9. Der Verallgemeinerte Euklid'sche Algorithmus

Vom ggT zu Kettenbrüchen

Euklid gibt im zehnten Buch seiner *Elemente* einen Algorithmus an, um von *zwei gegebenen kommensurablen Grössen ihr grösstes gemeinsames Mass zu finden*. In neuerer Terminologie heisst das, von zwei gegebenen (positiven) Zahlen ihren *grösster gemeinsamer Teiler* (ggT) zu finden, wobei vorausgesetzt ist, dass solch ein gemeinsamer Teiler existiert.

Der Algorithmus wird wie folgt beschrieben:

(0) Die beiden Grössen seien a_0 und a_1, wobei a_0 und a_1 beide positiv sein sollen.
(1) Ist $a_0 = a_1$, so ist $a_1 = \mathrm{ggT}(a_0, a_1)$ und wir sind fertig.
(2) Sonst existiert eine grösste *natürliche Zahl* b_0, so dass gilt:

$$a_0 \geq b_0 a_1$$

b_0 ist also die kleinste natürliche Zahl für die gilt: $a_0 < (b_0 + 1) \cdot a_1$.
Beachte: Im Falle $a_0 < a_1$ ist $b_0 = 0$.
(3) Ist $a_0 = b_0 a_1$, so ist wieder $a_1 = \mathrm{ggT}(a_0, a_1)$.
(4) Ist $a_0 > b_0 a_1$, so muss gelten $a_0 - b_0 a_1 < a_1$, sonst wäre $a_0 \geq (b_0 + 1) \cdot a_1$, was der Definition von b_0 im Schritt 2 widerspricht. Weil $a_0 > b_0 a_1$ ist $a_0 - b_0 a_1 > 0$. Definieren wir nun $a_2 := a_0 - b_0 a_1$, so ist $a_0 = b_0 a_1 + a_2$ und $0 < a_2 < a_1$.
(5) Nun gehen wir mit den Zahlen a_1 und a_2 zurück zum Schritt 2 und finden eine grösste natürliche Zahl b_1, so dass $a_1 \geq b_1 a_2$.

Betrachten wir die Zahlen a_0 und a_1 als Streckenlängen (wie dies Euklid getan hat), so ist es nicht schwierig einzusehen, dass dieser Algorithmus die grösste Strecke liefert, welche in beiden Strecken enthalten ist. Mit Zahlen ausgedrückt liefert der Algorithmus also den grössten gemeinsamen Teiler der Zahlen a_0 und a_1.

Ein Vorteil des Euklid'schen Algorithmus zur Berechnung des ggT's zweier Zahlen ist, dass wir nicht zuerst die Primfaktorzerlegung der beiden Zahlen bestimmen müssen, und wir somit auch von relativ grossen Zahlen den ggT berechnen können.

Beispiel: Für $a_0 = 986$ und $a_1 = 357$ erhalten wir:

$$\begin{aligned} 986 &= 2 \cdot 357 + 272 \\ 357 &= 1 \cdot 272 + 85 \\ 272 &= 3 \cdot 85 + 17 \\ 85 &= 5 \cdot 17 + 0 \end{aligned}$$

Damit ist $\mathrm{ggT}(986, 357) = 17$. Insbesondere erhalten wir $a_2 = 272$, $a_3 = 85$, $a_4 = 17$, $a_5 = 0$, und ferner ist $b_0 = 2$, $b_1 = 1$, $b_2 = 3$, $b_3 = 5$.

Von diesem Algorithmus ist es nun ein kleiner Schritt zu den sogenannten *Kettenbrüchen*: Ein **endlicher Kettenbruch** ist ein Bruch von der Form

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots \cfrac{1}{b_{n-1} + \cfrac{1}{b_n}}}}}}$$

wobei $b_0, \ldots, b_n$ ganze Zahlen und höchstens mit Ausnahme von b_0 alle b_i positiv sind.

