Diophantische Gleichung und der erweiterte Euklidsche Algorithmus

1 Diophantische Gleichungen

Eine Gleichung

$$f(a,b,c,\ldots) = 0 \tag{1}$$

für die nur *ganze* Zahlen als Lösungen gesucht werden, heißt diophantische Gleichung. So hat z.B. die quadratische Gleichung

$$a^2 + b^2 = c^2 \tag{2}$$

unendlich viele ganzzahlige Lösungen a, b, c , so z.B.

$$\begin{array}{ccc} a & b & c \\ \hline 3 & 4 & 5 \\ 5 & 12 & 13 \\ \ldots\ldots\ldots & & \end{array} \tag{3}$$

Für die allgemeine nichtlineare Gleichung

$$a^n + b^n = c^n \tag{4}$$

existiert bis in jüngster Zeit lediglich die Fermat'sche Vermutung[1], welche besagt, daß für $n > 2$ keine ganzzahligen Lösungen existieren. Erst 1994 Zeit ist es dem Mathematiker Andrew Wiles gelungen, dafür einen Beweis anzugeben.

Wir wollen uns hier mit dem einfacheren Fall der linearen Diophantischen Gleichung beschäftigen. Gesucht sind ganzzahlige Lösungen a, b für die Gleichung

$$\boxed{am + bn = c \qquad a, b, m, n, c \in \mathbb{Z}} \quad . \tag{5}$$

[1] Pierre de Fermat, 1601-1663; er schrieb 1637 in einer Veröffentlichung, daß er einen elegenten Beweis gefunden hätte, doch der Rand sei zu schmal um ihn hier niederzuschreiben

Beweis von Andrew Wiles: 1994 (Buch von Simon Singh: Fermats last theorem)

Es kann gezeigt werden, daß diese Gleichung dann und nur dann Lösungen besitzt, wenn

$$\mathrm{ggT}(m,n) | c \quad , \tag{6}$$

d.h. (m, n) muß Teiler von c sein. Teilt man Gl. 5 durch (m, n), so erhält man

$$am' + bn' = c' \quad . \tag{7}$$

Diese Gleichung ist lösbar, für

$$\mathrm{ggT}(m', n') = 1 | c' \quad . \tag{8}$$

Zunächst betrachten wir die vereinfachte Gleichung

$$a_1 m' + b_1 n' = 1 \quad \text{mit} \quad (m', n') = 1 \quad . \tag{9}$$

Mit Hilfe des erweiterten Euklid'schen Algorithmus lassen sich dafür Lösungen a_1, b_1 finden. Damit erhält man aber auch Lösungen für die Gln. 7 und 5:

$$\boxed{\begin{array}{rcl} a & = & c' \cdot a_1 \\ b & = & c' \cdot b_1 \end{array}} \quad . \tag{10}$$

Aus dieser Basislösung lassen sich nun aber beliebig viele Lösungen ableiten ([11]), nämlich

$$\begin{array}{rcll} a' & = & a + t \cdot n' & t \in \mathbb{Z} \\ b' & = & b - t \cdot m' & \end{array} \quad , \tag{11}$$

was einfach wie folgt zu bestätigen ist:

$$(a + tn')m' + (b - tm')n' = am' + bn' + tn'm' - tn'm' = c' \quad . \tag{12}$$

Beispiel 1.1: *Zu lösen sei die lineare Diophantische Gleichung*

$$a \cdot \underbrace{15}_{m} + b \cdot \underbrace{10}_{n} = 25 \quad . \tag{13}$$

Wegen $(15, 10) = 5 | 25$ *existiert eine Lösung. Durch Division mit* $(15, 10) = 5$ *erhalten wir*

$$a \cdot 3 + b \cdot 2 = 5 \quad , \tag{14}$$

und die vereinfachte Gleichung

$$a_1 \cdot 3 + b_1 \cdot 2 = 1 \quad . \tag{15}$$

Mit dem Euklid'schen Algorithmus, oder wie hier unmittelbar zu sehen ist, erhalten wir die Lösung $a_1 = 1, b_1 = -1$ *und daraus*

$$\begin{array}{rcl} a & = & c' \cdot a_1 = 5 \\ b & = & c' \cdot b_1 = -5 \end{array} \quad . \tag{16}$$

