 \cdot 247 + 97 \\ 247 &= 2 \cdot 97 + 53 \\ 97 &= 1 \cdot 53 + 44 \\ 53 &= 1 \cdot 44 + 9 \\ 44 &= 4 \cdot 9 + 8 \\ 9 &= 1 \cdot 8 + 1 \\ 8 &= 8 \cdot 1 + 0 \end{aligned}$$

Also ist der ggT 1.

Der ggT lässt sich mit dem euklidischen Algorithmus also sehr schnell berechnen. Daher wird dieser Algorithmus in der Praxis auch oft eingesetzt.

Bemerkung: Man kann auch theoretisch zeigen, dass der euklidische Algorithmus schnell ist: Um den ggT zweier natürlicher Zahl $a > b$ zu berechnen, braucht man mit dem euklidischen Algorithmus

$$\leq 4.785 \log_{10} a$$

Divisionen mit Rest.

Für die ggT-Berechnung braucht man im euklidischen Algorithmus die Quotienten q_i nicht, sofern man $a_i \bmod a_{i+1}$ anders als durch $a_i - \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor a_{i+1}$ berechnen kann. Man erhält dann folgende Variante:

SATZ (Euklidischer Algorithmus (Variante II)). *Seien $a, b \in \mathbb{N}_0$ gegeben. Rekursiv werden Zahlen $a_i \in \mathbb{N}_0$ definiert, wobei mit $a_0 = a$ und $a_1 = b$ begonnen wird. Sind für einen Index $i \geq 0$ die Zahlen a_i und a_{i+1} bereits definiert, so unterscheidet man:*

- *Ist $a_{i+1} = 0$, so bricht man ab. Es ist dann $\mathrm{ggT}(a, b) = a_i$.*
- *Ist $a_{i+1} > 0$, so definiert man $a_{i+2} = a_i \bmod a_{i+1}$.*

Explizit:

$$a_0, \quad a_1, \quad a_2 = a_0 \bmod a_1, \quad a_3 = a_1 \bmod a_2, \quad a_4 = a_2 \bmod a_3, \quad \ldots \quad a_{n+1} = a_{n-1} \bmod a_n = 0.$$

Dann ist

$$\mathrm{ggT}(a, b) = a_n.$$

Beweis: Ist $a_{i+1} > 0$, so ist $a_{i+2} = a_i \bmod a_{i+1}$, also

$$a_i = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor a_{i+1} + (a_i \bmod a_{i+1}) = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor a_{i+1} + a_{i+2},$$

und damit

$$\mathrm{ggT}(a_i, a_{i+1}) = \mathrm{ggT}(\left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor a_{i+1} + a_{i+2}, a_{i+1}) = \mathrm{ggT}(a_{i+2}, a_{i+1}) = \mathrm{ggT}(a_{i+1}, a_{i+2}).$$

Es folgt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_1, a_2) = \cdots = \mathrm{ggT}(a_{n-1}, a_n) = \mathrm{ggT}(a_n, a_{n+1}) = \mathrm{ggT}(a_n, 0) = a_n.$$

Beispiel: $a = 12345$, $b = 987$ liefern folgende Zahlenfolge a_i:

$$12345, \quad 987, \quad 501, \quad 486, \quad 15, \quad 6, \quad 3, \quad 0.$$

Startet man mit $a = 987$, $b = 12345$, so erhält man die Folge

$$987, \quad 12345, \quad 987, \quad 501, \quad 486, \quad 15, \quad 6, \quad 3, \quad 0.$$

Bemerkungen:

(1) Mit der wie folgt definierten Python-Funktion kann man $\mathrm{ggT}(a, b)$ für $a, b \in \mathbb{N}_0$ schnell berechnen:

```
def ggT(a,b):
  while b>0:
    a,b=b,a%b
  return a
```

(2) SAGE berechnet den ggT von a und b mit dem Befehl `gcd(a,b)`.

SATZ (Eigenschaften des ggT - II). *Seien $a, b, c, d \in \mathbb{Z}$. Dann gilt:*

(1) *Für $d \in \mathbb{Z}$ gilt die Äquivalenz*

$$d \mid a \text{ und } d \mid b \quad \Longleftrightarrow \quad d \mid \mathrm{ggT}(a, b).$$

(2) *Gilt für $g \in \mathbb{Z}$ die Äquivalenz*

$$d \mid a \text{ und } d \mid b \quad \Longleftrightarrow \quad d \mid g,$$

so ist

$$\mathrm{ggT}(a, b) = |g|.$$

(3) $\mathrm{ggT}(ab, ac) = |a| \, \mathrm{ggT}(b, c)$.

Beweis:

(1) Dies folgt sofort aus $T(a) \cap T(b) = T(\mathrm{ggT}(a, b))$.

(2) Erfüllt g die angegebene Eigenschaft, so folgt die Äquivalenz

$$d \in T(\mathrm{ggT}(a,b)) \quad \Longleftrightarrow \quad d \in T(a) \cap T(b) \quad \Longleftrightarrow \quad d \in T(g),$$

also $T(\mathrm{ggT}(a,b)) = T(g)$. Im Fall $(a,b) = (0,0)$ folgt $g = 0$, andernfalls ist

$$|g| = \max T(g) = \max T(\mathrm{ggT}(a,b)) = \mathrm{ggT}(a,b).$$

(3) Da im Fall $a = 0$ die Aussage richtig ist, können wir nun $a \neq 0$ voraussetzen. Aus $a \mid ab$ und $a \mid ac$ folgt $a \mid \mathrm{ggT}(ab, ac)$, also gibt es ein $g \in \mathbb{Z}$ mit $\mathrm{ggT}(ab, ac) = ag$. Für $d \in \mathbb{Z}$ gilt die Äquivalenz:

$$d \mid b \text{ und } d \mid c \quad \Longleftrightarrow \quad ad \mid ab \text{ und } ad \mid ac \quad \Longleftrightarrow \quad ad \mid \mathrm{ggT}(ab, ac) \quad \Longleftrightarrow$$
$$\Longleftrightarrow \quad ad \mid ag \quad \overset{a \neq 0}{\Longleftrightarrow} \quad d \mid g.$$

Die Charakterisierung in (2) liefert

$$\mathrm{ggT}(b,c) = |g| = |\frac{\mathrm{ggT}(ab,ac)}{a}| = \frac{\mathrm{ggT}(ab,ac)}{|a|},$$

woraus die Behauptung folgt. ■

4. Der erweiterte euklidische Algorithmus

Der folgende Satz gibt eine wichtige Eigenschaft des ggT an, die sowohl theoretisch als auch praktisch oft benutzt wird:

SATZ. *Zu $a, b \in \mathbb{Z}$ gibt es $x, y \in \mathbb{Z}$ mit*

$$\mathrm{ggT}(a,b) = xa + yb.$$

Der nachfolgende Satz gibt einen konstruktiven Beweis der Aussage.

Bemerkungen:

(1) Manchmal kann man auf den ersten Blick eine Lösung der Gleichung $xa + yb = \mathrm{ggT}(a,b)$ sehen. Beispielsweise gilt für $a = 27$, $b = 13$

$$1 \cdot 27 - 2 \cdot 13 = 1,$$

woraus dann auch $\mathrm{ggT}(27, 13) = 1$ folgt.

(2) Gilt $\mathrm{ggT}(a,b) = xa + yb$, so gilt offensichtlich für alle $k \in \mathbb{Z}$

$$\mathrm{ggT}(a,b) = (x + kb)a + (y - ka)b.$$

(3) Wendet man den euklidischen Algorithmus auf $a = a_0$ und $b = a_1$ an, so erhält man das folgende Schema:

$$\begin{aligned}
a_0 &= q_0 a_1 + a_2 \quad \text{mit} \quad 0 < a_2 < a_1,\\
a_1 &= q_1 a_2 + a_3 \quad \text{mit} \quad 0 < a_3 < a_2,\\
&\vdots\\
a_i &= q_i a_{i+1} + a_{i+2} \quad \text{mit} \quad 0 < a_{i+2} < a_{i+1},\\
&\vdots\\
a_{n-2} &= q_{n-2} a_{n-1} + a_n \quad \text{mit} \quad 0 < a_n < a_{n-1},\\
a_{n-1} &= q_{n-1} a_n + 0 \quad \text{mit} \quad a_{n+1} = 0.
\end{aligned}$$

Dann ist $a_n = \mathrm{ggT}(a,b)$. Man kann nun beginnend mit der vorletzten Zeile durch sukzessives Eliminieren a_n als Linearkombination von a_0 und a_1 schreiben, also $x, y \in \mathbb{Z}$ finden mit $a_n = xa_0 + ya_1$. Ist n klein, funktioniert dies auch praktisch.