Wir stellen uns nun die Frage, ob sich jeder Bruch der Form $\frac{a_0}{a_1}$ als endlicher Kettenbruch schreiben lässt, und wenn ja, wie wir den entsprechenden Kettenbruch berechnen können. Um dies zu beantworten, gehen wir wie folgt vor:

Zuerst berechnen wir mit dem Euklid'schen Algorithmus den ggT von a_0 und a_1.

$$\begin{array}{rcll}
a_0 &=& b_0 \cdot a_1 + a_2 & \Rightarrow \quad \dfrac{a_0}{a_1} = b_0 + \dfrac{a_2}{a_1} = b_0 + \dfrac{1}{\frac{a_1}{a_2}} \\
a_1 &=& b_1 \cdot a_2 + a_3 & \Rightarrow \quad \dfrac{a_1}{a_2} = b_1 + \dfrac{a_3}{a_2} = b_1 + \dfrac{1}{\frac{a_2}{a_3}} \\
a_2 &=& b_2 \cdot a_3 + a_4 & \Rightarrow \quad \dfrac{a_2}{a_3} = b_2 + \dfrac{a_4}{a_3} = b_2 + \dfrac{1}{\frac{a_3}{a_4}} \\
&\vdots & & \qquad\quad \vdots \\
a_n &=& b_n \cdot a_{n+1} + 0 & \Rightarrow \quad \dfrac{a_n}{a_{n+1}} = b_n
\end{array}$$

Es gilt also

$$\frac{a_0}{a_1} = b_0 + \frac{1}{\frac{a_1}{a_2}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\frac{a_2}{a_3}}} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\frac{a_3}{a_4}}}}$$

und allgemein erhalten wir

$$\frac{a_0}{a_1} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \cfrac{1}{\ddots \cfrac{1}{b_{n-1} + \cfrac{1}{b_n}}}}}}$$

Dieser letzte Ausdruck ist nun ein endlicher Kettenbruch, den wir der besseren Lesbarkeit wegen mit $[b_0, b_1, \ldots, b_n]$ bezeichnen.

Da der Bruch $\frac{a_0}{a_1}$ beliebig war, können wir also *jeden* Bruch (d. h. jede rationale Zahl) als endlichen Kettenbruch schreiben. Es gilt natürlich auch das Umgekehrte, nämlich dass jeder endliche Kettenbruch einer rationalen Zahl entspricht, denn jeder endliche Kettenbruch kann in einen normalen Bruch umgewandelt werden.

Zum Beipiel haben wir $\frac{986}{357} = [2, 1, 3, 5]$, denn:

$$\frac{986}{357} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{5}}}$$

Verwandeln wir den Kettenbruch $[2, 1, 3, 5]$ in einen normalen Bruch, so erhalten wir nicht $\frac{986}{357}$, sondern $\frac{58}{21}$, also einen gekürzten Bruch (es gilt $\frac{58}{21} = \frac{58 \cdot 17}{21 \cdot 17} = \frac{986}{357}$). Aus Proposition 9.1 und Lemma 9.2 wird folgen, dass dies immer der Fall ist, denn verwandeln wir einen Kettenbruch in einen normalen Bruch, so ist dieser Bruch *immer* gekürzt.

Wir wollen nun untersuchen, was passiert, wenn die Grössen (bzw. reellen Zahlen) a_0 und a_1 keinen gemeinsamen Teiler haben. Dafür setzen wir zum Beispiel $a_0 = \sqrt{2}$ und $a_1 = 1$:

$$\begin{array}{ccccccc}
 & & \frac{\sqrt{2}}{1} & = & 1 & + & (\sqrt{2} - 1) \\
\frac{1}{\sqrt{2}-1} & = & \frac{\sqrt{2}+1}{1} & = & 2 & + & (\sqrt{2} - 1) \\
\frac{1}{\sqrt{2}-1} & = & \frac{\sqrt{2}+1}{1} & = & 2 & + & (\sqrt{2} - 1) \\
 & & \vdots & & \vdots & & \vdots
\end{array}$$

Der Euklid'sche Algorithmus angewandt auf $a_0 = \sqrt{2}$ und $a_1 = 1$ bricht nie ab und liefert uns somit unendlich viele positive natürliche Zahlen b_n. Das heißt, dass der Kettenbruch von $\frac{a_0}{a_1} = \sqrt{2}$ *unendlich* ist. In unserem Fall erhalten wir den Kettenbruch

$$[1, 2, 2, 2, 2, \ldots] = [1, \overline{2}\,].$$

Ein **unendlicher Kettenbruch** ist ein nicht abbrechender Bruch von der Form

$$b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{\ldots}}}$$

wobei $b_0, b_1, b_2 \ldots$ ganze Zahlen und höchstens mit Ausnahme von b_0 alle b_i positiv sind.