Nach Gl. 11 ergeben sich weitere Lösungen zu

$$a' = a + tn' = 5 + t \cdot 2 \tag{17}$$

$$b' = b - tm' = -5 - t \cdot 3 \quad , \tag{18}$$

und damit auszugsweise

t	-4	-3	-2	-1	0
a'	-3	-1	$\mathbf{1}$	3	5
b'	7	4	$\mathbf{1}$	-2	-5

$\underbrace{\qquad\qquad}_{a', b' \in \mathbb{N}}$

Häufig ist es notwendig natürliche Lösungen $a', b' \in \mathbb{N}$ *zu finden. Aus obiger Tabelle können wir die Existenz einer natürlichen Lösung erkennen. Man kann zeigen ([11]), daß mindestens eine natürliche Lösung zu finden ist, wenn*

$$(m, n) | c \quad \text{und} \quad (m, n)c > a \cdot b \quad . \tag{19}$$

2 Über die Zerlegung ganzer Zahlen

Die folgende Zerlegung von Zahlen ist von grundlegender Bedeutung.

Definition 2.1: **Zerlegung ganzer Zahlen** ([7]) $(a, m, q, r \in \mathbb{Z},\ m \neq 0)$ *Eine ganze Zahl* a *kann eindeutig dargestellt werden als ganzzahliges Vielfaches* $(q \in \mathbb{Z})$ *einer zweiten Zahl* m *und einem Rest* r*:*

$$\boxed{a = m \cdot q + r} \quad , \tag{20}$$

mit:

$$\boxed{\begin{array}{ll} 0 \leq r < m & \text{für} \quad m > 0 \\ 0 \geq r > m & \text{für} \quad m < 0 \end{array}} \quad . \tag{21}$$

Die beiden Unbekannten q *und* r *ermitteln wir durch eine Ganzzahldivision sowie eine sogenannte Reduktion modulo* m*:*

$$\boxed{\begin{array}{rcll} q & = & \lfloor a/m \rfloor = a \operatorname{div} m & \textit{Quotient (ganzz. Anteil)} \\ r & = & a \bmod m & \textit{Rest (a modulo m)} \\ & = & a - m \cdot \lfloor a/m \rfloor & \\ & = & a - m(a \operatorname{div} m) & \end{array}} \quad , \tag{22}$$

und somit:

$$a = m \cdot \lfloor a/m \rfloor + (a \bmod m) \quad . \tag{23}$$

Mit der Operation `div` *wird die Ganzzahldivision bezeichnet; sie steht typischerweise bei Rechnern als Maschinenbefehl zur Verfügung.*

Für den Sonderfall $m = 0$ *führt die Zerlegung auf*

$$a = 0 \cdot q + r \quad ,$$

was erfüllt wird für:

$$q \in \mathbb{Z} \quad \textit{beliebig, und} \quad r = a \quad . \tag{24}$$

Dies führt auf die Definition

$$a \bmod 0 = a \quad . \tag{25}$$

Beispiele für die Reduktion modulo m:

$$\begin{array}{lll} 7 \bmod 5 = 2; & 15 \bmod 5 = 0; & a \bmod 1 = 0 \\ -2 \bmod 3 = 1; & 5 \bmod -3 = -1; & -8 \bmod -3 = -2 \end{array}$$

Für die Ermittlung des Restes durch Anwendung der Reduktion modulo a auf arithmetische Ausdrücke gelten die folgenden Regeln. Dafür soll abgekürzt die Schreibweise

$$< a >_m := a \bmod m \tag{26}$$

eingeführt werden. Damit gilt:

$$< a+b >_m \;=\; << a >_m + < b >_m >_m \tag{27}$$
$$< a-b >_m \;=\; << a >_m - < b >_m >_m \tag{28}$$
$$< a \cdot b >_m \;=\; << a >_m \cdot < b >_m >_m \tag{29}$$

Beweis von Gl. (27): Für $a = k \cdot m + a_0$, und $b = l \cdot m + b_0$ mit $\forall k, l \in \mathbb{Z}$ folgt:

$$< a+b >_m = < (k+l)m + a_0 + b_0 >_m = < a_0 + b_0 >_m = << a >_m + < b >_m >_m \quad \clubsuit\clubsuit$$