Beispiel: Für 10 und 7 liefert der euklidische Algorithmus das Schema

$$\begin{aligned} 10 &= 1 \cdot 7 + 3, \\ 7 &= 2 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Beginnend mit der vorletzten Zeile folgt

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (10 - 1 \cdot 7) = -2 \cdot 10 + 3 \cdot 7.$$

Eine systematischere Vorgehensweise liefert der erweiterte euklidische Algorithmus.

SATZ (Erweiterter euklidischer Algorithmus). *Seien $a, b \in \mathbb{N}_0$. Man definiert rekursiv Zahlenfolgen q_i, a_i, x_i, y_i durch folgende Vorschrift:*

- *$a_0 = a$, $a_1 = b$, $x_0 = 1$, $x_1 = 0$, $y_0 = 0$, $y_1 = 1$.*
- *Sind $a_i, a_{i+1}, x_i, x_{i+1}, y_i, y_{i+1}$ bereits definiert, so unterscheidet man:*
  - *Ist $a_{i+1} = 0$, so endet die Konstruktion.*
  - *Ist $a_{i+1} > 0$, so definiert man*

$$q_i = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor \quad \text{und} \quad a_{i+2} = a_i \bmod a_{i+1} \ (\text{oder } a_{i+2} = a_i - q_i a_{i+1})$$

und

$$x_{i+2} = x_i - q_i x_{i+1} \quad \text{und} \quad y_{i+2} = y_i - q_i y_{i+1}.$$

Ist $n \in \mathbb{N}_0$ der Index mit $a_{n+1} = 0$, so kann man die Vorgehensweise in folgender Tabelle zusammenfassen:

	a_0	$x_0 = 1$	$y_0 = 0$
	a_1	$x_1 = 0$	$y_1 = 1$
$q_0 = \left\lfloor \frac{a_0}{a_1} \right\rfloor$	$a_2 = a_0 - q_0 a_1$	$x_2 = x_0 - q_0 x_1$	$y_2 = y_0 - q_0 y_1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$*$	a_i	x_i	y_i
$*$	a_{i+1}	x_{i+1}	y_{i+1}
$q_i = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor$	$a_{i+2} = a_i - q_i a_{i+1}$	$x_{i+2} = x_i - q_i x_{i+1}$	$y_{i+2} = y_i - q_i y_{i+1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$*$	a_{n-1}	x_{n-1}	y_{n-1}
$*$	a_n	x_n	y_n
$q_{n-1} = \left\lfloor \frac{a_{n-1}}{a_n} \right\rfloor = \frac{a_{n-1}}{a_n}$	$a_{n+1} = 0$	x_{n+1}	y_{n+1}

Dann gilt

$$a_i = x_i a + y_i b \text{ für } 0 \le i \le n+1,$$

und insbesondere

$$\mathrm{ggT}(a, b) = a_n \quad \text{und} \quad \mathrm{ggT}(a, b) = x_n a + y_n b.$$

Beweis:

(1) Die Aussage $\mathrm{ggT}(a, b) = a_n$ haben wir schon beim euklidischen Algorithmus gezeigt.

(2) Wir denken uns die Zeilen der Tabelle von 0 bis $n+1$ nummeriert. Wir zeigen durch Induktion, dass

$$a_i = x_i a + y_i b \text{ für } i = 0, \ldots, n+1$$

gilt. Für $i = 0$ und $i = 1$ folgt dies aus der Definition von x_0, y_0, x_1, y_1. Ist nun $i \ge 0$ und die Aussage bereits für i und $i+1$ gezeigt, also

$$\begin{aligned} a_i &= x_i a + y_i b, \\ a_{i+1} &= x_{i+1} a + y_{i+1} b, \end{aligned}$$

so folgt sofort

$$\begin{aligned} x_{i+2}a + y_{i+2}b &= (x_i - q_i x_{i+1})a + (y_i - q_i y_{i+1})b = \\ &= (ax_i + y_i b) - q_i(x_{i+1}a + y_{i+1}b) = a_i - q_i a_{i+1} = a_{i+2}, \end{aligned}$$

also die Behauptung. ■

Bemerkung: Das im Satz angegebene Verfahren lässt sich auch per Hand gut ausführen: Seien $a, b \in \mathbb{N}_0$ gegeben.

- START: Lege eine Tabelle mit 4 Spalten (für q-Werte und a_i, x_i, y_i): In die ersten beiden Zeilen trägt man folgende Werte ein, wobei die q-Spalte noch frei bleibt:

q	a_i	x_i	y_i
	a	1	0
	b	0	1

- WIEDERHOLE: Hat man die Zeilen i und $i+1$ bereits bestimmt, wobei die Zählung mit 0 begonnen wird, und ist $a_{i+1} \neq 0$, so erhält man die Zeile $i+2$ wie folgt:

$\vdots$	$\vdots$	$\vdots$	$\vdots$
$*$	a_i	x_i	y_i
$*$	a_{i+1}	x_{i+1}	y_{i+1}
$q_i = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor$	$a_{i+2} = a_i - q_i a_{i+1}$	$x_{i+2} = x_i - q_i x_{i+1}$	$y_{i+2} = y_i - q_i y_{i+1}$

  Man berechnet also zunächst den abgerundeten Quotienten $q_i = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor$ und dann damit $a_{i+2}, x_{i+2}, y_{i+2}$. (Man beachte, dass $a_{i+2} = a_i - q_i a_{i+1} = a_i \bmod a_{i+1}$ ist.)
- ENDE: Falls $a_{i+1} = 0$ ist, so ist man in folgender Situation:

$\vdots$	$\vdots$	$\vdots$	$\vdots$
q_{i-2}	a_i	x_i	y_i
q_{i-1}	$a_{i+1} = 0$	x_{i+1}	y_{i+1}

  In diesem Fall ist man fertig: $a_i = x_i a + y_i b$ und $a_i = \mathrm{ggT}(a, b)$. (Die Werte x_{i+1} und y_{i+1} muss man nicht mehr berechnen, da sie nicht benötigt werden. Man kann sie aber als Test benutzen, denn es muss ja dann $0 = a_{i+1} = x_{i+1}a + y_{i+1}b$ gelten.)

Beispiele:

(1) $a = 14$, $b = 11$

q	a_i	x_i	y_i
	14	1	0
	11	0	1
1	3	1	-1
3	2	-3	4
1	1	4	-5
2	0	-11	14

Die Zahlen der vorletzten Zeile liefern

$$1 = \mathrm{ggT}(a, b) = 4 \cdot a - 5 \cdot b$$

(2) $a = 91$, $b = 83$

q	a_i	x_i	y_i
	91	1	0
	83	0	1
1	8	1	-1
10	3	-10	11
2	2	21	-23
1	1	-31	34
2	0	83	-91

Die Zahlen der vorletzten Zeile liefern

$$1 = \mathrm{ggT}(a, b) = -31 \cdot a + 34 \cdot b$$

(3) $a = 12345$, $b = 987$

q	a_i	x_i	y_i
	12345	1	0
	987	0	1
12	501	1	-12
1	486	-1	13
1	15	2	-25
32	6	-65	813
2	3	132	-1651
2	0	-329	4115

Die Zahlen der vorletzten Zeile liefern

$$3 = \mathrm{ggT}(a, b) = 132 \cdot a - 1651 \cdot b$$

(4) $a = 8462$, $b = 3876$

q	a_i	x_i	y_i
	8462	1	0
	3876	0	1
2	710	1	-2
5	326	-5	11
2	58	11	-24
5	36	-60	131
1	22	71	-155
1	14	-131	286
1	8	202	-441
1	6	-333	727
1	2	535	-1168
3	0	-1938	4231

Die Zahlen der vorletzten Zeile liefern

$$2 = \mathrm{ggT}(a, b) = 535 \cdot a - 1168 \cdot b$$

Nun tauschen wir die Zahlen: $a = 3876$, $b = 8462$

q	a_i	x_i	y_i
	3876	1	0
	8462	0	1
0	3876	1	0
2	710	-2	1
5	326	11	-5
2	58	-24	11
5	36	131	-60
1	22	-155	71
1	14	286	-131
1	8	-441	202
1	6	727	-333
1	2	-1168	535
3	0	4231	-1938

Die Zahlen der vorletzten Zeile liefern

$$2 = \mathrm{ggT}(a, b) = -1168 \cdot a + 535 \cdot b$$

(5) $a = 1234567$, $b = 7654321$

q	a_i	x_i	y_i
	1234567	1	0
	7654321	0	1
0	1234567	1	0
6	246919	-6	1
4	246891	25	-4
1	28	-31	5
8817	15	273352	-44089
1	13	-273383	44094
1	2	546735	-88183
6	1	-3553793	573192
2	0	7654321	-1234567