Ist $\xi \in \mathbb{R}$ eine beliebige, positive, irrationale Zahl, so können wir ξ immer als unendlichen Kettenbruch schreiben. Dazu definieren wir für positive reelle Zahlen α,

$$\lfloor \alpha \rfloor := \max\{n \in \mathbb{N} : n \leq \alpha\}.$$

Dann gilt:

$$\begin{array}{ccccccl}
\xi & = & b_0 & + & r_1 & & \text{mit } b_0 := \lfloor \xi \rfloor \text{ und } r_1 := \xi - b_0, \text{ wobei } 0 < r_1 < 1 \text{ bzw. } \frac{1}{r_1} > 1 \\
\frac{1}{r_1} & = & b_1 & + & r_2 & & \text{mit } b_1 := \lfloor \frac{1}{r_1} \rfloor \text{ und } r_2 := \frac{1}{r_1} - b_1, \text{ wobei } 0 < r_2 < 1 \text{ bzw. } \frac{1}{r_2} > 1 \\
\frac{1}{r_2} & = & b_2 & + & r_3 & & \text{mit } b_2 := \lfloor \frac{1}{r_2} \rfloor \text{ und } r_3 := \frac{1}{r_2} - b_2, \text{ wobei } 0 < r_3 < 1 \text{ bzw. } \frac{1}{r_3} > 1 \\
\vdots & & \vdots & & \vdots & &
\end{array}$$

und wir erhalten den Kettenbruch $[b_0, b_1, b_2, \ldots]$.

Es stellt sich nun die Frage, wie der Kettenbruch $[b_0, b_1, b_2, \ldots]$ mit ξ zusammenhängt. Ein natürlicher Ansatz ist, den unendlichen Kettenbruch jeweils nach endlich vielen Schritten abzubrechen und die entsprechenden rationalen Zahlen zu berechnen. Wie wir zeigen werden, nähern sich diese rationalen Zahlen der irrationalen Zahl ξ an, deshalb werden sie *Näherungsbrüche* genannt. Zum Beispiel erhalten wir für den unendlichen Kettenbruch $[1, \overline{2}]$ die folgenden Näherungsbrüche $\frac{P_n}{Q_n}$:

$$\frac{P_0}{Q_0} = \frac{1}{1}, \quad \frac{P_1}{Q_1} = \frac{3}{2}, \quad \frac{P_2}{Q_2} = \frac{7}{5}, \quad \frac{P_3}{Q_3} = \frac{17}{12}, \quad \frac{P_4}{Q_4} = \frac{41}{29}, \ldots$$

Näherungsbrüche sind immer gekürzte Brüche welche, wie wir sehen werden, relativ schnell konvergieren. Wir können also zum Beispiel $\sqrt{2}$ beliebig genau berechnen. Was uns noch fehlt, ist ein einfacher Algorithmus, welcher uns erlaubt, die Näherungsbrüche ohne grossen Aufwand zu berechnen; dies liefert die folgende rekursive Formel:

$$\begin{aligned} P_{-2} &:= 0, \qquad P_{-1} := 1, \qquad P_n := b_n P_{n-1} + P_{n-2} \\ Q_{-2} &:= 1, \qquad Q_{-1} := 0, \qquad Q_n := b_n Q_{n-1} + Q_{n-2} \end{aligned}$$

Graphisch dargestellt erhalten wir für den Kettenbruch $[1, \overline{2}]$ folgendes Schema:

n	*-2*	*-1*	*0*	*1*	*2*	*3*	*4*	...
b_n			1	2	2	2	2	...
P_n	**0**	**1**	1	3	7	17	41	...
Q_n	**1**	**0**	1	2	5	12	29	...

Jede Zahl der dritten Zeile entsteht, indem man die darüberstehende mit der vorausgehenden Zahl der dritten Zeile multipliziert und die nächstvorausgehende addiert; analog für die vierte Zeile.

Diesen Algorithmus zur Berechnung von Näherungsbrüchen nennen wir **verallgemeinerter Euklid'scher Algorithmus**, abgekürzt **vEA**. Wir zeigen nun, dass der vEA korrekt ist, bzw. dass die Brüche $\frac{P_n}{Q_n}$ tatsächlich Näherungsbrüche sind.

PROPOSITION 9.1. *Sei $[b_0, b_1, \ldots]$ ein unendlicher Kettenbruch. Dann gilt für alle natürlichen Zahlen n:*

$$[b_0, \ldots, b_n] = \frac{P_n}{Q_n}$$

wobei die Zahlen P_n und Q_n mit dem vEA *berechnet werden.*

Beweis. Den Beweis führen wir mit Induktion nach n.

$n = 0$: Es gilt $P_0 = b_0$ und $Q_0 = 1$, also ist $\frac{P_0}{Q_0} = b_0 = [b_0]$.

