WiSe '21/'22, hhu
K. Halupczok

Vorlesung Einführung in die Zahlentheorie

EZ4: Kettenbrüche

Stichworte: Endlicher Kettenbruch, Teilnenner, Kettenbruchentwicklung (KBE), Näherungsbruch (NB), Rekursionsformeln für NBe, normierter KB, erweiterter euklidischer Algorithmus = Schema zur Berechnung der Bézout-Koeffizienten

---

4.1. Einleitung: Der euklidische Algorithmus wird so erweitert, dass er ein explizites und schnelles Rechenverfahren zur Bestimmung von Bézout-Koeffizienten liefert.

4.2. Motivation: Setze $\alpha = \frac{b}{a} \in \mathbb{Q}$ (prinzipiell kann $\alpha \in \mathbb{R}$ eine beliebige reelle Zahl sein).

$\rightsquigarrow$ Schema: $\alpha = \underbrace{\lfloor \alpha \rfloor}_{=:q_0} + \varepsilon$ mit $0 \le \varepsilon < 1$. Falls $\alpha \notin \mathbb{Z}$, ist $\varepsilon \neq 0$, setze $s_1 = \frac{1}{\varepsilon} > 1$.

$\rightsquigarrow \alpha = q_0 + \frac{1}{s_1}$ mit $s_1 > 1$. Falls $s_1 \notin \mathbb{Z}$, s.o.

$s_1 = \underbrace{q_1}_{:=\lfloor s_1 \rfloor} + \frac{1}{s_2}$ mit $s_2 > 1$. $\quad\vdots$ $\quad$ (Somit: $s_k = \frac{r_{k-1}}{r_k}$, $k \ge 1$.)

$\vdots$

$s_k = q_k + \frac{1}{s_{k+1}}$, abbrechen, wenn $s_n \in \mathbb{Z}$, sonst weiter.

Es halten so in ℓ Schritten: $\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_k + \frac{1}{s_{k+1}}}}}$

Da der euklidische Algo abbricht bei $r_m \neq 0$ mit $s_n = \frac{r_{m-1}}{r_m} = q_m \in \mathbb{Z}$, stellt damit ein endlicher Kettenbruch die rationale Zahl α dar.

4.3. Def.: (1) Seien $q_0, q_1, \dots, q_m$ ganze Zahlen (allg.: reelle Zahlen) mit $q_1, \dots, q_m > 0$. Unter dem endlichen Kettenbruch $[q_0; q_1, q_2, \dots, q_m]$ verstehen wir sowohl das $(m+1)$-Tupel $(q_0, q_1, \dots, q_m)$ als auch seinen Wert $[q_0; q_1, \dots, q_m] := q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + 1/q_m}}$.

Man nennt $[q_0; q_1, \dots, q_m]$ einen $(m+1)$-gliedrigen Kettenbruch. Die $q_1, q_2, \dots, q_m$ heißen Teilnenner. (engl. partial quotient/denominator. Die Übersetzung "Teilbrüche" ist irreführend.)

(2) Für $0 \le k \le m$ nennen wir den Kettenbruch $s_k := [q_k; q_{k+1}, \dots, q_m]$ den k-ten Rest des Kettenbruches in (1).

Wir haben so $s_0 = [q_0; q_1, \dots, q_m]$, $s_1 = [q_1; q_2, \dots, q_m]$, $\dots$, $s_m = [q_m] = q_m$.

Für den Wert des Kettenbruches in (1) gilt $[q_0; q_1, \dots, q_m] = [q_0; q_1, \dots, q_{k-1}, s_k]$ für $0 \le k \le m$.

4.4. **Bem.:** Eine rekursive Def. des Wertes in 4.3(1) ist auch möglich:
$[q_0] := q_0$, $[q_0; q_1] = q_0 + \frac{1}{q_1}$, und für $n \geq 1$: $[q_0; q_1, \dots, q_n] = [q_0; s_1] = q_0 + \frac{1}{s_1}$
(wo $s_1 > 0$ per Rekursion). Oder auch: $[q_0; q_1, \dots, q_n] = [q_0; q_1, \dots, q_{n-1}, s_{n-1}]$
$= [q_0; q_1, \dots, q_{n-2}, q_{n-1} + \frac{1}{q_n}]$ (ist n-gliedrig).

4.5. Wir behandeln hier nur endliche KBe. Die Berechnung der Teilnenner heißt Kettenbruchentwicklung.

4.6. **Abkürzungen:** KB = Kettenbruch, KBE = Kettenbruchentwicklung.

4.7. **Def.:** Jedem endlichen KB $[q_0; q_1, \dots, q_k]$ ordnen wir rekursiv ein Paar $(c,d) \in \mathbb{Z} \times \mathbb{N}$ zu gemäß der Rekursion: $k=0$: $\binom{c}{d} := \binom{q_0}{1}$

$k \geq 1$: $\binom{c}{d} := \binom{q_0 c' + d'}{c'} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \binom{c'}{d'}$,

wo (c', d') zum KB $s_1 = [q_1; q_2, \dots, q_n]$ gehöre.