Die Zahlen der vorletzten Zeile liefern

$$1 = \mathrm{ggT}(a, b) = -3553793 \cdot a + 573192 \cdot b$$

(6) $a = 987654321$, $b = 123456789$

q	a_i	x_i	y_i
	987654321	1	0
	123456789	0	1
8	9	1	-8
13717421	0	-13717421	109739369

Die Zahlen der vorletzten Zeile liefern

$$9 = \mathrm{ggT}(a, b) = 1 \cdot a - 8 \cdot b$$

(7) $a = 9876543211$, $b = 1234567891$

q	a_i	x_i	y_i
	9876543211	1	0
	1234567891	0	1
8	83	1	-8
14874311	78	-14874311	118994489
1	5	14874312	-118994497
15	3	-237988991	1903911944
1	2	252863303	-2022906441
1	1	-490852294	3926818385
2	0	1234567891	-9876543211

Die Zahlen der vorletzten Zeile liefern

$$1 = \mathrm{ggT}(a, b) = -490852294 \cdot a + 3926818385 \cdot b$$

(8) Das Verfahren funktioniert auch, wenn $a = 0$ oder $b = 0$ gilt:
$a = 2$, $b = 0$

q	a_i	x_i	y_i
	2	1	0
	0	0	1

Die Zahlen der vorletzten Zeile liefern

$$2 = \mathrm{ggT}(a, b) = 1 \cdot a + 0 \cdot b$$

Für $a = 0$, $b = 2$ erhält man

q	a_i	x_i	y_i
	0	1	0
	2	0	1
0	0	1	0

Die Zahlen der vorletzten Zeile liefern

$$2 = \mathrm{ggT}(a, b) = 0 \cdot a + 1 \cdot b$$

Im Fall $a = 0$, $b = 0$ ergibt sich

q	a_i	x_i	y_i
	0	1	0
	0	0	1

Die Zahlen der vorletzten Zeile liefern

$$0 = \mathrm{ggT}(a, b) = 1 \cdot a + 0 \cdot b$$

(9) $a = 15847523452462634165$, $b = 87648572364875263842$

q	a_i	x_i	y_i
	15847523452462634165	1	0
	87648572364875263842	0	1
0	15847523452462634165	1	0
5	8410955102562093017	-5	1
1	7436568349900541148	6	-1
1	974386752661551869	-11	2
7	615861081269678065	83	-15
1	358525671391873804	-94	17
1	257335409877804261	177	-32
1	101190261514069543	-271	49
2	54954886849665175	719	-130
1	46235374664404368	-990	179
1	8719512185260807	1709	-309
5	2637813738100333	-9535	1724
3	806070970959808	30314	-5481
3	219600825220909	-100477	18167
3	147268495297081	331745	-59982
1	72332329923828	-432222	78149
2	2603835449425	1196189	-216280
27	2028772789353	-32729325	5917709
1	575062660072	33925514	-6133989
3	303584809137	-134505867	24319676
1	271477850935	168431381	-30453665
1	32106958202	-302937248	54773341
8	14622185319	2591929365	-468640393
2	2862587564	-5486795978	992054127
5	309247499	30025909255	-5428911028
9	79360073	-275719979273	49852253379
3	71167280	857185847074	-154985671165
1	8192793	-1132905826347	204837924544
8	5624936	9920432457850	-1793689067517
1	2567857	-11053338284197	1998526992061
2	489222	32027109026244	-5790743051639
5	121747	-171188883415417	30952242250256
4	2234	716782642687912	-129599712052663
54	1111	-38877451588562665	7029336693094058
2	12	78471685819813242	-14188273098240779
92	7	-7258272547011380929	1312350461731245726
1	5	7336744232831194171	-1326538734829486505
1	2	-14595016779842575100	2638889196560732231
2	1	36526777792516344371	-6604317127950950967
2	0	-87648572364875263842	15847523452462634165

Die Zahlen der vorletzten Zeile liefern

$$1 = \mathrm{ggT}(a,b) = 36526777792516344371 \cdot a - 6604317127950950967 \cdot b$$

Bemerkungen:

(1) Mit der folgenden Python-Funktion kann man für $a, b \in \mathbb{N}_0$ schnell $\mathrm{ggT}(a,b)$ und $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = xa + yb$ berechnen:

```
def eea(a,b):
  x,y=1,0
  xx,yy=0,1
  while b>0:
    q=a//b
    a,b=b,a-q*b # Alternativ: a,b=b,a%b
    x,xx=xx,x-q*xx
    y,yy=yy,y-q*yy
  return a,x,y
```

(2) SAGE berechnet zu $a, b \in \mathbb{Z}$ mit dem Befehl `xgcd`(a,b) Zahlen $\mathrm{ggT}(a,b), x, y$ mit $\mathrm{ggT}(a,b) = xa + yb$.

5. Teilerfremdheit

Zwei ganze Zahlen $a, b \in \mathbb{Z}$ heißen **teilerfremd**, wenn gilt $\mathrm{ggT}(a, b) = 1$.

SATZ. *Für $a, b, c, a', b' \in \mathbb{Z}$ gilt:*

(1) $\mathrm{ggT}(a, b) = 1$, $a \mid bc \Longrightarrow a \mid c$.
(2) $\mathrm{ggT}(a, b) = 1$, $a \mid c$ *und* $b \mid c \Longrightarrow ab \mid c$.
(3) $\mathrm{ggT}(a, b) = 1$, $a' \mid a$ *und* $b' \mid b \Longrightarrow \mathrm{ggT}(a', b') = 1$.
(4) *Ist* $\mathrm{ggT}(a, b) \geq 1$, *so gilt* $\mathrm{ggT}(\frac{a}{\mathrm{ggT}(a,b)}, \frac{b}{\mathrm{ggT}(a,b)}) = 1$. *Anders ausgedrückt: Man kann schreiben*

$$a = \mathrm{ggT}(a, b) \cdot a', \quad b = \mathrm{ggT}(a, b) \cdot b' \quad \text{und} \quad \mathrm{ggT}(a', b') = 1$$

mit Zahlen $a', b' \in \mathbb{Z}$.

Beweis:

(1) Wegen $\mathrm{ggT}(a, b) = 1$ existieren $x, y \in \mathbb{Z}$ mit $ax + by = 1$. Multipliziert man die Gleichung mit c, so folgt
$$acx + bcy = c.$$
Wegen $a \mid ac$ und $a \mid bc$ (Voraussetzung) teilt a die linke Seite der Gleichung, und damit auch die rechte Seite, d.h. $a \mid c$, wie behauptet.
(2) Wegen $b \mid c$ gibt es ein $d \in \mathbb{Z}$ mit $c = bd$. Aus $a \mid c$ wird $a \mid bd$. Mit $\mathrm{ggT}(a, b) = 1$ und (1) folgt $a \mid d$. Schreiben wir $d = ae$ mit $e \in \mathbb{Z}$, so wird $c = bd = bae$, also gilt $ab \mid c$, wie behauptet.
(3) Aus $a' \mid a$ folgt $T(a') \subseteq T(a)$, aus $b' \mid b$ folgt $T(b') \subseteq T(b)$. Wegen $\mathrm{ggT}(a, b) = 1$ ist $T(a) \cap T(b) = \{1\}$, woraus dann mit
$$\{1\} \subseteq T(a') \cap T(b') \subseteq T(a) \cap T(b) = \{1\}$$
sofort $\mathrm{ggT}(a', b') = 1$ folgt.
(4) Wir bemerken zunächst, dass wegen $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$ natürlich $\frac{a}{\mathrm{ggT}(a,b)}, \frac{b}{\mathrm{ggT}(a,b)} \in \mathbb{Z}$ gilt. Mit dem erweiterten euklidischen Algorithmus finden wir $x, y \in \mathbb{Z}$ mit $xa + yb = \mathrm{ggT}(a, b)$. Division durch $\mathrm{ggT}(a, b)$ liefert
$$x \cdot \frac{a}{\mathrm{ggT}(a, b)} + y \cdot \frac{b}{\mathrm{ggT}(a, b)} = 1.$$
Es folgt
$$\mathrm{ggT}(\frac{a}{\mathrm{ggT}(a, b)}, \frac{b}{\mathrm{ggT}(a, b)}) \mid 1,$$
und damit
$$\mathrm{ggT}(\frac{a}{\mathrm{ggT}(a, b)}, \frac{b}{\mathrm{ggT}(a, b)}) = 1,$$
was zu zeigen war. ■

6. Die Gleichung $ax + by = c$

Wir wollen zu gegebenen $a, b, c \in \mathbb{Z}$ die ganzzahligen Lösungen der Gleichung
$$ax + by = c$$
bestimmen.
Wir wissen, wie wir mit dem erweiterten euklidischen Algorithmus eine ganzzahlige Lösung der Gleichung
$$ax + by = \mathrm{ggT}(a, b)$$
bestimmen können. Der folgende Satz verallgemeinert diese Gleichung und gibt die Gesamtheit der Lösungen an:

SATZ. *Seien $a, b, c \in \mathbb{Z}$ mit $(a, b) \neq (0, 0)$. Es sollen die ganzzahligen Lösungen der Gleichung $ax + by = c$ bestimmt werden.*

(1) **Fall** $\mathrm{ggT}(a, b) \nmid c$**:** *In diesem Fall hat die Gleichung $ax + by = c$ keine ganzzahligen Lösungen.*

(2) **Fall** $\mathrm{ggT}(a,b) \mid c$**:** *Schreibt man* $a = \mathrm{ggT}(a,b)\cdot a'$, $b = \mathrm{ggT}(a,b)\cdot b'$, $c = \mathrm{ggT}(a,b)\cdot c'$, *so sind* $a', b', c' \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a',b') = 1$ *und die Gleichung* $ax + by = c$ *ist äquivalent zur Gleichung*

$$a'x + b'y = c'.$$

- *Bestimme* $u, v \in \mathbb{Z}$ *mit* $a'u + b'v = 1$ *(beispielsweise mit dem erweiterten euklidischen Algorithmus).*
- $(x_0, y_0) = (c'u, c'v)$ *ist eine Lösung der Gleichung* $a'x + b'y = c'$.
- *Die Lösungen der Gleichung* $ax + by = c$ *sind*

$$(x,y) = (x_0 + b'm, y_0 - a'm) \text{ mit } m \in \mathbb{Z}.$$

Beweis:

(1) **Fall** $\mathrm{ggT}(a,b) \nmid c$**:** Gäbe es $x, y \in \mathbb{Z}$ mit $ax + by = c$, so wäre die linke Seite durch $\mathrm{ggT}(a,b)$ teilbar, also auch die rechte Seite, im Widerspruch zur Voraussetzung $\mathrm{ggT}(a,b) \nmid c$.

(2) **Fall** $\mathrm{ggT}(a,b) \mid c$**:** Da $\mathrm{ggT}(a,b)$ die drei Zahlen a, b, c teilt, gibt es wegen $\mathrm{ggT}(a,b) \geq 1$ eindeutig bestimmte Zahlen $a', b', c' \in \mathbb{Z}$ mit

$$a = \mathrm{ggT}(a,b)\cdot a', \quad b = \mathrm{ggT}(a,b)\cdot b', \quad c = \mathrm{ggT}(a,b)\cdot c'.$$

Trivialerweise gilt für die Gleichung wegen $\mathrm{ggT}(a,b) \neq 0$

$$ax + by = c \quad \Longleftrightarrow \quad a'x + b'y = c'.$$

- Es ist $\mathrm{ggT}(a',b') = 1$. Es gibt dann $u, v \in \mathbb{Z}$ mit

  $$a'u + b'v = 1.$$

  Passende Zahlen u, v findet man beispielsweise mit dem erweiterten euklidischen Algorithmus.
- Multipliziert man $a'u + b'v = 1$ mit c', so erhält man

  $$a'(c'u) + b'(c'v) = c',$$

  also ist $(x_0, y_0) = (c'u, c'v)$ eine (spezielle) Lösung der Gleichung $a'x + b'y = c'$.
- Sei (x,y) irgendeine Lösung der Gleichung $a'x + b'y = c'$. Es folgt $a'x + b'y = a'x_0 + b'y_0$, also $a'(x - x_0) = b'(y_0 - y)$. Die rechte Seite der letzten Gleichung ist durch b' teilbar, sodass folgt

  $$b' \mid a'(x - x_0).$$

  Wegen $\mathrm{ggT}(a',b') = 1$ folgt

  $$b' \mid x - x_0,$$

  es gibt also ein $m \in \mathbb{Z}$ mit

  $$x - x_0 = b'm.$$

  Setzt man dies in $a'(x - x_0) = b'(y_0 - y)$ ein, so bleibt

  $$a'b'm = b'(y_0 - y).$$

  Im Fall $b' \neq 0$ folgt

  $$y = y_0 - a'm.$$

  Also erhalten wir insgesamt

  $$(x,y) = (x_0 + b'm, y_0 - a'm).$$

  (Das Ergebnis gilt auch im Fall $b' = 0$.)
- Umgekehrt sieht man, dass für $(x,y) = (x_0 + b'm, y_0 - a'm)$

  $$a'x + b'y = a'(x_0 + b'm) + b'(y_0 - a'm) = a'x_0 + b'y_0 = c'$$

  gilt. Daraus folgt die Behauptung. ■

FOLGERUNG. *Sind* $a, b \in \mathbb{Z}$ *mit* $\mathrm{ggT}(a,b) = 1$, *so gibt es* $x_0, y_0 \in \mathbb{Z}$ *mit* $ax_0 + by_0 = 1$ *und es gilt*

$$\{(x,y) \in \mathbb{Z}\times\mathbb{Z} : ax + by = 1\} = \{(x_0 + bm, y_0 - am) : m \in \mathbb{Z}\}.$$

Beispiel: Wir wollen die ganzzahligen Lösungen der Gleichung

$$33x - 12y = 9$$

bestimmen. Es ist $\mathrm{ggT}(33, -12) = 3$ (wegen $33, 12, 9, 3, 0$) und $3 \mid 9$, also ist die Gleichung lösbar. Division durch 3 gibt die äquivalente Gleichung

$$11x - 4y = 3.$$

Wir brauchen zunächst eine Lösung von $11u - 4v = 1$. Durch etwas Probieren finden wir die Lösung $(u, v) = (-1, -3)$. (Natürlich hätten wir auch den erweiterten euklidischen Algorithmus benutzen können.) Multiplikation mit 3 liefert die Lösung $(x_0, y_0) = (-3, -9)$ von $11x - 4y = 3$. Die allgemeine Lösung ist daher

$$(x, y) = (-3 + 4m, -9 + 11m) \text{ für } m \in \mathbb{Z}.$$

7. Bruchrechnung

Rationale Zahlen werden durch Brüche $\frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $b \neq 0$ gegeben. Die Gleichheit von Brüchen wird dabei durch folgende Äquivalenz charakterisiert: Für $a, b, c, d \in \mathbb{Z}$ mit $b, d \neq 0$ gilt

$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad ad = bc.$$

Brüche kann man kürzen:

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

Man kann dann (nach eventueller Multiplikation von Zähler und Nenner mit -1) eine Darstellung

$$\frac{a}{b} \text{ mit } a \in \mathbb{Z}, b \in \mathbb{N}, \mathrm{ggT}(a, b) = 1$$

erreichen. So etwas nennt man einen gekürzten Bruch.

LEMMA. *Zwei gekürzte Brüche $\frac{a}{b}$ und $\frac{c}{d}$ sind genau dann gleich, wenn $a = c$ und $b = d$ gilt, d.h. wenn ihre Zähler und ihre Nenner gleich sind.*

Beweis: Es gelte $\frac{a}{b} = \frac{c}{d}$. Dann ist $ad = bc$. Nun gilt $b \mid bc$, also $b \mid ad$, woraus mit $\mathrm{ggT}(a, b) = 1$ sofort $b \mid d$ folgt. Wir können also schreiben $d = bk$ mit $k \in \mathbb{N}$. Setzt man in $ad = bc$ ein, so ergibt sich $abk = bc$, also $c = ak$. Wegen

$$1 = \mathrm{ggT}(c, d) = \mathrm{ggT}(ak, bk) = k \cdot \mathrm{ggT}(a, b) = k \cdot 1 = k$$

folgt $a = c$ und $b = d$, wie behauptet. ■

Ist $q \in \mathbb{Q}$, so gibt es also eine eindeutige Darstellung

$$q = \frac{a}{b} \text{ mit } a \in \mathbb{Z}, b \in \mathbb{N}, \mathrm{ggT}(a, b) = 1.$$

Man nennt a den **Zähler** von q und b den **Nenner** von q. Den Nenner kann man auch so charakterisieren:

$$b = \min\{n \in \mathbb{N} : n \cdot q \in \mathbb{Z}\}.$$

8. kgV

Wir definieren für $a \in \mathbb{Z}$ die Menge der positiven Vielfachen von a:

$$V(a) = \{e \in \mathbb{N} : a \mid e\}.$$

Die Null spielt eine Sonderrolle, denn $V(0) = \emptyset$. Für $a \neq 0$ gilt

$$V(a) = \{k|a| : k \in \mathbb{N}\}.$$

Nun definieren wir für $a, b \in \mathbb{Z}$ das **kleinste gemeinsame Vielfache** von a und b durch

$$\mathrm{kgV}(a, b) = \begin{cases} \min(V(a) \cap V(b)), & \text{falls } a \neq 0 \text{ und } b \neq 0, \\ 0, & \text{falls } a = 0 \text{ oder } b = 0, \end{cases}$$

was natürlich mit

$$\mathrm{kgV}(a,b) = \begin{cases} \{e \in \mathbb{N} : a \mid e \text{ und } b \mid e\}, & \text{falls } a \neq 0 \text{ und } b \neq 0, \\ 0, & \text{falls } a = 0 \text{ oder } b = 0 \end{cases}$$