Beweis von Gl. (29): Für $a = k \cdot m + a_0$, und $b = l \cdot m + b_0$ mit $\forall k, l \in \mathbb{Z}$ folgt:

$$\begin{aligned} < a \cdot b >_m \;&=\; < (km + a_0) \cdot (lm + b_0) >_m = < klm^2 + kb_0 m + la_0 m + a_0 b_0 >_m \\ &=\; < (klm + kb_0 + la_0)m + a_0 b_0 >_m = << a >_m \cdot < b >_m >_m \end{aligned} \quad \clubsuit\clubsuit$$

3 Der Euklid'sche Algorithmus

Eingabewerte: zwei positive ganze Zahlen m, n
Ausgabewert: Der größte gemeinsame Teiler der beiden Zahlen, $\mathrm{ggT}(m, n)$

Der Algorithmus kann durch die folgende Anweisungsfolge definiert werden:

A1: Dividiere m ganzzahlig durch n und bezeichne den entstehenden Rest mit r .

A2: Falls $r = 0 \Rightarrow \mathrm{ggT}(m, n) = n$ und Ende des Algorithmus.

A3: Setze $m \leftarrow n$, $n \leftarrow r$.

A4: Gehe zurück nach A1 .

Zahlenbeispiel: Gegeben: $m = 119$, $n = 544$, gesucht: $\mathrm{ggT}(m, n) = ?$

A1: $m/n = 119/544 \Rightarrow r \leftarrow 119$
A2: $r \neq 0$
A3: $m \leftarrow 544$, $n \leftarrow 119$
A1: $m/n = 544/119 = 4 + 68/119 \Rightarrow r \leftarrow 68$
A2: $r \neq 0$
A3: $m \leftarrow 119$, $n \leftarrow 68$
A1: $m/n = 119/68 \Rightarrow r \leftarrow 51$
A2: $r \neq 0$
A3: $m \leftarrow 68$, $n \leftarrow 51$
A1: $m/n = 68/51 \Rightarrow r \leftarrow 17$
A2: $r \neq 0$
A3: $m \leftarrow 51$, $n \leftarrow 17$
A1: $m/n = 51/17 \Rightarrow r \leftarrow 0$
A2: $\mathrm{ggT}(m, n) = n = 17 \Rightarrow$ STOP ☺

Abb. 1 verdeutlicht graphisch in Form eines Ablaufdiagramms die Anweisungskette.

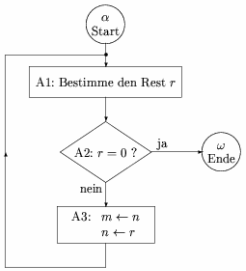

Abbildung 1: Ablaufdiagramm des Euklid'schen Algorithmus

Euklid'scher Algorithmus Der größte gemeinsame Teiler soll mit runden Klammern wie folgt abgekürzt werden:

$$(a, b) := \mathrm{ggT}(a, b) \quad . \tag{30}$$

Sind zwei Zahlen teilerfremd oder relativ prim, so gilt

$$(a, b) = 1 \quad , \tag{31}$$

andernfalls läßt sich ein gemeinsamer Faktor kürzen, so z.B. bei:

$$\frac{12}{15} = \frac{\not{3} \cdot 4}{\not{3} \cdot 5} = \frac{4}{5} \quad . \tag{32}$$

Falls ein gemeinsamer negativer Faktor existiert, dann auch der entsprechende positive Wert, und deshalb erhalten wir

$$(a, b) \geq 1 \qquad a, b \in \mathbb{Z} \quad (\text{außer für } a = b = 0) \quad . \tag{33}$$

