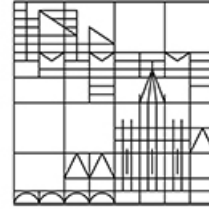


Fachbereich Informatik und
Informationswissenschaft

Universität
Konstanz



Skriptum
zum Brückenkurs
Mathematik

*gehalten in den Wintersemestern 2008/09, 2009/10, 2010/11, 2011/12,
2012/13, 2013/14, 2014/15, 2015/16 und in den Sommersemestern
2011, 2012, 2013, 2014, 2015, 2016*

von

Sven Kosub

5. April 2016

Version v9.1

Inhaltsverzeichnis

| | | |
|----------|----------------------------------|-----------|
| 1 | Arithmetik | 1 |
| 1.1 | Zahlenbereiche | 1 |
| 1.2 | Primzahlen | 5 |
| 1.3 | Divisionsreste | 6 |
| 1.4 | Algorithmus von EUKLID | 8 |
| | Literaturverzeichnis | 11 |

1.1 Zahlenbereiche

Natürliche Zahlen. \mathbb{N} ist die Menge der *natürlichen* Zahlen: $0, 1, 2, 3, \dots$

Die natürliche Zahl a ist eine Abkürzung für $\underbrace{1 + 1 + \dots + 1}_{a\text{-mal}}$; a^n ist eine Abkürzung für $\underbrace{a \cdot a \cdot \dots \cdot a}_{a\text{-mal}}$.

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 \mathbb{N}_+ . (In der Mathematik wird dann \mathbb{N} verwendet.)

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

- | | | | |
|----|---|---|-------------------|
| 1. | $(k + n) + m = k + (n + m)$ | } | Assoziativgesetze |
| | $(k \cdot n) \cdot m = k \cdot (n \cdot m)$ | | |
| 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:

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. \mathbb{Z} ist die Menge der *ganzen* Zahlen: $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$

Die ganzen Zahlen ermöglichen es, alle Subtraktionen stets auch ausführen zu können, wie z.B. $3 - 5 = -2$. Die Zahl $-a$ (mit der natürlichen Zahl a) ist dabei eine Abkürzung für $\underbrace{(-1) + (-1) + \dots + (-1)}_{a\text{-mal}} = a \cdot (-1)$.

Rechenregeln:

- 1.-5. übertragen sich von \mathbb{N}
6. Für ganze Zahl n gilt $n + (-n) = 0$ inverses Element

Beispiel: Wieso ist die Regel $(-1) \cdot (-1) = 1$ plausibel?

Mit Hilfe der Rechenregeln erhalten wir:

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

Somit folgt weiter:

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

Rationale Zahlen. \mathbb{Q} ist 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:

- p ist ganze Zahl und q ist natürliche Zahl, $q \neq 0$
- p ist natürliche Zahl und q ist ganze Zahl, $q \neq 0$

Dezimalschreibweise:

- $\frac{1}{2} = 0,5$ (Periodenlänge 0)
- $\frac{1}{3} = 0,333\dots = 0,\overline{3}$ (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

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

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

Rechenregeln:

1.-6. übertragen sich von \mathbb{Z}

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

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

Reelle Zahlen. \mathbb{R} ist die Menge aller *reellen* Zahlen, d.h., die Menge der endlichen und unendlichen Dezimalzahlen.

Beispiele:

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

Rechenregeln:

1.-7. übertragen sich von \mathbb{Q} (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:

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

Es gilt also $a^{\log_a b} = b$.

Aus den Potenzrechenregeln ergeben sich somit die Rechenregeln für den *Logarithmus*:

1. $\log_a(b \cdot c) = \log_a b + \log_a c$

$$2. \log_a b^c = c \cdot \log_a b$$

Reelle Zahlen können in natürlicher Weise angeordnet werden. Dies wird durch die folgenden Anordnungsaxiome beschrieben:

1. Für alle reellen Zahlen a, b gilt entweder $a = b$, $a < b$ oder $a > b$ (*Trichotomiegesetz*).
2. Für alle reellen Zahlen a, b, c gilt: Ist $a < b$ und ist $b < c$, so ist $a < c$ (*Transitivgesetz*).
3. Für alle reellen Zahlen a, b, c gilt: Ist $a < b$, so ist $a + c < b + c$ (*Monotoniegesetz der Addition*).
4. Für alle reellen Zahlen a, b, c gilt: Ist $a < b$ und ist $0 < c$, so ist $a \cdot c < b \cdot c$ (*Monotoniegesetz der Multiplikation*).

