# 1 Arithmetik

## 1.1 Zahlenbereiche

### Natürliche Zahlen

Mit $\mathbb{N}$ bezeichnen wir die Menge der natürlichen Zahlen: $0, 1, 2, 3, \ldots$ Die natürliche Zahl $a$ ist dabei eine Abkürzung für $\underbrace{1 + 1 + \cdots + 1}_{a-\text{mal}}$; $a^n$ ist eine Abkürzung für $\underbrace{a \cdot a \cdot \ldots \cdot a}_{a-\text{mal}}$. 0 ist eine natürliche Zahl. (In der Mathematik wird sehr häufig 0 nicht als natürliche Zahl aufgefasst; wenn 0 zu den natürlichen Zahlen gezählt werden soll, wird $\mathbb{N}_0$ verwendet.) Wird 0 als natürliche Zahl ausgeschlossen, so schreiben wir $\mathbb{N}_+$. (In der Mathematik wird dann $\mathbb{N}$ verwendet.)

Rechenregeln: Es seien $k, n, m$ beliebige natürliche Zahlen.

1. $(k + n) + m = k + (n + m)$ — Assoziativgesetze
   $(k \cdot n) \cdot m \quad = k \cdot (n \cdot m)$
2. $k \cdot (n + m) \;=\; k \cdot n + k \cdot m$ — Distributivgesetz
3. $n + m = m + n$ — Kommutativgesetze
   $n \cdot m \;\; = m \cdot n$
4. $n + 0 = n$ — neutrale Elemente
   $n \cdot 1 \;\; = n$
5. $n \cdot 0 = 0$

Aus diesen Rechenregeln und den oben eingeführten Abkürzungen lassen sich leicht die Potenzrechenregeln herleiten (für alle natürlichen Zahlen $a, b, n, m$):

1. $a^n \cdot a^m = a^{n+m}$
2. $(a^n)^m = a^{n \cdot m}$
3. $a^n \cdot b^n = (a \cdot b)^n$

Insbesondere legt die 4. Regel nahe, dass die Definition $a^0 =_{\text{def}} 1$ für alle natürlichen Zahlen $a$ vernünftig ist, um mit den Potenzen in natürlicher Weise rechnen zu können.

### Ganze Zahlen

Mit $\mathbb{Z}$ bezeichnen wir die Menge der ganzen Zahlen: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$ Die ganzen Zahlen ermöglichen es, alle Subtraktionen stets ausführen zu können, z.B. $3 - 5 = -2$. Die Zahl $-a$ (mit der natürlichen Zahl $a$) ist dabei eine Abkürzung für $\underbrace{(-1) + (-1) + \ldots + (-1)}_{a-\text{mal}} = a \cdot (-1)$.

Rechenregeln:

1.–5. übertragen sich von den natürlichen Zahlen

6. $n + (-n) = 0$ für alle natürlichen Zahlen $n$ — inverses Element

Eine Spezialfall für das Rechnen mit ganzen Zahlen ist die Vorzeichenregel: Wieso ist die Regel $(-1) \cdot (-1) = 1$ plausibel? – Mit Hilfe der Rechenregeln erhalten wir:

$$\begin{aligned} 0 &= (-1) \cdot 0 && \text{(5. Regel)} \\ &= (-1) \cdot (1 + (-1)) && \text{(6. Regel, inverses Element)} \\ &= (-1) \cdot 1 + (-1) \cdot (-1) && \text{(2. Regel, Distributivgesetz)} \\ &= -1 + (-1) \cdot (-1) && \text{(4. Regel, neutrales Element)} \end{aligned}$$

Somit folgt weiter:

$$\begin{aligned} 1 &= 1 + 0 && \text{(4. Regel, neutrales Element)} \\ &= 1 + (-1) + (-1) \cdot (-1) && \text{(siehe oben)} \\ &= 0 + (-1) \cdot (-1) && \text{(6. Regel, inverses Element)} \\ &= (-1) \cdot (-1) && \text{(4. Regel, neutrales Element)} \end{aligned}$$

Die Vorzeichenregel hängt wesentlich mit dem Distributivgesetz zusammen, das auch für alle ganzen Zahlen gelten soll.