Somit gilt offensichtlich auch

$$(a, a) = (a, 0) = |a| \quad . \tag{34}$$

Ohne Beschränkung der Allgemeinheit wollen wir nichtnegative ganze Zahlen betrachten $a, b \in \mathbb{Z}_{\geq}$ mit $a > b$ und wir erhalten aufbauend auf Gl. 20 die folgende Zerlegung:

$$a = b \cdot q + r \quad \text{mit } 0 \leq r < b \quad . \tag{35}$$

Die Grundlage des Euklid'schen Algorithmus besteht in der Reduktion des größten gemeinsamen Teilers zweier Zahlen auf zwei kleinere Zahlen durch Differenzbildung oder Ermittlung des Restes gemäß:

$$\begin{array}{lll} 1. & (a, b) & = \quad (a - b, b) \\ 2. & (a, b) & = \quad (a - b \cdot q, b) = (r, b) \end{array} \tag{36, 37}$$

Aufbauend auf Gl. (37) kann nun gezeigt werden, daß sich der Zahlenbereich bei jedem Reduktionsschritt halbiert. Für $a > b$ gilt nämlich:

$$0 \le r < a/2 \quad . \tag{38}$$

Daraus folgt eine äußerst günstige Komplexität des Euklid'schen Algorithmus von nur

$$\boxed{t(n) = O(\mathrm{ld}\, n) \quad \text{mit} \quad n = \max(a,b)} \quad , \tag{39}$$

welche auch bei sehr großen Zahlen nur wenig Iterationen und damit günstige Rechenzeiten garantiert.

Beweis von Gl. (38): Mit $a > b$, folgt unter Beachtung der folgenden Fallunterscheidung die Behauptung:

$$\begin{array}{llllll} \text{für} & b > a/2 & \text{und} & q = 1 & \text{folgt} & r = a - b < a/2 \quad , \\ \text{für} & b < a/2 & \text{und wegen} & 0 \le r < b & \text{folgt} & r < a/2 \quad , \\ \text{für} & b = a/2 & & & \text{folgt} & r = 0 \end{array} \qquad \clubsuit\clubsuit$$

Das folgende Zahlenbeispiel soll den Sachverhalt verdeutlichen. Mit $a = 217$, liefert die Division a/b durch alle Zahlen $0 < b < a$ einen Rest $r = a \bmod b$, welcher kleiner ist als $a/2$:

b	216	215	...	109	108	107	...	73	72	71	...
r	1	2	...	108	1	3	...	71	1	4	...

Wegen ihrer Bedeutung soll die Gl. (36) und damit bei wiederholter Anwendung auch Gl. (37) bewiesen werden.

Beweis von Gl. (36): Durch Abspaltung des größten gemeinsamen Faktors der beiden Zahlen $a, b \in \mathbb{Z}_{\ge}$ mit $a > b$ erhält man:

$$\begin{aligned} a &= g \cdot a' \\ b &= g \cdot b' \quad , \end{aligned}$$

mit

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

und es gilt somit

$$(a', b') = 1 \quad .$$

Wegen $a > b$ gilt außerdem

$$a' > b' \quad .$$

1. Notwendige Bedingung: Falls g Teiler von a und b ist, dann ist g auch Teiler von $(a-b)$ und b:

$$a - b = g \cdot a' - g \cdot b' = g(a' - b') \quad .$$

2. Hinreichende Bedingung: Es gibt keinen größeren gemeinsamen Teiler.
Wenn a' und b' keinen größeren gemeinsamen Faktor haben als 1, dann haben auch b' und $a' - b'$ keinen größeren gemeinsamen Faktor als 1, d.h. es gibt keinen größeren gemeinsamen Teiler von $(a-b, a)$, als von (a, b).
Die kanonische Primfaktorzerlegung von a und b, mit $a, b \in \mathbb{N}$ und $a, b > 1$, ist eindeutig ([11]):

$$\boxed{\begin{aligned} a &= a_0^{p_0} \cdot a_1^{p_1} \cdot \cdots \cdot a_r^{p_r} \\ b &= b_0^{q_0} \cdot b_1^{q_1} \cdot \cdots \cdot b_s^{q_s} \end{aligned}} \quad . \tag{40}$$

wobei die a_i, b_i Primzahlen sind und $p_i, q_i \ge 1$, für alle i.