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

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 \mathbb{R}

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, ..., wobei 1 üblicherweise nicht zu den Primzahlen gezählt wird.

Theorem 1.1 (Primzahlzerlegung) *Es sei n ein natürliche Zahl $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen $2 \leq p_1 < p_2 < \dots < p_k$ und positive natürliche Zahlen a_1, a_2, \dots, a_k mit*

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

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

Beispiele: Die folgenden Zahlenbeispiele illustrieren das Konzept der Primzahlzerlegung.

- $24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3^1$
- $111 = 3^1 \cdot 37^1$
- $113 = 113^1$
- $36 = 6^2 = 2 \cdot 3 \cdot 2 \cdot 3 = 2^2 \cdot 3^2$

Beweis: Wir beweisen die Aussage in zwei Schritten:

- *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 $n_1 = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ sowie $n_2 = q_1^{b_1} \cdot q_2^{b_2} \cdot \dots \cdot q_m^{a_k}$ Primzahlzerlegungen, so gilt

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

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

Somit existiert eine Primzahlzerlegung stets.

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

$$n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k} = q_1^{b_1} \cdot \dots \cdot q_m^{b_m}$$

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 Zahl k ist eindeutig, denn aus $k \cdot m + r = k' \cdot m + r$ folgt $(k - k') \cdot m = 0$, also $k = k'$.

Damit definieren wir die *Modulo-Funktion* für n und m :

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

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

- $\text{mod}(7, 3) = 1$, denn $7 = 2 \cdot 3 + 1$
- $\text{mod}(-7, 3) = 2$, denn $-7 = (-3) \cdot 3 + 2$
- $\text{mod}(9, 3) = 0$, denn $9 = 3 \cdot 3$
- $\text{mod}(-9, 3) = 0$, 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. $\text{mod}(k + n, m) = \text{mod}(\text{mod}(k, m) + \text{mod}(n, m), m)$.
2. $\text{mod}(k \cdot n, m) = \text{mod}(\text{mod}(k, m) \cdot \text{mod}(n, m), m)$.
3. $\text{mod}(n^k, m) = \text{mod}(\text{mod}(n, m)^k, m)$, falls $k > 0$.

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

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

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

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

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

$$\begin{aligned}\text{mod}(13^{73} \cdot 17^{25} + (-2)^{113}, 4) \\ &= \text{mod}(\text{mod}(13, 4)^{73} \cdot \text{mod}(17, 4)^{25} + \text{mod}((-2)^2, 4)^{56} \cdot \text{mod}(-2, 4), 4) \\ &= \text{mod}(1^{73} \cdot 1^{25} + 0, 4) \\ &= 1\end{aligned}$$

Wie finden wir die in der Definition der Teilbarkeit von n durch m mit Rest r angegebene Zahl k , so dass $n = k \cdot m + r$ gilt? Dafür verwenden wir Rundungsregeln, die durch GAUSS-Klammern ausgedrückt 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* GAUSS-Klammer $\lfloor x \rfloor$ 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 GAUSS-Klammern kann die Modulo-Funktion wie folgt dargestellt werden (ohne dass auf eine geeignetes k abgestellt werden muss):

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

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

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

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 $n = 2 \cdot k + 1$ 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 $\text{kgV}(n, m)$, ist die kleinste natürliche Zahl k , so dass n und m jeweils k teilen.
2. Der größte gemeinsame Teiler von n und m , symbolisch $\text{ggT}(n, m)$, ist die größte natürliche Zahl k , so dass k jeweils n und m teilt.