## Rationale Zahlen

Mit $\mathbb{Q}$ bezeichnen wir die Menge der rationalen Zahlen, d.h. die Menge der Brüche $\frac{p}{q}$ mit $q \neq 0$ sowie $p, q$ ganze Zahlen. Die rationalen Zahlen ermöglichen es, jede lineare Gleichung $q \cdot x - p = 0$ stets zu lösen. Zur Definition der rationalen Zahlen genügt es auch zu fordern:

1. $p$ ist ganze Zahl und $q$ ist natürliche Zahl, $q \neq 0$
2. $p$ ist natürliche Zahl und $q$ ist ganze Zahl, $q \neq 0$

Eine alternative Darstellungsform rationaler Zahlen ist die Dezimalschreibweise:

- $\frac{1}{2} = 0,5$ (Periodenlänge 0)
- $\frac{1}{3} = 0,333\ldots = 0,\overline{3}$ (Periodenlänge 1)
- $\frac{1}{7} = 0,\overline{142857}$ (Periodenlänge 6)
- $\frac{1}{30} = 0,0\overline{3}$ (schließlich periodisch)

Beachte: Die Dezimalschreibweise ist nicht eindeutig. Zum Beispiel gilt $1 = 0,\overline{9}$, denn

$$\begin{aligned} x &= 0,\overline{9} \\ 10x &= 9,\overline{9} \end{aligned}$$

Somit gilt $9x = 10x - x = 9,\overline{9} - 0,\overline{9} = 9$, d.h. $x = 1$.

Rechenregeln:

1.–6. übertragen sich von den ganzen Zahlen

7. $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = 1$ für $p \neq 0, q \neq 0$ — inverses Element

Als Schreibweise verwenden wir: $\left(\frac{p}{q}\right)^{-1} = \frac{1}{\frac{p}{q}} =_{\text{def}} \frac{q}{p}$.

## Reelle Zahlen

Mit $\mathbb{R}$ bezeichnen wir die Menge aller *reellen* Zahlen, d.h., die Menge der endlichen und unendlichen Dezimalzahlen. Beispielhaft seien folgende reelle Zahlen erwähnt:

1. Jede rationale Zahl ist reell; $r$ ist rational genau dann, wenn $r$ eine schließlich periodische Darstellung besitzt
2. $\pi = 3,141592\ldots$ ist irrational und transzendent
3. $e = 2,7182818\ldots$ ist irrational und transzendent
4. $\sqrt{2} = 1,41421356\ldots$ ist irrational und algebraisch
5. Irrationalität von $\pi + e$ ist offen

Rechenregeln:

1.–7. übertragen sich von den rationalen Zahlen (mit $r \cdot \frac{1}{r} = 1$ für $r \neq 0$ bei der 7. Regel)

Insbesondere lässt sich in den reellen Zahlen die Gleichung $a^x = b$ für alle positiven natürlichen Zahlen lösen, und wir definieren:

$$\log_a b =_{\text{def}} x$$

Es gilt also $a^{\log_a b} = b$. Aus den Potenzrechenregeln ergeben sich somit die Rechenregeln für den Logarithmus:

1. $\log_a(b \cdot c) = \log_a b + \log_a c$
2. $\log_a b^c = c \cdot \log_a b$
3. $\log_a c = \dfrac{\log_b c}{\log_b a}$

Reelle Zahlen können in natürlicher Weise angeordnet werden. Dies wird durch die folgenden Anordnungsaxiome beschrieben (für beliebige reellen Zahlen $a, b, c$):

1. Es gilt entweder $a = b$, $a < b$ oder $a > b$ — Trichotomie
2. Ist $a < b$ und ist $b < c$, so ist $a < c$ — Transitivität
3. Ist $a < b$, so ist $a + c < b + c$ — Monotonie der Addition
4. Ist $a < b$ und ist $0 < c$, so ist $a \cdot c < b \cdot c$ — Monotonie der Multiplikation

## Komplexe Zahlen

Mit $\mathbb{C}$ bezeichnen wir die Menge der komplexen Zahlen, d.h. die Mengen der Zahlenpaare $(a, b)$, wobei $a$ und $b$ reelle Zahlen sind, mit den folgenden Operationen:

1. Addition auf $\mathbb{C}$: $\quad (a, b) + (c, d) =_{\text{def}} (a + c, b + d)$
2. Multiplikation auf $\mathbb{C}$: $\quad (a, b) \cdot (c, d) =_{\text{def}} (ac - bd, ad + bc)$

Eine alternative und die übliche Schreibweise für komplexe Zahlen ist mit $i =_{\text{def}} (0, 1)$:

$$(a, b) = a + b \cdot i$$

Hierbei steht $i$ für die imaginäre Einheit: $i = \sqrt{-1}$. Damit gilt

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i \quad \text{sowie} \quad i^4 = 1$$

Ist $z = a + b \cdot i$, so sind $\text{Re}(z)$ der Realteil von $z$ und $\text{Im}(z)$ der Imaginärteil von $z$. Eine komplexe Zahl $z$ heißt reell, falls $\text{Im}(z) = 0$ gilt; $z$ heißt imaginär, falls $\text{Re}(z) = 0$.