Wegen $(a', b') = 1$, folgt $\{a'_i\} \cap \{b'_i\} = \emptyset$ (die Schnittmenge ist die leere Menge).
Aus

$$\underbrace{(\{a'_i\} \cap \{b'_i\})}_{\text{gem. Faktoren von } a', b'} \cap \{b'_i\}) = \{a'_i\} \cap \{b'_i\} = \emptyset$$

folgt

$$(a' - b', b') = 1 \quad ,$$

d.h. es gibt keinen zusätzlichen gemeinsamen Faktor von b' und $a' - b'$. Man kann nur einen gemeinsamen Faktor von $(a' - b')$ vor die Klammer ziehen, wenn er sowohl in a' als auch in b' enthalten ist, d.h. wenn $\{a'_i\} \cap \{b'_i\} \neq \emptyset$. $\clubsuit\clubsuit$

4 Der erweiterte Euklid'sche Algorithmus

Ausgangspunkt für die sich anschließenden Überlegungen sei das folgende

Problem: *Gegeben seien zwei positive ganze Zahlen m, n. Berechne den größten gemeinsamen Teiler $d = \mathrm{ggT}(m,n)$ und zwei ganze Zahlen a, b, welche die folgende Gleichung erfüllen (wobei wir voraussetzen, daß die Zerlegung gilt):*

$$d = a \cdot m + b \cdot n \quad . \tag{41}$$

Dieses Problem läßt sich mit Hilfe des erweiterten Euklid'schen Algorithmus lösen, welcher durch die folgende Anweisungsfolge definiert wird:

A1: *Initialisieren*
Setze $a' \leftarrow b \leftarrow 1,\ a \leftarrow b' \leftarrow 0,\ c \leftarrow m,\ d \leftarrow n$.

A2: *Dividieren*
Zerlege c gemäß $c = qd + r$ (wobei $0 \le r < d$) und bestimme q und r mit Hilfe von $q = c \mathbin{\mathrm{div}} d$ und $r = c \bmod d$.

A3: *Rest abfragen*
Falls $r = 0 \Rightarrow\ d = am + bn$ und Ende des Algorithmus.

A4: *Wiederholen*
Setze $c \leftarrow d,\ d \leftarrow r,\ t \leftarrow a',\ a' \leftarrow a,\ a \leftarrow t - qa,\ t \leftarrow b',\ b' \leftarrow b,\ b \leftarrow t - qb$.
Gehe zurück nach A2 .

Abb. 2 verdeutlicht graphisch in Form eines Ablaufdiagramms die Anweisungskette.

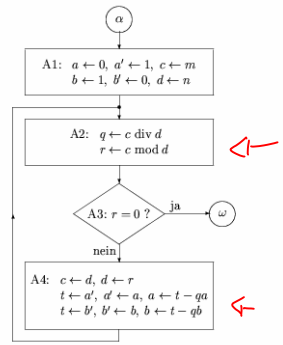

Abbildung 2: Ablaufdiagramm des erweiterten Euklid'schen Algorithmus

Beispiel 4.1: *Gegeben:* $m = 963$, $n = 657$, *gesucht:* $d = \mathrm{ggT}(m,n)$ *und ganze Zahlen* a, b, *welche* $d = am + bn$ *erfüllen.*
Der Algorithmus liefert die folgenden Ergebnisse:

a'	a	b'	b	c	d	q	r	
1	0	0	1	963	657	1	306	
0	1	1	−1	657	306	2	45	
1	−2	−1	3	306	45	6	36	
−2	13	3	−19	45	36	1	9	
13	−15	−19	22	36	9	4	0	*STOP*

und somit $9 = \mathrm{ggT}(963, 657)$ *sowie* $(-15)\cdot 963 + 22 \cdot 657 = 8845 - 8816 = 9$.

Gemäß Gl. (37) gilt die Reduktion

$$\mathrm{ggT}(m,n) = (m,n) = (\underbrace{m - q\cdot n}_{r}, n) \qquad m > n \quad . \tag{42}$$