Beispiele:

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

Lemma 1.5 *Es seien n und m positive natürliche Zahlen mit Primfaktordarstellungen $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$ und $m = p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_k^{b_k}$, 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:*

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

Beweis: (nur erste Gleichung) Es seien n und m mit den Primfaktordarstellungen wie oben beschrieben gegeben. Es sei $x = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \dots \cdot p_k^{\max(a_k, b_k)}$. 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 Primfaktoren $p_i^{a_i}$ 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 $\text{kgV}(n, m) = x$. ■

Beispiele: Mit den Primzahlzerlegungen $24 = 2^3 \cdot 3^1$ und $36 = 2^2 \cdot 3^2$ gilt

$$\text{kgV}(24, 36) = 2^3 \cdot 3^2 = 72 \text{ sowie } \text{ggT}(24, 36) = 2^2 \cdot 3^1 = 12.$$

Theorem 1.6 *Es seien n und m positive natürliche Zahlen. Dann gilt:*

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

Beweis: Es seien $n = p_1^{a_1} \cdot \dots \cdot p_k^{a_k}$ und $m = p_1^{b_1} \cdot \dots \cdot p_k^{b_k}$ Primfaktorzerlegungen wie in Lemma 1.5 beschrieben. Nach Lemma 1.5 folgt:

$$\begin{aligned} \text{kgV}(n, m) \cdot \text{ggT}(n, m) &= p_1^{\max(a_1, b_1)} \cdot \dots \cdot p_k^{\max(a_k, b_k)} \cdot p_1^{\min(a_1, b_1)} \cdot \dots \cdot p_k^{\min(a_k, b_k)} \\ &= p_1^{\max(a_1, b_1) + \min(a_1, b_1)} \cdot \dots \cdot p_k^{\max(a_k, b_k) + \min(a_k, b_k)} \\ &= p_1^{a_1 + b_1} \cdot \dots \cdot p_k^{a_k + b_k} \\ &= p_1^{a_1} \cdot \dots \cdot p_k^{a_k} \cdot p_1^{b_1} \cdot \dots \cdot p_k^{b_k} \\ &= n \cdot m \end{aligned}$$

Damit ist das Theorem bewiesen. ■

Korollar 1.7 *Es seien n und m natürliche Zahlen. Dann gilt*

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

Algorithmus: EUKLID
 Eingabe: positive natürliche Zahlen n, m mit $m \leq n$
 Ausgabe: $\text{ggT}(m, n)$

1. IF m teilt n
2. RETURN m
3. ELSE
4. RETURN EUKLID(mod(n, m), m)

Abbildung 1.1: Algorithmus von EUKLID

Wie bestimmen wir $\text{ggT}(n, m)$? Sind 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 1.1). Dieser ist eine direkte Umsetzung der rekursiven Anwendung der folgenden Resultate.

Lemma 1.8 *Sind m, n positive natürliche Zahlen mit $m \leq n$ und m teilt nicht n , so gilt*

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

Beweis: Wir müssen zeigen: Jeder Teiler von m und n ist auch ein Teiler von $n - m$ und umgekehrt. Zunächst sei d ein Teiler von n und m , d.h., $d|n$ und $d|m$. Es 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 mithin $d|n - m$. Es sein 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 $d|n$. ■

Korollar 1.9 *Sind m und n positive natürliche Zahlen mit $m \leq n$ und m teilt nicht n , so gilt*

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

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

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

Damit ist das Korollar bewiesen. ■

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

$$\begin{aligned}\text{EUKLID}(36, 120) &= \text{EUKLID}(12, 36) \\ &= 12\end{aligned}$$

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

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

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

Literaturverzeichnis

- [MM06] Christoph Meinel und Martin Mundhenk. *Mathematische Grundlagen der Informatik. Mathematisches Denken und Beweisen. Eine Einführung.* 3., überarbeitete und erweiterte Auflage. B. G. Teubner Verlag, Wiesbaden, 2006.
- [Ste07] Angelika Steger. *Diskrete Strukturen. Band 1: Kombinatorik-Graphentheorie-Algebra.* 2. Auflage. Springer-Verlag, Berlin, 2007.
- [SS02] Thomas Schickinger und Angelika Steger. *Diskrete Strukturen. Band 2: Wahrscheinlichkeitstheorie und Statistik.* Springer-Verlag, Berlin, 2002.
- [WHK04] Manfred Wolff, Peter Hauck und Wolfgang Küchlin. *Mathematik für Informatik und Bioinformatik.* Springer-Verlag, Berlin, 2004.