Rechenregeln:

1.–7. übertragen sich von den rellen Zahlen

Für die komplexen Zahlen lassen sich einige bemerkenswerte Gleichungen formulieren:

1. $\sqrt{i} = \frac{1}{2} \cdot \sqrt{2}(1+i)$
2. $e^{i\pi} = -1$
3. $i^i = e^{-\frac{\pi}{2}}$

## 1.2 Primzahlen

Es seien $n$ und $m$ ganze Zahlen. Dann teilt $m$ die Zahl $n$ (symbolisch $m|n$), falls es eine ganze Zahl $k$ gibt mit

$$n = k \cdot m.$$

Bei dieser Definition ist zu beachten, dass jede Zahl 0 teilt.

Eine Zahl $n$ heißt Primzahl, falls 1 und $n$ die einzigen natürlichen Zahlen sind, die $n$ teilen. Die ersten Primzahlen sind somit: $1, 2, 3, 5, 7, 11, 13, 17, \ldots$, wobei 1 üblicherweise nicht zu den Primzahlen gezählt wird.

**Theorem 1.1**

Es sei $n$ eine natürliche Zahl, $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen $2 \leq p_1 < p_2 < \ldots < p_k$ und positive natürliche Zahlen $a_1, a_2, \ldots, a_k$ mit

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}.$$

Bevor wir das Theorem beweisen, wollen wir es an einigen Beispielen verdeutlichen.

**Beispiele:** Die folgenden Zahlenbeispiele illustrieren das Konzept der Primzahlzerlegung (mit den zugehörigen Parametern nach obigem Theorem):

- $24 = 2 \cdot 12 = 2^3 \cdot 3^1 \quad (k = 2,\ p_1 = 2,\ p_2 = 3,\ a_1 = 3, a_2 = 1)$
- $36 = 2^2 \cdot 3^2 \quad (k = 2,\ p_1 = 2,\ p_2 = 3,\ a_1 = 2, a_2 = 2)$
- $111 = 3^1 \cdot 37^1 \quad (k = 2,\ p_1 = 3,\ p_2 = 37,\ a_1 = 1, a_2 = 1)$
- $113 = 113^1 \quad (k = 1,\ p_1 = 113,\ a_1 = 1)$
- $120 = 5 \cdot 24 = 2^3 \cdot 3^1 \cdot 5^1 \quad (k = 3,\ p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ a_1 = 3,\ a_2 = 1,\ a_3 = 1)$

**Beweis:** Wir beweisen die Aussage in zwei Schritten:

1. Existenz: Es sei $n \geq 2$ eine natürliche Zahl. Dann gibt es zwei Fälle:
   - Ist $n$ eine Primzahl, dann sind wir fertig.

- Ist $n$ keine Primzahl, dann gibt es natürliche Zahlen $n_1, n_2 \geq 2$ mit $n = n_1 \cdot n_2$. Für $n_1$ und $n_2$ können wir nun wieder die gleichen Überlegungen anstellen, d.h., sind $n_1 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ sowie $n_2 = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}$ Primzahlzerlegungen, so gilt

$$n = n_1 \cdot n_2 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}.$$

  Durch Zusammenfassen gleicher Faktoren erhalten wir die gewünschte Zerlegung. Da stets $n > n_1, n_2$ gilt, bricht das Verfahren nach endlich vielen Schritten ab.

Somit existiert eine Primzahlzerlegung stets.