übereinstimmt, und für $a_1, \ldots, a_n \in \mathbb{Z}$

$$\mathrm{kgV}(a_1, a_2, \ldots, a_n) = \begin{cases} \min(V(a_1) \cap V(a_2) \cap \cdots \cap V(a_n)), & \text{falls alle } a_1, a_2, \ldots, a_n \neq 0, \\ 0, & \text{falls ein } a_i = 0 \text{ ist.} \end{cases}$$

(Im Fall $a_1, a_2, \ldots, a_n \neq 0$ ist $a_1 a_2 \ldots a_n \in V(a_1) \cap V(a_2) \cap \cdots \cap V(a_n)$, sodass das minimale Element des Durchschnitts wohldefiniert ist.) Aus der Definition folgt

$$\mathrm{kgV}(a_1, a_2, \ldots, a_n) = \mathrm{kgV}(a_1, \mathrm{kgV}(a_2, \ldots, a_n)),$$

sodass man sich praktisch auf den Fall $n = 2$ beschränken kann.

LEMMA. *Für $a, b \in \mathbb{Z} \setminus \{0\}$ gilt*

$$V(a) \cap V(b) = V(\frac{ab}{\mathrm{ggT}(a,b)}) \quad \textit{und} \quad \mathrm{kgV}(a,b) = \frac{|ab|}{\mathrm{ggT}(a,b)},$$

also

$$V(a) \cap V(b) = V(\mathrm{kgV}(a,b)).$$

Beweis: Für $e \in \mathbb{N}$ gilt wegen $\mathrm{ggT}(\frac{a}{\mathrm{ggT}(a,b)}, \frac{b}{\mathrm{ggT}(a,b)}) = 1$

$$\begin{aligned} a \mid e \text{ und } b \mid e \quad &\iff \quad \frac{a}{\mathrm{ggT}(a,b)} \mid \frac{e}{\mathrm{ggT}(a,b)} \text{ und } \frac{b}{\mathrm{ggT}(a,b)} \mid \frac{e}{\mathrm{ggT}(a,b)} \quad \iff \\ &\iff \quad \frac{a}{\mathrm{ggT}(a,b)} \cdot \frac{b}{\mathrm{ggT}(a,b)} \mid \frac{e}{\mathrm{ggT}(a,b)} \quad \iff \\ &\iff \quad \frac{ab}{\mathrm{ggT}(a,b)} \mid e. \end{aligned}$$

Daher gilt

$$V(a) \cap V(b) = V(\frac{ab}{\mathrm{ggT}(a,b)}),$$

woraus natürlich auch $\mathrm{kgV}(a,b) = \frac{|ab|}{\mathrm{ggT}(a,b)}$ und der Rest folgt. ■

Ähnlich wie für den ggT zweier Zahlen erhalten wir auch für das kgV eine Charakterisierung:

SATZ. *Seien $a, b \in \mathbb{Z}$. Dann gilt:*

(1) *Für $e' \in \mathbb{Z}$ gilt die Äquivalenz*

$$a \mid e' \textit{ und } b \mid e' \quad \iff \quad \mathrm{kgV}(a,b) \mid e'.$$

(2) *Sei $e \in \mathbb{Z}$. Gilt für alle $e' \in \mathbb{Z}$ die Äquivalenz*

$$a \mid e' \textit{ und } b \mid e' \quad \iff \quad e \mid e',$$

so ist

$$\mathrm{kgV}(a,b) = |e|.$$

Beweis: Im Fall $a, b \neq 0$ folgt dies aus dem vorangegangenen Lemma. Ist $a = 0$ oder $b = 0$, so überlegt man sich die Aussagen direkt. ■

Bemerkung: Da man den ggT mit dem euklidischen Algorithmus schnell berechnen kann, kann man auch das kgV mit folgender Formel schnell berechnen:

$$\mathrm{kgV}(a,b) = \begin{cases} 0, & \text{falls } a = 0 \text{ oder } b = 0, \\ \frac{|ab|}{\mathrm{ggT}(a,b)}, & \text{falls } a \neq 0 \text{ und } b \neq 0. \end{cases}$$

SATZ. *Für $a, b \in \mathbb{Z}$ gilt*

$$\mathrm{ggT}(a,b)\mathrm{kgV}(a,b) = |ab|.$$

Beweis: Sind $a, b \neq 0$, so steht die Aussage im vorangegangenen Lemma. Im Fall $a = 0$ oder $b = 0$ sind die linke und rechte Seite 0, die Behauptung also ebenfalls richtig. ■

9. Primzahlen und der Fundamentalsatz der Arithmetik

Jede ganze Zahl a hat die Teiler ± 1 und $\pm a$, weswegen man diese Teiler auch „triviale Teiler“ nennt. Die positiven Teiler einer ganzen Zahl a hatten wir mit $T(a)$ bezeichnet:

$$T(a) = \{d \in \mathbb{N} : d \mid a\}.$$

Es gilt

$$T(0) = \mathbb{N} \quad \text{und} \quad T(1) = \{1\}.$$

Für $a \geq 2$ ist $\{1, a\} \subseteq T(a)$.

Bemerkung: Ist $a \in \mathbb{N}$ und $d \in T(a)$, so gilt

$$\frac{a}{d} \in T(a) \quad \text{und} \quad a = d \cdot \frac{a}{d}.$$

DEFINITION. *Eine natürliche Zahl $p > 1$ heißt* **Primzahl**, *wenn die einzigen positiven Teiler von p die Zahlen 1 und p sind, d.h. $T(p) = \{1, p\}$, wenn also p nur triviale Teiler hat.*

Die ersten Primzahlen sind

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad 37, \quad 41, \quad 43, \quad 47, \quad \ldots$$

Für eine Primzahl p gilt also wegen $T(p) \in \{1, p\}$

$$\mathrm{ggT}(p, a) \in \{1, p\} \text{ für alle } a \in \mathbb{Z},$$

also

$$p \mid a \quad \text{oder} \quad \mathrm{ggT}(p, a) = 1.$$

LEMMA. *Jede natürliche Zahl $n \geq 2$ ist Produkt von Primzahlen:*

$$n = p_1 p_2 \ldots p_r \text{ mit Primzahlen } p_1, \ldots, p_r.$$

Beweis: Wir beweisen die Aussage durch Induktion: $n = 2$ ist eine Primzahl. Sei nun $n \geq 3$ und die Ausssage bereits für alle kleineren natürlichen Zahlen bewiesen. Wir betrachten $T(n)$.

- Ist $T(n) = \{1, n\}$, so ist n eine Primzahl, wir sind fertig.
- Ist $T(n) \supsetneq \{1, n\}$, so gibt es eine Zahl $d \in T(n) \setminus \{1, n\}$. Dann ist $d' = \frac{n}{d} \in \mathbb{N}$ und $n = dd'$ mit $1 < d, d' < n$. Wir wenden die Induktionsvoraussetzung auf d und d' an und erhalten Primzahlen $q_1, \ldots, q_s, q'_1, \ldots, q'_{s'}$ mit

  $$d = q_1 \ldots q_s \text{ und } d' = q'_1 \ldots q'_{s'}.$$

  Dann ist

  $$n = q_1 \ldots q_s q'_1 \ldots q'_{s'},$$

  und es folgt die Behauptung. ■

Bemerkung: Auf der Beweisidee beruhen auch moderne Faktorisierungsverfahren für große Zahlen n:

- Untersuche, ob n eine Primzahl ist. Erstaunlicherweise gibt es hier schnelle, praktische Methoden.
- Ist n keine Primzahl, versuche, eine Zerlegung $n = dd'$ mit $1 < d, d' < n$ zu finden. Dies ist heutzutage noch ein schwieriges praktisches Problem.