Damit läßt sich wie beim einfachen Euklid'schen Algorithmus die Vorgehensweise nachvollziehen und wir erhalten

$$\begin{aligned}
\overbrace{(963}^{m}, \overbrace{657)}^{n} &= (\overbrace{963 - 1\cdot 657}^{r_1 = m - q_1 n}, \overbrace{657}^{n}) = (306, 657) = (\overbrace{306}^{r_1}, \overbrace{657 - 2\cdot 306}^{r_2 = m - q_2 r_1}) = (306, 45) \\
&= (\overbrace{306 - 6\cdot 45}^{r_3 = r_1 - q_3 r_2}, \overbrace{45}^{r_2}) = (36, 45) = (\overbrace{36}^{r_3}, \overbrace{45 - 1\cdot 36}^{r_4 = r_2 - q_4 r_3}) = (36, 9) \\
&= (\overbrace{36 - 4\cdot 9}^{r_3 = r_3 - q_5 r_4}, \overbrace{9}^{r_4}) = (0, 9) = 9 \quad ,
\end{aligned} \tag{43}$$

also demnach $d = r_4 = 9$, da $r_5 = 0$. Durch rückwärtige Auflösung dieser Gleichungen erhält man

$$\begin{aligned}
d = 9 &= 45 - 36 \\
&= 45 - (306 - 45\cdot 6)
\end{aligned}$$

$$\begin{aligned}
&= -306 + 7\cdot 45 \\
&= -306 + 7(657 - 306\cdot 2) \\
&= 7\cdot 657 - 15\cdot 306 \\
&= 7\cdot 657 - 15(963 - 657) \\
&= -15\cdot 963 + 22\cdot 657 \quad ,
\end{aligned} \tag{44}$$

woraus sich nun unmittelbar die ganzzahligen Unbekannten a, b zur Lösung der linearen Gleichung ablesen lassen

$$\boxed{d = a\cdot m + b\cdot n = (-15)\cdot m + 22\cdot n} \quad . \tag{45}$$

Man kann nun allerdings feststellen, daß dies nicht die einzige Lösung ist, sondern daß man daraus unendlich viele Lösungen a', b' ableiten kann:

$$a' = -15 + 657\cdot k \qquad \forall k \in \mathbb{Z} \tag{46}$$
$$b' = 22 - 963\cdot k \quad . \tag{47}$$

So erhält man z.B. für $k = 1$ die Lösung

$$\begin{aligned}
a' &= -15 + 657 = 642 \\
b' &= 22 - 963 = -941 \quad ,
\end{aligned}$$

und damit

$$9 = 642\cdot 963 - 941\cdot 657 \quad .$$

Wir werden auf diese allgemeine Lösung später noch zurückkommen.

Wir wollen nun die exemplarische Vorgehensweise des erweiterten Euklid'schen Algorithmus im obigem Zahlenbeispiel verallgemeinern. Die fortgesetzte Zerlegung läßt sich mit den im Zahlenbeispiel bereits verwendeten Variablen wie folgt aufschreiben,

wobei wiederum angenommen wird, daß $r_5 = 0$ den Algorithmus beendet

$$\begin{aligned}
m &= n\cdot q_1 + r_1 && 0 < r_1 < n \\
n &= r_1\cdot q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2\cdot q_3 + r_3 && 0 < r_3 < r_2 \\
(*)\quad r_2 &= r_3\cdot q_4 + r_4 && 0 < r_4 < r_3 \\
r_3 &= r_4\cdot q_5 + \underbrace{0}_{r_5} && \text{und damit: } d = (m,n) = r_4 \quad .
\end{aligned} \tag{48}$$

Die letzten beiden Zeilen lassen sich allgemein bei Abbruch wegen $r_{j+1} = 0$ wie folgt formulieren:

$$\boxed{\begin{aligned} r_{j-2} &= r_{j-1}\cdot q_j + r_j \qquad 0 < r_j < r_{j-1} \\ r_{j-1} &= r_j\cdot q_{j+1} + 0 \end{aligned}} \quad . \tag{49}$$

Versucht man man Gl. 48 wiederum rückwärts auzulösen, wobei man bei der vorletzten Zeile $(*)$ beginnt, so erhält man:

$$\begin{aligned}
r_4 = d &= r_2 - r_3 q_4 \\
&= r_2 - q_4(r_1 - r_2 q_3) \\
&= r_2(1 + q_3 q_4) - q_4 r_1 \\
&= (n - r_1 q_2)(1 + q_3 q_4) - q_4 r_1 \\
&= n(1 + q_3 q_4) - r_1(q_4 + q_2 + q_2 q_3 q_4) \\
&= n(1 + q_3 q_4) - (m - n q_1)(q_4 + q_2 + q_2 q_3 q_4) \\
&= n(1 + q_1 q_2 + q_1 q_4 + q_3 q_4 + q_1 q_2 q_3 q_4) - m(q_2 + q_4 + q_2 q_3 q_4) \quad .
\end{aligned} \tag{50}$$