2. Eindeutigkeit: Es seien für $n \geq 2$ zwei Zerlegungen gegeben:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}.$$

   Wir betrachten die kleinste als Faktor vorkommende Primzahl. Ohne Beeinträchtigung der Allgemeinheit sei dies $p_1$. Dann teilt $p_1$ sowohl die linke als auch die rechte Zerlegung. Somit gibt es ein $j$ mit $p_1 | q_j$. Da $q_j$ eine Primzahl ist, gilt $p_1 = q_j$. Dividieren wir also beide Primzahlzerlegungen durch $p_1$, so erhalten wir zwei Primzahlzerlegungen mit einem Faktor weniger. Diese Argumentation können wir wiederholen, bis auf einer Seite keine Faktoren mehr übrig sind. Dann sind aber auch auf der anderen Seite keine Faktoren übrig. Somit kommen alle Faktoren auf der linken Seite als Faktoren auf der rechten Seite vor und auch umgekehrt.

Damit ist das Theorem bewiesen. ■

## 1.3 Divisionsreste

Es seien $n$ eine ganze Zahl, $m$ eine natürliche Zahl, $m \geq 2$. Dann teilt $m$ die Zahl $n$ mit Rest $r$, $0 \leq r \leq m-1$, falls eine ganze Zahl $k$ existiert mit

$$n = k \cdot m + r.$$

Die in der Definition vorkommende Zahlen $k$ und $r$ sind eindeutig, denn aus $k \cdot m + r = k' \cdot m + r'$ folgt

$$0 \leq |k \cdot m - k' \cdot m| = |k - k'| \cdot m = |r' - r| \leq m - 1,$$

somit $|k - k'| = 0$ und folglich $k = k'$ und $r = r'$. Damit definieren wir die Modulo-Funktion für zwei Argumente $n$ und $m$:

$$\mathrm{mod}(n, m) = r \quad \Longleftrightarrow_{\mathrm{def}} \quad m \text{ teilt } n \text{ mit Rest } r$$

**Beispiele**: Wir bestimmen die Werte der Modulo-Funktion für verschiedene Argumente:

- $\mathrm{mod}(7, 3) = 1$, denn $7 = 2 \cdot 3 + 1$
- $\mathrm{mod}(-7, 3) = 2$, denn $-7 = (-3) \cdot 3 + 2$
- $\mathrm{mod}(9, 3) = 0$, denn $9 = 3 \cdot 3$
- $\mathrm{mod}(-9, 3) = 0$, denn $-9 = (-3) \cdot 3$

Das folgende Theorem, das wir ohne Beweis angeben, fasst wichtige Rechenregeln für Divisionsreste zusammen.

**Theorem 1.2**

Es seien $k, n$ und $m$ ganze Zahlen, $m \geq 2$.

1. $\text{mod}(k + n, m) = \text{mod}(\text{mod}(k, m) + \text{mod}(n, m))$
2. $\text{mod}(k \cdot n, m) = \text{mod}(\text{mod}(k, m) \cdot \text{mod}(n, m))$
3. $\text{mod}(n^k, m) = \text{mod}(\text{mod}(n, m)^k, m)$

**Beispiele**: Die ersten drei Beispiele veranschaulichen die Korrektheit der drei Rechenregeln aus Theorem 1.2:

$$\begin{aligned}
\text{mod}(5+7,4) &= \text{mod}(\text{mod}(5,4)+\text{mod}(7,4),4)\\
&= \text{mod}(1+3,4)\\
&= 0\\
&= \text{mod}(12,4)
\end{aligned}$$

$$\begin{aligned}
\text{mod}(5\cdot 7,4) &= \text{mod}(\text{mod}(5,4)\cdot\text{mod}(7,4),4)\\
&= \text{mod}(1\cdot 3,4)\\
&= 3\\
&= \text{mod}(35,4)
\end{aligned}$$

$$\begin{aligned}
\text{mod}(5^7,4) &= \text{mod}(\text{mod}(5,4)^7,4)\\
&= \text{mod}(1^7,4)\\
&= 1\\
&= \text{mod}(78125,4)
\end{aligned}$$

Die Rechenregeln können verwendet werden, um Divisionsreste komplexer Ausdrücke zu bestimmen, ohne diese explizit auszurechnen:

$$\begin{aligned}
&\text{mod}\left(13^{73}\cdot 17^{25}+(-2)^{113},4\right)\\
&= \text{mod}\left(\text{mod}(13,4)^{73}\cdot\text{mod}(17,4)^{25}+\text{mod}\left((-2)^2,4\right)^5 6\cdot\text{mod}(-2,4),4\right)\\
&= \text{mod}\left(1^{73}\cdot 1^{25}+0,4\right)\\
&= 1
\end{aligned}$$