Wie eindeutig ist die Zerlegung einer natürlichen Zahl in ein Produkt von Primzahlen? Wir benötigen hierfür eine wichtige Aussage über Primzahlen:

LEMMA. *Sei p eine Primzahl.*

(1) *Für $a, b \in \mathbb{Z}$ gilt die Implikation*

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ oder } p \mid b.$$

(2) *Für $a_1, \ldots, a_n \in \mathbb{Z}$ gilt die Implikation*

$$p \mid a_1 a_2 \ldots a_n \quad \Longrightarrow \quad p \mid a_1 \text{ oder } p \mid a_2 \text{ oder } \ldots \text{ oder } p \mid a_n.$$

Beweis: Die zweite Aussage folgt durch Induktion aus der ersten, weswegen wir uns auf den Beweis von (1) beschränken. Seien also $a, b \in \mathbb{Z}$ mit $p \mid ab$. Wir unterscheiden zwei Fälle:

- $\mathrm{ggT}(p, a) = 1$**:** Dann folgt aus $p \mid ab$ und $\mathrm{ggT}(p, a) = 1$ mit einem früheren Lemma sofort $p \mid b$.
- $\mathrm{ggT}(p, a) = p$**:** Dann gilt $p \mid a$. ■

LEMMA. *Sind $p_1, \ldots, p_r, q_1, \ldots, q_s$ (nicht notwendig verschiedene) Primzahlen mit*

$$p_1 \ldots p_r = q_1 \ldots q_s,$$

so gilt $r = s$ und es gibt eine Permutation σ mit $q_i = p_{\sigma(i)}$ für $i = 1, \ldots, r$. D.h. bis auf die Reihenfolge der Faktoren ist die Zerlegung in ein Produkt von Primzahlen eindeutig.

Beweis: Sei

$$M = \{n \in \mathbb{N}_{\geq 2} : n \text{ besitzt mindestens zwei verschiedene Darstellungen als Produkt von Primzahlen}\}.$$

Wir wollen zeigen, dass $M = \emptyset$ ist. Angenommen, es wäre $M \neq \emptyset$. Sei $n = \min M$. Wir schreiben

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

mit zwei verschiedenen Darstellungen als Produkt von Primzahlen. p_1 teilt $p_1 \ldots p_r$, also

$$p_1 \mid q_1 \ldots q_s.$$

Nach dem vorangegangenen Lemma gibt es einen Index i mit $p_1 \mid q_i$. Da q_i aber eine Primzahl ist mit $T(q_i) = \{1, q_i\}$, folgt $p_1 = q_i$. Nach Umbenennung der q_j können wir $q_i = q_1$ annehmen, also $p_1 = q_1$. Dann hat die Zahl $\frac{n}{p_1}$ zwei verschiedene Darstellungen als Produkt von Primzahlen:

$$\frac{n}{p_1} = p_2 \ldots p_r = q_2 \ldots q_s,$$

und damit $\frac{n}{p_1} \in M$. Dies ist aber ein Widerspruch zur Minimalität von $n \in M$. Also ist die Annahme falsch, es gilt $M = \emptyset$, und damit die Behauptung. ■

Wir haben gezeigt, dass sich jede natürliche Zahl $n \geq 2$ (bis auf Reihenfolge der Faktoren) eindeutig als Produkt von Primzahlen schreiben lässt. Fasst man gleiche Primzahlen zu einer Potenz zusammen, so kommt man auf folgenden Satz:

SATZ (Fundamentalsatz der Arithmetik). *Jede ganze Zahl $n \neq 0$ lässt sich eindeutig (bis auf die Reihenfolge der Faktoren) schreiben als*

$$n = \pm p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$$

mit paarweise verschiedenen Primzahlen $p_1, p_2, \ldots, p_r$, natürlichen Zahlen $e_1, e_2, \ldots, e_r$ und $r \in \mathbb{N}_0$. Die Primzahlen $p_1, \ldots, p_r$ werden auch die **Primteiler** *der Zahl n genannt. (Den Sonderfall $n = \pm 1$ erhält man für $r = 0$.)*

Bemerkungen:

(1) Gerade wenn die Primfaktorzerlegung mehrerer Zahlen gleichzeitig betrachtet wird, schreibt man oft auch
$$\prod_i p_i^{e_i} \quad \text{mit} \quad e_i \geq 0,$$
wobei dann p_i eventuell auch alle Primzahlen durchlaufen kann. Eine andere Schreibweise ist
$$\prod_p p^{e_p},$$
wobei p alle Primzahlen durchläuft und nur endlich viele $e_p \in \mathbb{N}_0$ von 0 verschieden sind. Die Primteiler der Zahl sind dann genau die Primzahlen p mit $e_p > 0$.

(2) Trotz der Wichtigkeit der Primfaktorzerlegung natürlicher Zahlen, ist bis heute kein wirklich schnelles Verfahren zur Primfaktorzerlegung bekannt.

Beispiele: Hier sind die Primfaktorzerlegungen der natürlichen Zahlen ≤ 100:

1	$21 = 3 \cdot 7$	$41 = 41$	$61 = 61$	$81 = 3^4$
$2 = 2$	$22 = 2 \cdot 11$	$42 = 2 \cdot 3 \cdot 7$	$62 = 2 \cdot 31$	$82 = 2 \cdot 41$
$3 = 3$	$23 = 23$	$43 = 43$	$63 = 3^2 \cdot 7$	$83 = 83$
$4 = 2^2$	$24 = 2^3 \cdot 3$	$44 = 2^2 \cdot 11$	$64 = 2^6$	$84 = 2^2 \cdot 3 \cdot 7$
$5 = 5$	$25 = 5^2$	$45 = 3^2 \cdot 5$	$65 = 5 \cdot 13$	$85 = 5 \cdot 17$
$6 = 2 \cdot 3$	$26 = 2 \cdot 13$	$46 = 2 \cdot 23$	$66 = 2 \cdot 3 \cdot 11$	$86 = 2 \cdot 43$
$7 = 7$	$27 = 3^3$	$47 = 47$	$67 = 67$	$87 = 3 \cdot 29$
$8 = 2^3$	$28 = 2^2 \cdot 7$	$48 = 2^4 \cdot 3$	$68 = 2^2 \cdot 17$	$88 = 2^3 \cdot 11$
$9 = 3^2$	$29 = 29$	$49 = 7^2$	$69 = 3 \cdot 23$	$89 = 89$
$10 = 2 \cdot 5$	$30 = 2 \cdot 3 \cdot 5$	$50 = 2 \cdot 5^2$	$70 = 2 \cdot 5 \cdot 7$	$90 = 2 \cdot 3^2 \cdot 5$
$11 = 11$	$31 = 31$	$51 = 3 \cdot 17$	$71 = 71$	$91 = 7 \cdot 13$
$12 = 2^2 \cdot 3$	$32 = 2^5$	$52 = 2^2 \cdot 13$	$72 = 2^3 \cdot 3^2$	$92 = 2^2 \cdot 23$
$13 = 13$	$33 = 3 \cdot 11$	$53 = 53$	$73 = 73$	$93 = 3 \cdot 31$
$14 = 2 \cdot 7$	$34 = 2 \cdot 17$	$54 = 2 \cdot 3^3$	$74 = 2 \cdot 37$	$94 = 2 \cdot 47$
$15 = 3 \cdot 5$	$35 = 5 \cdot 7$	$55 = 5 \cdot 11$	$75 = 3 \cdot 5^2$	$95 = 5 \cdot 19$
$16 = 2^4$	$36 = 2^2 \cdot 3^2$	$56 = 2^3 \cdot 7$	$76 = 2^2 \cdot 19$	$96 = 2^5 \cdot 3$
$17 = 17$	$37 = 37$	$57 = 3 \cdot 19$	$77 = 7 \cdot 11$	$97 = 97$
$18 = 2 \cdot 3^2$	$38 = 2 \cdot 19$	$58 = 2 \cdot 29$	$78 = 2 \cdot 3 \cdot 13$	$98 = 2 \cdot 7^2$
$19 = 19$	$39 = 3 \cdot 13$	$59 = 59$	$79 = 79$	$99 = 3^2 \cdot 11$
$20 = 2^2 \cdot 5$	$40 = 2^3 \cdot 5$	$60 = 2^2 \cdot 3 \cdot 5$	$80 = 2^4 \cdot 5$	$100 = 2^2 \cdot 5^2$

Bemerkung: SAGE bestimmt (bzw. versucht zu bestimmen) mit dem Befehl `factor(n)` die Primfaktorzerlegung von n.