Aus dieser unübersichtlichen Formulierung läßt sich nicht ohne weiteres ein allgemeingültiger, geschlossener Ausdruck ableiten. Wesentlich einfacher ist es, eine rekursive Auflösung zu finden. Dazu wird angenommen, daß ein Abbruch des Algorithmus bei $r_i = 0$ eine dazugehörige Lösung a_{i-1}, b_{i-1} besitzt. Man führt nun rekursiv eine Lösung mit Abbruch bei $r_i = 0$ auf die Lösung

für einen Abbruch bei $r_{i-1} = 0$ zurück. Man erhält:

$$\begin{aligned}
&\text{Für } r_1 = 0: && m = nq_1 \Rightarrow d = \underbrace{0}_{a_0}\cdot m + \underbrace{1}_{b_0}\cdot n = n \\
&\text{Für } r_2 = 0: && d = r_1 = \underbrace{1}_{a_1}\cdot m + \underbrace{(-q_1)}_{b_1}\cdot n \\
&\text{Für } r_3 = 0: && d = r_2 = n - r_1 q_2 = n - q_2(a_1 m + n b_1) \\
& && = \underbrace{(a_0 - q_2 a_1)}_{a_2}\cdot m + \underbrace{(b_0 - q_2 b_1)}_{b_2}\cdot n \\
&\text{Für } r_4 = 0: && d = r_3 = \underbrace{(a_1 - q_3 a_2)}_{a_3}\cdot m + \underbrace{(b_1 - q_3 b_2)}_{b_3}\cdot n \quad ,
\end{aligned} \tag{51}$$

oder allgemein

$$\boxed{\begin{aligned} &a_i = a_{i-2} - q_i a_{i-1} \quad ; \quad b_i = b_{i-2} - q_i b_{i-1} \qquad i = 2, 3, \ldots \\ &\text{mit:} \quad a_0 = 0,\ a_1 = 1 \quad ; \quad b_0 = 1,\ b_1 = -q_1 \end{aligned}} \tag{52}$$

Es gilt außerdem

$$b_i a_{i+1} - a_i b_{i+1} = (-1)^i \quad \text{für} \quad i \geq 0 \quad , \tag{53}$$

sowie $(a_i, b_i) = 1$.

Diese Formeln lassen sich mit Hilfe der vollständigen Induktion beweisen.

In Anlehnung an Zahlenbeispiel 4.1 sei die rekursive Lösung noch einmal aufgeschrieben. Aus $r_5 = 0$ ergibt sich die Lösung $a = a_4$, $b = b_4$. Mit den folgenden Zerlegungsquotienten $q_1 = 1$, $q_2 = 2$, $q_3 = 6$, $q_4 = 1$ ergibt sich:

$$\begin{array}{lll} i=2: & a_2 = a_0 - q_2 \cdot 1 & b_2 = b_0 - q_2 \cdot b_1 \\ & \quad = 0 - q_2 = -2 & \quad = 1 - 2 \cdot (-1) = 3 \\ i=3: & a_3 = a_1 - q_3 \cdot a_2 & b_3 = b_1 - q_3 \cdot b_2 \\ & \quad = 1 - 6 \cdot (-2) = 13 & \quad = -1 - 6 \cdot 3 = -19 \\ i=4: & a = a_4 = a_2 - q_4 \cdot a_3 & b = b_4 = b_2 - q_4 \cdot b_3 \\ & \quad = -2 - 1 \cdot 13 = \underline{\underline{-15}} & \quad = 3 - 1 \cdot (-19) = \underline{\underline{22}} \end{array} \tag{54}$$