Wie finden wir die in der Definition der Teilbarkeit von $n$ durch $m$ mit Rest $r$ angegegebene Zahl $k$, für die $n = k \cdot m + r$ gilt? Dazu verwenden wir Rundungsregeln, die durch Gaußklammern ausgedrckt werden. Für eine beliebige reelle Zahl $x$ definieren wir:

$$\begin{aligned}
\lfloor x \rfloor &=_{\text{def}} \text{ größte ganze Zahl } z \text{ mit } z \leq x\\
\lceil x \rceil &=_{\text{def}} \text{ kleinste ganze Zahl } z \text{ mit } z \geq x
\end{aligned}$$

Die untere Gaußklammer $\lfloor x \rfloor$ bewirkt, dass die Zahl $x$ auf die nächst kleinere ganze Zahl abgerundet wird; mit der oberen Klammer $\lceil x \rceil$ wird $x$ zur nächst größeren ganzen Zahl aufgerundet.

**Beispiele**: Einige Zahlbeispiele verdeutlichen die Rundungsregeln:

$$\left\lfloor \frac{3}{2} \right\rfloor = 1, \quad \left\lceil \frac{3}{2} \right\rceil = 2, \quad \left\lfloor \frac{-3}{2} \right\rfloor = -2, \quad \left\lceil \frac{-3}{2} \right\rceil = -1$$

Mit Hilfe der Gaußklammern kann die Modulo-Funktion wie folgt dargestellt werden (ohne dass auf ein geeignetes $k$ referenziert werden muss):

$$n = \left\lfloor \frac{n}{m} \right\rfloor \cdot m + \mathrm{mod}(n, m)$$

für ganze Zahlen $n$ und $m$ mit $m \geq 2$. Dies ist leicht einzusehen: Für $r = \mathrm{mod}(n, m)$ gibt es ein $k$ mit $n = k \cdot m + r$. Also gilt wegen $r < m$

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

**Proposition 1.3**

Für jede ganze Zahl $n$ gilt $\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n$.

**Beweis:** (Fallunterscheidung) Es sei $n$ eine ganze Zahl.

- 1. Fall: $n$ ist gerade, d.h., es gilt $n = 2k$ für eine ganze Zahl $k$. Dann gilt

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2k}{2} \right\rfloor + \left\lceil \frac{2k}{2} \right\rceil = \lfloor k \rfloor + \lceil k \rceil = 2k = n.$$

- 2. Fall: $n$ ist ungerade, d.h., es gilt $n = 2k + 1$ für eine ganze Zahl $k$. Dann gilt

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2k+1}{2} \right\rfloor + \left\lceil \frac{2k+1}{2} \right\rceil = \left\lfloor k + \frac{1}{2} \right\rfloor + \left\lceil k + \frac{1}{2} \right\rceil = k + (k+1) = 2k + 1 = n.$$

Damit ist die Proposition bewiesen. ■

## 1.4 Algorithmus von Euklid

**Definition 1.4**

Es seien $n$ und $m$ positive natürliche Zahlen.

1. Das kleinste gemeinsame Vielfache von $n$ und $m$, symbolisch $\mathrm{kgV}(n, m)$, ist die kleinste natürliche Zahl $k$, sodass $n$ und $m$ jeweils $k$ teilen.
2. Der größte gemeinsame Teiler von $n$ und $m$, symbolisch $\mathrm{ggT}(n, m)$, ist die größte natürliche Zahl $k$, sodass $k$ jeweils $n$ und $m$ teilt.

**Beispiele**: Einige Zahlbeispiele verdeutlichen die Begriffsbildung:

- $\mathrm{kgV}(3,5) = 15$ und $\mathrm{ggT}(3,5) = 1$
- $\mathrm{kgV}(3,6) = 6$ und $\mathrm{ggT}(3,6) = 3$
- $\mathrm{kgV}(4,6) = 12$ und $\mathrm{ggT}(4,6) = 2$

Der Standardweg, um das kleinste gemeinsame Vielfache und den größten gemeinsamen Teiler von $n$und $m$ zu bestimmen, geht über die Primzahlzerlegungen von $n$ und $m$, die wir uns in folgendem Lemma in geeigneter Weise zurechtlegen.