Mit der eindeutigen Primfaktorzerlegung ganzer Zahlen erhält man eine schöne Charakterisierung der Teilbarkeitsrelation:

SATZ. *Sind $a, b \in \mathbb{Z}$, $a, b \neq 0$, mit den Primfaktorzerlegungen*
$$a = \pm \prod_p p^{a_p} \quad \textit{und} \quad b = \pm \prod_p p^{b_p},$$
so gilt
$$a | b \quad \Longleftrightarrow \quad a_p \leq b_p \textit{ für alle } p,$$
oder kurz geschrieben:
$$\pm \prod_p p^{a_p} | \pm \prod_p p^{b_p} \quad \Longleftrightarrow \quad a_p \leq b_p \textit{ für alle } p.$$

Beweis:

- $\Longrightarrow$ Wegen $a|b$ existiert $c \in \mathbb{Z}$, $c \neq 0$, mit $b = ac$. Sei $c = \pm \prod p^{c_p}$ die Primfaktorzerlegung von c. Dann folgt aus $b = ac$

$$\pm \prod p^{b_p} = \pm \prod p^{a_p} \cdot \prod p^{c_p} = \pm \prod p^{a_p + c_p}.$$

  Die Eindeutigkeit der Primfaktorzerlegung liefert $b_p = a_p + c_p$, was wegen $c_p \geq 0$ die Behauptung $b_p \geq a_p$ zeigt.
- $\Longleftarrow$ Ist $a_p \leq b_p$, so ist $b_p - a_p \geq 0$, also $c = \prod p^{b_p - a_p}$ eine natürliche Zahl. Wie eben sieht man $b = \pm ac$ und damit $a|b$, was behauptet war. ■

Beispiele: Es ist

$$12 = 2^2 \cdot 3, \quad 30 = 2 \cdot 3 \cdot 5, \quad 36 = 2^2 \cdot 3^2, \quad 60 = 2^2 \cdot 3 \cdot 5.$$

Wenn man will, kann man die Darstellungen auch künstlich mit p^0 ergänzen, damit in allen Darstellungen die gleichen Primzahlen vorkommen:

$$12 = 2^2 \cdot 3^1 \cdot 5^0, \quad 30 = 2^1 \cdot 3^1 \cdot 5^1, \quad 36 = 2^2 \cdot 3^2 \cdot 5^0, \quad 60 = 2^2 \cdot 3^1 \cdot 5^1.$$

Vergleicht man die Exponenten, so erhält man mit dem vorangegangenen Satz

$$12 \nmid 30, \quad 12 \mid 36, \quad 12 \mid 60, \quad 30 \nmid 36, \quad 30 \mid 60, \quad 36 \nmid 60.$$

FOLGERUNG. *(Bei den folgenden Produkten der Art $\prod_p p^{a_p}$ sind immer nur endlich viele Exponenten a_p von 0 verschieden, auch wenn dies nicht explizit erwähnt wird.)*

(1) *Teiler:*

$$T(\prod_p p^{a_p}) = \{\prod_p p^{c_p} : 0 \leq c_p \leq a_p \text{ für alle } p\}.$$

(2) *Gemeinsame Teiler:*

$$T(\prod_p p^{a_p}) \cap T(\prod_p p^{b_p}) = \{\prod_p p^{c_p} : 0 \leq c_p \leq \min(a_p, b_p) \text{ für alle } p\}.$$

$$\mathrm{ggT}(\prod_p p^{a_p}, \prod_p p^{b_p}) = \prod_p p^{\min(a_p, b_p)}.$$

(3) *Teilerfremdheit:*

$$\mathrm{ggT}(\prod_p p^{a_p}, \prod_p p^{b_p}) = 1 \quad \Longleftrightarrow \quad a_p = 0 \text{ oder } b_p = 0.$$

Zwei Zahlen sind also genau dann teilerfremd, wenn die Menge der Primteiler von a disjunkt ist zur Menge der Primteiler von b.

(4) *Die Vielfachen einer Zahl:*

$$V(\prod_p p^{a_p}) = \{\prod_p p^{c_p} : c_p \geq a_p \text{ für alle } p\}$$

(5) *Gemeinsame Vielfache:*

$$V(\prod_p p^{a_p}) \cap V(\prod_p p^{b_p}) = \{\prod_p p^{c_p} : c_p \geq \max(a_p, b_p)\}$$

$$\mathrm{kgV}(\prod_p p^{a_p}, \prod_p p^{b_p}) = \prod_p p^{\max(a_p, b_p)}.$$

Beispiele:

(1) Mit dem euklidischen Algorithmus hatten wir in 6 Schritten

$$\mathrm{ggT}(12345, 987) = 3$$

bestimmt. Nun ist

$$12345 = 3 \cdot 5 \cdot 823 \quad \text{und} \quad 987 = 3 \cdot 7 \cdot 47,$$

was das Ergebnis bestätigt. Mit der kgV-Formel des Satzes erhält man

$$\mathrm{kgV}(12345, 987) = 3 \cdot 5 \cdot 7 \cdot 47 \cdot 823 = 4061505.$$

(2) Mit dem euklidischen Algorithmus erhält man in 2 Schritten

$$\mathrm{ggT}(10^{90} - 1, 10^{80} - 1) = 9999999999.$$

Mittels Faktorisierung ergibt sich

$$\begin{aligned} 10^{90} - 1 &= 3^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 211 \cdot 241 \cdot 271 \cdot 2161 \cdot 9091 \cdot 29611 \cdot 52579 \cdot \\ &\quad \cdot 238681 \cdot 333667 \cdot 2906161 \cdot 3762091 \cdot 8985695684401 \cdot 4185502830133110721, \\ 10^{80} - 1 &= 3^2 \cdot 11 \cdot 17 \cdot 41 \cdot 73 \cdot 101 \cdot 137 \cdot 271 \cdot 3541 \cdot 9091 \cdot 27961 \cdot 1676321 \cdot 5070721 \cdot \\ &\quad \cdot 5882353 \cdot 5964848081 \cdot 1972106116664671749835968 1 \end{aligned}$$

und

$$9999999999 = 3^2 \cdot 11 \cdot 41 \cdot 271 \cdot 9091.$$

Die eindeutige Primfaktorzerlegung für ganze Zahlen erweitert sich sofort auf die rationalen Zahlen:

SATZ. *Jede rationale Zahl $a \in \mathbb{Q} \setminus \{0\}$ hat eine eindeutige Darstellung*

$$a = \pm \prod_p p^{a_p} \text{ mit } a_p \in \mathbb{Z},$$

wo das Produkt über alle Primzahlen läuft und nur endlich viele a_p von 0 verschieden sind. Dabei gilt

$$\text{Zähler}(a) = \pm \prod_{\substack{p \\ a_p > 0}} p^{a_p} \quad \textit{und} \quad \text{Nenner}(a) = \prod_{\substack{p \\ a_p < 0}} p^{-a_p}.$$

Beispiele:

$$\frac{17}{18} = \frac{17}{2 \cdot 3^2} = 2^{-1} \cdot 3^{-2} \cdot 17, \quad \frac{24}{65} = \frac{2^3 \cdot 3}{5 \cdot 13} = 2^3 \cdot 3 \cdot 5^{-1} \cdot 13^{-1}.$$

10. Die p-adischen Bewertungen v_p

DEFINITION. *Für eine Primzahl p wird die* **p-adische Bewertung** $v_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ *wie folgt definiert: Hat $a \in \mathbb{Q} \setminus \{0\}$ die Primfaktorzerlegung*

$$a = \pm \prod_{q \text{ prim}} q^{a_q}, \quad \textit{so sei} \quad v_p(a) = a_p.$$

($v_p(a)$ ist also der Exponent von p in der Primfaktorzerlegung von a.)

Beispiele: Aus $\frac{17}{18} = 2^{-1} \cdot 3^{-2} \cdot 17$ folgt

$$v_2(\frac{17}{18}) = -1, \quad v_3(\frac{17}{18}) = -2, \quad v_5(\frac{17}{18}) = 0, \quad v_7(\frac{17}{18}) = 0, \quad v_{11}(\frac{17}{18}) = 0, \quad v_{13}(\frac{17}{18}) = 0, \quad v_{17}(\frac{17}{18}) = 1,$$

$$v_p(\frac{17}{18}) = 0 \text{ für alle } p \geq 19.$$

Bemerkungen: Unmittelbar aus der Definition ergeben sich folgende Eigenschaften:

(1) Für $a \in \mathbb{Q} \setminus \{0\}$ gilt

$$a = \pm \prod_p p^{v_p(a)}.$$

(2) Für $a \in \mathbb{Q} \setminus \{0\}$ gibt es nur endlich viele p mit $v_p(a) \neq 0$.

(3)
$$v_p(1) = v_p(-1) = 0.$$

(4) Für $a \in \mathbb{Q} \setminus \{0\}$ gilt
$$\text{Zähler}(a) = \pm \prod_{\substack{p \\ v_p(a)>0}} p^{v_p(a)} \quad \text{und} \quad \text{Nenner}(a) = \pm \prod_{\substack{p \\ v_p(a)<0}} p^{-v_p(a)}.$$

Wir wollen zunächst ein paar Eigenschaften von v_p für die ganzen Zahlen betrachten.