An dieser Stelle soll der Zusammenhang einer fortgesetzten Zerlegung mit einem Kettenbruch erwähnt werden. Die Menge der Quotienten $\{q_i\}$ definiert eindeutig den Bruch m/n. Es gilt nämlich

$$\begin{aligned} \frac{m}{n} &= q_1 + \frac{r_1}{n} = q_1 + \frac{1}{n/r_1} = q_1 + \frac{1}{q_2 + \frac{1}{r_1/r_2}} \\ \frac{n}{r_1} &= q_2 + \frac{r_2}{r_1} \\ \frac{r_1}{r_2} &= q_3 + \frac{r_3}{r_2} \\ &\cdots\cdots\cdots\cdots \end{aligned} \tag{55}$$

und schließlich

$$\frac{m}{n} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\vdots}}}$$

$$\begin{aligned} &\cfrac{1}{q_{j-1} + \frac{1}{q_j}} \\ &= (q_1 + 1/(q_2 + 1/(q_3 + 1/(\ldots/(q_{j-1} + 1/q_j)\ldots)))) \\ &= \langle q_1, q_2, \ldots, q_{j-1}, q_j \rangle \quad , \end{aligned} \tag{56}$$

wobei mit den spitzen Klammern eine symbolische Schreibweise für den Kettenbruch gewählt wurde. Jede *rationale* Zahl besitzt einen *endlichen* Kettenbruch. Der Euklid'sche Algorithmus bricht demnach auch nach endlich vielen Schritten ab. Jede rationale Zahl kann genau auf zwei Arten als Kettenbruch dargestellt werden, nämlich

$$\frac{m}{n} = \langle q_1, q_2, \ldots, q_{j-1}, q_j \rangle = \langle q_1, q_2, \ldots, q_{j-1}, q_j - 1, 1 \rangle \quad . \tag{57}$$

Beispiel 4.2: **Kettenbruch einer rationalen Zahl** *Es gilt*

$$\begin{aligned} \frac{51}{22} &= \langle 2, 3, 7 \rangle = \langle 2, 3, 6, 1 \rangle \\ &= 2 + \frac{1}{\langle 3, 7 \rangle} = 2 + \frac{1}{3 + \frac{1}{7}} \\ &= 2 + \frac{1}{\langle 3, 6, 1 \rangle} = 2 + \frac{1}{3 + \frac{1}{\langle 6, 1 \rangle}} = 2 + \frac{1}{3 + \frac{1}{6+1}} \end{aligned} \tag{58}$$

Bei irrationalen Zahlen hingegen, bekommen wir einen unendlichen Kettenbruch ([11]), also z.B.

$$\sqrt{2} = \langle 1, 2, 2, \ldots \rangle \quad . \tag{59}$$

Literatur

[1] Ayres F.: Algebra - Theorie und Anwendungen. McGraw-Hill 1978.

[2] Burkhardt H., Barbosa L.C.: Contributions to the Application of the Viterbi-Algorithm. IEEE Trans. on Information Theory, vol. IT-31, no. 5, Sept. 85, S. 626-634.

[3] Mc Clellan J.H., Rader C.M.: Number Theory in Digital Signal Processing. Prentice-Hall, 1979.

[4] Gilbert W. J.: Modern Algebra with Applications. John Wiley 1976.

[5] Hamming R. W.: Information und Codierung. VCH Verlagsgesellschaft, 1987.

[6] Horowitz E., Sahni S.: Fundamentals of Computer Algorithms. Computer Science Press 1978.

[7] Knuth D. E.: The Art of Computer Programming. Vol. 1 (2. Auflage): Fundamental Algorithms. Addison-Wesley 1973.

[8] Knuth D. E.: The Art of Computer Programming. Vol. 2: Seminumerical Algorithms. Addison-Wesley 1969.

[9] Knuth D. E.: The Art of Computer Programming. Vol. 3: Sorting and Searching. Addison-Wesley 1973.

[10] Mehlhorn K.: Datenstrukturen und effiziente Algorithmen, Bd.1.

[11] Niven I., Zuckerman H.S.: Einführung in die Zahlentheorie I,II. BI-Hochschultaschenbücher Bd. 46 und 47, 1976.

[12] Waldschmidt H.: Einführung in die Informatik für Ingenieure. Oldenbourg Verlag 1980.

[13] Wirth N.: Algorithmen und Datenstrukturen (3. Auflage). Teubner Verlag 1983.