**Lemma 1.5**

Es seien $n$ und $m$ positive natürliche Zahlen mit den Primfaktordarstellungen $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k}$ und $m = p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k}$, wobei $a_i = 0$ bzw. $b_i = 0$, falls $n$ bzw. $m$ nicht durch $p_i$ teilbar ist. Es gelte weiterhin $b_k > 0$ oder $a_k > 0$. Dann gelten folgende Gleichungen:

$$\begin{aligned} \mathrm{kgV}(n,m) &= p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)} \\ \mathrm{ggT}(n,m) &= p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\min(a_k,b_k)} \end{aligned}$$

**Beweis:** (nur erste Gleichung) Es seien $n$ und $m$ mit den Primfaktordarstellungen wie oben beschrieben gegeben. Es sei $x =_{\mathrm{def}} p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)}$. Dann teilen die Primfaktoren $p_i^{a_i}$ von $n$ und $p_i^{b_i}$ von $m$ jeweils $p_i^{\max(a_i,b_i)}$. Mithin teilen $n$ und $m$ die Zahl $x$. Jede weitere Zahl $y$, die von $n$ und $m$ geteilt wird, muss durch die Promfaktoren $p_i^{a_i}$ und $p_i^{b_i}$ teilbar sein, also auch durch $p_i^{\max(a_i,b_i)}$. Damit teilt $x$ die Zahl $y$. Also gilt $x \leq y$. Folglich gilt $\mathrm{kgV}(n,m) = x$ und das Lemma ist bewiesen. ■

**Beispiele**: Mit den Primfaktordarstellungen $120 = 2^3 \cdot 3^1 \cdot 5^1$ und $36 = 2^2 \cdot 3^2 \cdot 5^0$ gilt

$$\mathrm{kgV}(120,36) = 2^3 \cdot 3^2 \cdot 5^1 = 360 \quad \text{sowie} \quad \mathrm{ggT}(120,36) = 2^2 \cdot 3^1 \cdot 5^0 = 12.$$

**Theorem 1.6**

Es seien $n$ und $m$ positive natürliche Zahlen. Dann gilt:

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

**Beweis:** Es seien $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k}$ und $mn = p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k}$ die Primfaktordastellungen von $n$ und $m$ wie in Lemma 1.5 beschrieben. Dann folgt nach Lemma 1.5:

$$\begin{aligned} &\mathrm{kgV}(n,m) \cdot \mathrm{ggT}(n,m) \\ &= p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)} \cdot p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\min(a_k,b_k)} \\ &= p_1^{\max(a_1,b_1)+\min(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)+\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)+\min(a_k,b_k)} \\ &= p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdot \ \cdots \ \cdot p_k^{a_k+b_k} \\ &= p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k} \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k} \\ &= n \cdot m \end{aligned}$$

Algorithmus: Euklid
Eingabe: positive natürliche Zahl $n, m$ mit $n \geq m$
Augsabe: $\mathrm{ggT}(n, m)$

```
[1]   if m teilt n then
[2]      return m
[3]   else
[4]      return Euklid(mod(n, m), m)
```

**Abbildung 1** Algorithmus von Euklid

Damit ist das Theorem bewiesen. ■

**Korollar 1.7**

Es seien $n$ und $m$ positive natürliche Zahlen. Dann gilt:

$$\mathrm{kgV}(n, m) = \frac{n \cdot m}{\mathrm{ggT}(n, m)} \quad \text{bzw.} \quad \mathrm{ggT}(n, m) = \frac{n \cdot m}{\mathrm{kgV}(n, m)}$$

Wie bestimmen wir $\mathrm{ggT}(n, m)$? Sin die Primfaktorzerlegungen von $n$ und $m$ bekannt, so gibt uns Lemma 1.5 eine einfache Möglichkeit dafür an die Hand. Allerdings ist die Bestimmung von Primfaktorzerlegungen algorithmisch nicht einfach. Einen eleganten Ausweg, der ohne die Primfaktorzerlegung auskommt, ist der Algorithmus von Euklid (siehe Abbildung 1). Dieser ist eine direkte Umsetzung der rekursiven Anwendung der folgenden Resultate.