Bemerkung: Sei $n \in \mathbb{Z} \setminus \{0\}$. Der Funktionswert $v_p(n)$ gibt an, wie oft p in n aufgeht, d.h.
$$p^{v_p(n)} \mid n, \quad \text{aber} \quad p^{v_p(n)+1} \nmid n.$$
Insbesondere gilt natürlich
$$v_p(n) \geq 0.$$
Da die 0 durch jede beliebig hohe p-Potenz teilbar ist, definiert man auch manchmal $v_p(0) = \infty$.

LEMMA. *Ist p eine Primzahl, so gilt für die p-adische Bewertung:*
(1) $v_p(mn) = v_p(m) + v_p(n)$ *für* $m, n \in \mathbb{Z} \setminus \{0\}$.
(2) $v_p(m+n) \geq \min(v_p(m), v_p(n))$ *für* $m, n \in \mathbb{Z} \setminus \{0\}$ *im Fall* $m + n \neq 0$.
(3) *Sind* $m, n \in \mathbb{Z} \setminus \{0\}$ *mit* $v_p(m) \neq v_p(n)$, *so gilt* $v_p(m+n) = \min(v_p(m), v_p(n))$.

Beweis:

- Ist
$$m = \pm \prod_p p^{v_p(m)}, \quad n = \pm \prod_p p^{v_p(n)},$$
so ist
$$mn = \pm \prod_p p^{v_p(m)+v_p(n)}.$$
Wegen der Eindeutigkeit der Primfaktorzerlegung folgt
$$v_p(mn) = v_p(m) + v_p(n).$$
Dies beweist (1).
- Was passiert mit der Summe? Der Fall $m + n = 0$ muss nicht betrachtet werden. Wir schreiben
$$m = p^{m_p} m', \quad n = p^{n_p} n' \quad \text{mit} \quad p \nmid m', \quad p \nmid n'$$
und unterscheiden zwei Fälle, da wir o.E. $m_p \geq n_p$ annehmen können.
  - **Fall $m_p > n_p$:**
$$m + n = p^{m_p} m' + p^{n_p} n' = p^{n_p} \cdot \left(n' + p^{m_p - n_p} m'\right).$$
Wegen $m_p - n_p > 0$ und $p \nmid n'$ gilt
$$p \nmid n' + p^{m_p - n_p}.$$
Daher geht p genau n_p-mal in $m + n$ auf. Also ist
$$v_p(m+n) = n_p = v_p(n) = \min(v_p(m), v_p(n)).$$
  - **Fall $m_p = n_p$:**
$$m + n = p^{m_p} m' + p^{n_p} n' = p^{m_p} \cdot (m' + n').$$
Wir klammern p aus $m' + n'$ so oft wie möglich aus, d.h. wir schreiben
$$m' + n' = p^{\ell} \cdot k \text{ mit } \ell \in \mathbb{N}_0, \quad k \in \mathbb{Z} \setminus \{0\}, \quad p \nmid k.$$
Dann gilt
$$m + n = p^{m_p + \ell} \cdot k,$$
und damit
$$v_p(m+n) = m_p + \ell \geq m_p = \min(v_p(m), v_p(n)).$$

Dies beweist (2) und (3). ■

Dass die Aussage (2) des vorangegangenen Lemmas nicht wesentlich verbessert werden kann, zeigt folgendes Beispiel.

Beispiel: Sei $e \geq 1$ und

$$m = 1, \quad n = 2^e - 1.$$

Dann gilt

$$m + n = 2^e$$

und

$$v_2(m) = 0, \quad v_2(n) = 0, \quad v_2(m+n) = e.$$

Die Differenz $v_p(m+n) - \min(v_p(m), v_p(n))$ kann also beliebig groß werden.

Bemerkung: Die Eigenschaft (3) des Lemmas folgt aus der Eigenschaft (2). Seien $m, n \in \mathbb{Z} \setminus \{0\}$ mit $v_p(m) \neq v_p(n)$. O.E. können wir $v_p(m) < v_p(n)$ annehmen. Angenommen, es wäre $v_p(m+n) > v_p(m)$. Mit $v_p(m+n) \geq v_p(m) + 1$, $v_p(n) \geq v_p(m) + 1$ und $m = (m+n) + (-n)$ folgt dann

$$v_p(m) \geq \min(v_p(m+n), v_p(-n)) \geq \min(v_p(m) + 1, v_p(m)) + 1) = v_p(m) + 1,$$

ein Widerspruch. Also gilt die Eigenschaft (3).

Die Eigenschaften der Bewertungen v_p lassen sich leicht von $\mathbb{Z}$ auf $\mathbb{Q}$ übertragen:

SATZ. *Sei p eine Primzahl und $v_p : \mathbb{Q} \setminus \{0\} \to \mathbb{Z}$ die zugehörige p-adische Bewertung.*

(1) *v_p ist surjektiv.*
(2) *$v_p(1) = v_p(-1) = 0$.*
(3) *$v_p(ab) = v_p(a) + v_p(b)$ für alle $a, b \in \mathbb{Q} \setminus \{0\}$.*
(4) *$v_p(a+b) \geq \min(v_p(a), v_p(b))$ für alle $a, b \in \mathbb{Q} \setminus \{0\}$ im Fall $a + b \neq 0$.*
(5) *Sind $a, b \in \mathbb{Q} \setminus \{0\}$ mit $v_p(a) \neq v_p(b)$, so gilt $v_p(a+b) = \min(v_p(a), v_p(b))$.*
(6) *Sind $a_1, a_2, \ldots, a_r \in \mathbb{Q} \setminus \{0\}$ mit*

$$v_p(a_1) < v_p(a_i) \text{ für } i = 2, \ldots, r,$$

so gilt

$$v_p(a_1 + a_2 + \cdots + a_r) = v_p(a_1).$$

Beweis:

(0) Wir bemerken zunächst, dass für $a, b \in \mathbb{Z} \setminus \{0\}$ gilt

$$v_p(\frac{a}{b}) = v_p(a) - v_p(b),$$

denn

$$v_p(\frac{a}{b}) = v_p\left(\frac{\pm \prod_q q^{v_q(a)}}{\pm \prod_q q^{v_q(b)}}\right) = v_p(\pm \prod_q q^{v_q(a) - v_a(b)}) = v_q(a) - v_q(b),$$

wobei q alle Primzahlen durchläuft.

(1) Dies folgt aus $v_p(p^n) = n$ für alle $n \in \mathbb{Z}$.
(2) Dies ist klar.
(3) Es ist

$$v_p(ab) = v_p((\pm \prod_q q^{v_q(a)}) \cdot (\pm \prod_q q^{v_q(b)})) = v_p(\prod_q q^{v_q(a) + v_q(b)}) = v_p(a) + v_p(b).$$

(4) Wir schreiben $a = \frac{k}{l}$, $b = \frac{m}{n}$ und erhalten mit den im vorangegangenen Lemma gezeigten Eigenschaften

$$\begin{aligned} v_p(a+b) &= v_p(\frac{k}{l}+\frac{m}{n}) = v_p(\frac{kn+lm}{ln}) = v_p(kn+lm) - v_p(ln) \geq \\ &\geq \min(v_p(kn), v_p(lm)) - v_p(ln) = \\ &= \min(v_p(kn) - v_p(ln), v_p(lm) - v_p(ln)) = \\ &= \min(v_p(\frac{k}{l}), v_p(\frac{m}{n}) = \min(v_p(a), v_p(b)). \end{aligned}$$

(5) Dies folgt wie in der Bemerkung vor dem Satz direkt aus (4).

(6) Dies ist eine Verallgemeinerung von (5) und wird durch Induktion nach r bewiesen. ■

Anwendung: Wir wollen zeigen, dass $\sqrt{2}$ irrational, d.h. keine rationale Zahl ist. Wir benutzen die 2-adische Bewertung v_2. Angenommen, $\sqrt{2}$ wäre eine rationale Zahl. Dann könnten wir $v_2(\sqrt{2})$ bilden und folgern

$$1 = v_2(2) = v_2(\sqrt{2}\cdot\sqrt{2}) = v_2(\sqrt{2}) + v_2(\sqrt{2}) = 2v_2(\sqrt{2}), \quad \text{also} \quad v_2(\sqrt{2}) = \frac{1}{2},$$

was aber nicht sein kann, da die Bewertung nur ganze Zahlen als Werte annimmt. Die Annahme ist also falsch. Damit haben wir gezeigt, dass $\sqrt{2}$ irrational ist.

Bemerkung: Manchmal definiert man auch $v_p(0) = \infty$. Dann erhält man eine Funktion $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Für ∞ benötigt man dann folgende Rechenregeln: Für alle $n \in \mathbb{Z}$ gilt

$$n + \infty = \infty + \infty = \infty \quad \text{und} \quad n < \infty.$$