Annahme: $[b_0, \ldots, b_n] = \frac{P_n}{Q_n}$ für ein $n \in \mathbb{N}$.

Wir müssen nun zeigen, dass aus der Annahme folgt: $[b_0, \ldots, b_n, b_{n+1}] = \frac{P_{n+1}}{Q_{n+1}}$. So, wie die Kettenbrüche aufgebaut sind, gilt:

$$[b_0, \ldots, b_n, b_{n+1}] = [b_0, \ldots, b_n + \frac{1}{b_{n+1}}]$$

Setzen wir $b'_n := b_n + \frac{1}{b_{n+1}}$, so erhalten wir

$$[b_0, \ldots, b_{n-1}, b_n + \frac{1}{b_{n+1}}] = [b_0, \ldots, b_{n-1}, b'_n]\,.$$

Wenn wir nun mit dem Algorithmus den Näherungsbruch $\frac{P'_n}{Q'_n}$ von $[b_0, \ldots, b'_n]$ berechnen, so erhalten wir $P'_n = b'_n P_{n-1} + P_{n-2}$, also

$$P'_n = \Big(b_n + \frac{1}{b_{n+1}}\Big) P_{n-1} + P_{n-2} = \quad \cdots \quad = \frac{b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}}{b_{n+1}}\,,$$

und entsprechend

$$Q'_n = \frac{b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}}{b_{n+1}}\,.$$

Somit haben wir:

$$[b_0, \ldots, b_{n-1}, b'_n] = \frac{P'_n}{Q'_n} = \frac{b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}}{b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}}$$

Da nun

$$[b_0, \ldots, b_{n-1}, b'_n] = [b_0, \ldots, b_{n-1}, b_n + \frac{1}{b_{n+1}}] = [b_0, \ldots, b_{n-1}, b_n, b_{n+1}]$$

müssen wir nur noch zeigen, dass die Gleichung $\frac{P'_n}{Q'_n} = \frac{P_{n+1}}{Q_{n+1}}$ gilt. Dazu schreiben wir P_{n+1} und Q_{n+1} etwas um: Mit dem Algorithmus erhalten wir $P_{n+1} = b_{n+1}P_n + P_{n-1}$, und wenn wir P_n durch $b_n P_{n-1} + P_{n-2}$ ersetzen, erhalten wir

$$P_{n+1} = b_{n+1}(b_n P_{n-1} + P_{n-2}) + P_{n-1} = b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}\,,$$

und entsprechend

$$Q_{n+1} = b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}\,.$$

Somit ist $\frac{P'_n}{Q'_n} = \frac{b_{n+1}b_n P_{n-1} + P_{n-1} + b_{n+1}P_{n-2}}{b_{n+1}b_n Q_{n-1} + Q_{n-1} + b_{n+1}Q_{n-2}} = \frac{P_{n+1}}{Q_{n+1}}$ und der Algorithmus ist korrekt. ⊣

Bemerkung: Als Folgerung aus Proposition 9.1 erhalten wir, dass wenn $[b_0, \ldots, b_n]$ der endliche Kettenbruch von $\frac{a}{b} \in \mathbb{Q}$ ist, immer $\frac{P_n}{Q_n} = \frac{a}{b}$ gilt.

Das folgende Lemma ist wichtig, um multiplikativ Inverse in speziellen Ringen, sogenannten *euklidischen Ringen*, zu berechnen.

LEMMA 9.2. *Sind $\frac{P_n}{Q_n}$ (für $n \in \mathbb{N}$) die zum Kettenbruch $[b_0, b_1, b_2, \ldots]$ gehörenden Näherungsbrüche, so gilt für alle $n \geq -1$:*

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$$

Beweis. Für den Beweis verwenden wir Induktion über n.
Für $n = -1$ ist $P_n = Q_{n-1} = 1$ und $P_{n-1} = Q_n = 0$, also

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}.$$

Gilt $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n-1}$ für ein $n \geq -1$, so ist

$$P_{n+1}Q_n - P_n Q_{n+1} = (b_{n+1}P_n + P_{n-1})Q_n - P_n(b_{n+1}Q_n + Q_{n-1}) = \\ P_{n-1}Q_n - P_n Q_{n-1} = -(-1)^{n-1} = (-1)^n,$$

womit die Behauptung bewiesen ist. ⊣

Bemerkung: Als Folgerung aus Lemma 9.2 erhalten wir, dass die Näherungsbrüche $\frac{P_n}{Q_n}$ immer gekürzt sind. Denn wäre $\mathrm{ggT}(P_n, Q_n) = d > 1$, so hätten wir $d \mid (qP_n - p\,Q_n)$ (für alle $p, q \in \mathbb{Z}$), und somit $|qP_n - p\,Q_n| \neq 1$.