**Lemma 1.8**

Sind $n$ und $m$ positive natürliche Zahlen mit $m \leq n$, so gilt

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

**Beweis:** Wir zeigen: Jeder Teiler von $m$ und $n$ ist auch ein Teiler von $n - m$ und $m$ und umgekehrt. Zunächst sei $d$ ein Teiler von $n$ und $m$, d.h., $d|n$ und $d|m$. Mithin gilt $n = k \cdot d$ und $m = k' \cdot d$ für geeignete $k, k'$. Somit gilt $n - m = k \cdot d - k' \cdot d = (k - k') \cdot d$ und folglich $d|n - m$. Es sei nun $d$ ein Teiler von $n - m$ und $m$, d.h., $d|n - m$ und $d|m$. Es gilt wieder $n - m = k \cdot d$ und $m = k' \cdot d$ für geeignete $k, k'$. Somit erhalten wir $n = n - m + m = k \cdot d + k' \cdot d = (k + k') \cdot d$ und mithin $d|n$. Damit ist das Lemma bewiesen. ■

**Korollar 1.9**

Sind $n$ und $m$ positive natürliche Zahlen mit $m \leq n$, so gilt

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

**Beweis:** Es sei $n = k \cdot m + \mathrm{mod}(n, m)$ für ein geeignetes $k \geq 0$. Durch wiederholte Anwendung von Lemma 1.8 erhalten wir

$$\begin{aligned} \mathrm{ggT}(n, m) &= \mathrm{ggT}(n - m, m) \\ &= \mathrm{ggT}(n - 2m, m) \\ &\vdots \\ &= \mathrm{ggT}(n - (k-1) \cdot m, m) \\ &= \mathrm{ggT}(m, n - k \cdot m) \\ &= \mathrm{ggT}(m, \mathrm{mod}(n, m)) \end{aligned}$$

Damit ist das Korollar bewiesen. ■

**Beispiele**: Wir wollen die Anwendung des Euklidischen Algorithmus an zwei Beispielen verdeutlichen, die auch einen Eindruck davon geben, wie unterschiedlich die Anzahlen der rekursiven Aufrufe sein können.

$$\begin{aligned} \mathrm{Euklid}(120, 36) &= \mathrm{Euklid}(36, 12) \\ &= 12 \end{aligned}$$

Die jeweiligen Primfaktorzerlegungen sind $120 = 2^3 \cdot 3^1 \cdot 5^1$ und $36 = 2^2 \cdot 3^2$. Gemäß Lemma 1.5 gilt $\mathrm{ggT}(120, 36) = 2^2 \cdot 3^1 \cdot 5^0 = 12$.

$$\begin{aligned} \mathrm{Euklid}(144, 89) &= \mathrm{Euklid}(89, 55) \\ &= \mathrm{Euklid}(55, 34) \\ &= \mathrm{Euklid}(34, 21) \\ &= \mathrm{Euklid}(21, 13) \\ &= \mathrm{Euklid}(13, 8) \\ &= \mathrm{Euklid}(8, 5) \\ &= \mathrm{Euklid}(5, 3) \\ &= \mathrm{Euklid}(3, 2) \\ &= \mathrm{Euklid}(2, 1) \\ &= 1 \end{aligned}$$

Die beiden Zahlen 89 und 144 sind benachbarte Fibonacci-Zahlen, die für den Algorithmus von Euklid schlechteste Eingaben bezüglich der Rekursionsanzahl darstellen.

Der Algorithmus von Euklid kann benutzt werden, um Brüche teilerfremd zu machen, ohne die Primzahlzerlegungen zu bestimmen. Zwei Zahlen $n$ und $m$ heißen teilerfremd, falls $\mathrm{ggT}(n, m) = 1$ Für beliebige positive natürliche Zahlen $n$ und $m$ gilt nun einerseits

$$\mathrm{ggT}\left(\frac{n}{\mathrm{ggT}(n, m)}, \frac{m}{\mathrm{ggT}(n, m)}\right) = 1$$

und andererseits

$$\frac{n}{m} = \frac{n}{m} \cdot \frac{\mathrm{ggT}(n, m)}{\mathrm{ggT}(n, m)} = \frac{n/\mathrm{ggT}(n, m)}{m/\mathrm{ggT}(n, m)}.$$

Der rechte Bruch ist mithin ein äquivalenter teilerfremder Bruch zu dem gegebenen Bruch auf der linken Seite und nicht weiter kürzbar.

**Beispiele**: Wenden wir den Algorithmus von Euklid auf die Zahlen 9724 und 10166 an, so erhalten wir

$$\begin{aligned} \mathrm{Euklid}(10166, 9724) &= \mathrm{Euklid}(9724, 442) \\ &= 442 \end{aligned}$$

und weiter

$$\frac{9724}{10166} = \frac{22}{23}.$$