EINDEUTIGKEIT DER PRIMFAKTORZERLEGUNG

Als Anwendung des vEA zeigen wir die Eindeutigkeit der Primfaktorzerlegung natürlicher Zahlen $n \geq 2$. Dazu beweisen wir zuerst folgendes Hilfsresultat:

LEMMA 9.3. *Seien $a, b, c \in \mathbb{N}$ positive Zahlen mit $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt $a \mid c$.*

Beweis. Sei $[b_0, \ldots, b_n]$ der Kettenbruch von $\frac{a}{b}$. Ist $n = 0$, so ist $b = 1$ und $a \mid c$. Ist $n > 1$, so ist, weil $\mathrm{ggT}(a, b) = 1$, $P_n = a$ und $Q_n = b$, und mit Lemma 9.2 gilt $a \cdot Q_{n-1} - b \cdot P_{n-1} = (-1)^{n-1}$. Somit existieren $k, l \in \mathbb{Z}$ mit $|k| = Q_{n-1}$ und $|l| = P_{n-1}$ sodass gilt $ak + bl = 1$. Weil $a \mid bc$ existiert ein $s \in \mathbb{N}$ mit $as = bc$. Nun ist

$$c = c \cdot 1 = c \cdot (ak + bl) = ack + bcl = ack + asl = a \cdot \underbrace{(ck + sl)}_{=:t} = a \cdot t$$

und wir erhalten $a \mid c$. ⊣

Eine Zahl $p \in \mathbb{N}$, $p > 1$, ist eine **Primzahl**, wenn aus $n \mid p$ folgt $n = 1$ oder $n = p$. Mit Induktion über $m \in \mathbb{N}$ lässt sich einfach zeigen, dass sich jede Zahl $m \in \mathbb{N}$ mit $m > 1$ als Produkt von Primzahlen schreiben lässt. Der folgende Satz besagt, dass dieses Produkt (bis auf die Reihenfolge der Faktoren) eindeutig ist.

THEOREM 9.4. *Für positive Zahlen $n, m \in \mathbb{N}$ seien*

$$a = \prod_{i \in n} p_i \quad \text{und} \quad b = \prod_{j \in m} q_j$$

wobei die p_i und q_j Primzahlen sind. Ist $a = b$, so ist $n = m$ und es existiert eine Bijektion $\pi : n \to m$ mit $p_i = q_{\pi(i)}$ für alle $i \in n$.

Beweis. Beweis mit Induktion nach n: Ist $n = 1$, so ist $a = p_0$ und $b = q_0$ und aus $a = b$ folgt $p_0 = q_0$. Sei $n > 1$ und sei der Satz bewiesen für $n - 1$. Für $n > 1$ gilt $p_0 \mid a$ und aus $a = b$ folgt somit $p_0 \mid b$ also

$$p_0 \mid q_0 \cdot \prod_{j \in m-1} q_{j+1}.$$

Gilt $p_0 \mid q_0$, so erhalten wir, weil p_0 und q_0 prim sind, $p_0 = q_0$ und wir können die Induktionsvoraussetzung anwenden auf

$$\prod_{i \in n-1} p_{i+1} = \prod_{j \in m-1} q_{j+1}.$$

Gilt $p_0 \nmid q_0$, so erhalten wir mit Lemma 9.3

$$p_0 \mid q_1 \cdot \prod_{j \in m \setminus 2} q_j.$$

Gilt $p_0 \mid q_1$, so ist $p_0 = q_1$, andernfalls wenden wir wieder Lemma 9.3 an. So fortgefahren, finden wir schliesslich ein $j_0 \in m$ für das gilt $p_0 = q_{j_0}$ und wir können die Induktionsvoraussetzung anwenden auf

$$\prod_{i \in n-1} p_{i+1} = \prod_{j \in m \setminus \{j_0\}} q_j.$$

⊣

Als Folgerung aus Theorem 9.4 erhalten wir nun leicht

KOROLLAR 9.5. *Jede natürliche Zahl $n \geq 2$ lässt sich, bis auf Vertauschung der Faktoren, eindeutig als Produkt von Primzahlen schreiben.*