4.8. **Beh.:** Es gilt $\frac{c}{d} = [q_0; q_1, \dots, q_k]$.

Bew.: $k=0$: $[q_0] = q_0 = \frac{c}{d}$ ✓, $k \geq 1$: $[q_0; q_1, \dots, q_k] = q_0 + \frac{1}{s_1} \overset{IV}{=} q_0 + \frac{d'}{c'} = \frac{q_0 c' + d'}{c'} = \frac{c}{d}$ ✓

(**Bem.:** wegen $s_1 > 0, d' > 0$ ist $c' > 0$.) □

4.9. **Def.:** Sei $[q_0; q_1, q_2, \dots, q_n]$ ein endlicher KB.
Das dem k-ten Abschnitt $[q_0; q_1, q_2, \dots, q_k]$, $k \geq 0$, aus 4.7 zugeordnete Paar $\binom{c_k}{d_k}$ heißt k-ter Näherungsbruch des KBes. Auch $\frac{c_k}{d_k}$ heißt k-ter Näherungsbruch. Aus formalen Gründen setzen wir
$\binom{c_{-1}}{d_{-1}} = \binom{1}{0}$, $\binom{c_{-2}}{d_{-2}} = \binom{0}{1}$.

4.10. **Beobachtung** (vgl. 4.14): Ist der KB endlich, etwa $= [q_0; q_1, \dots, q_n]$,
so ist der n-te Näherungsbruch $\frac{c_n}{d_n}$ gleich dem Wert dieses KBes.
Abkürzung: NB = Näherungsbruch (engl. convergent. Die Übersetzung "Konvergente" ist eher irreführend)

4.11. **Lemma** (Rekursionsformeln für NBe): Bezeichnungen wie eben in 4.9, setze

$c_{-2} = 0$, $c_{-1} = 1$, $c_0 = q_0$,
$d_{-2} = 1$, $d_{-1} = 0$, $d_0 = 1$.

Dann: $c_k = q_k c_{k-1} + c_{k-2}$,
$d_k = q_k d_{k-1} + d_{k-2}$, $k = 0, 1, 2, \dots$ ($k \leq n$ bei endl. KB)

In Matrizenform: $\binom{c_k}{d_k} = \underbrace{\begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix}}_{=: M_k} \binom{q_k}{1}$ (*).

Bem.: Die Rekursionen zeigen $d_k > 0$ für $k \geq 0$. (Und $d_k \geq d_{k-1}$, $c_k \geq c_{k-1}$ für $q_i \geq 1$.)

Bew. (von 4.11): Setzen $M_i := \begin{pmatrix} c_{i-1} & c_{i-2} \\ d_{i-1} & d_{i-2} \end{pmatrix}$ für $i = 0, 1, 2, \ldots$, also $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $M_1 = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}$.
Es gilt $\begin{pmatrix} c_0 \\ d_0 \end{pmatrix} = \begin{pmatrix} q_0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} q_0 \\ 1 \end{pmatrix}$, also ist ⊛ richtig für $k = 0$.
Weiter: habe $[q_1; q_2, \ldots, q_m]$ die NBe $\begin{pmatrix} c_i' \\ d_i' \end{pmatrix}$ mit $-2 \le i \le n-1$, $n \ge 1$.
Dann ist per Def. 4.7: $\begin{pmatrix} c_i \\ d_i \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c_{i-1}' \\ d_{i-1}' \end{pmatrix} = M_1 \begin{pmatrix} c_{i-1}' \\ d_{i-1}' \end{pmatrix}$ für $i \ge -1$.
Induktionsschritt: Sei $k \ge 1$ und Beh. wahr für $k-1$. Dann gilt für $[q_1; q_2, \ldots, q_m]$ nach Ind. vor. mit $n = k$: $\begin{pmatrix} c_{k-1}' \\ d_{k-1}' \end{pmatrix} = \begin{pmatrix} c_{k-2}' & c_{k-3}' \\ d_{k-2}' & d_{k-3}' \end{pmatrix}\begin{pmatrix} q_k \\ 1 \end{pmatrix}$. Wollen Rekursion für $[q_0; q_1, \ldots, q_m]$ zeigen. Aus $\begin{pmatrix} c_k \\ d_k \end{pmatrix} = M_1 \begin{pmatrix} c_{k-1}' \\ d_{k-1}' \end{pmatrix}$ folgt

$$\begin{pmatrix} c_k \\ d_k \end{pmatrix} = M_1 \begin{pmatrix} c_{k-1}' \\ d_{k-1}' \end{pmatrix} = M_1 \begin{pmatrix} c_{k-2}' & c_{k-3}' \\ d_{k-2}' & d_{k-3}' \end{pmatrix}\begin{pmatrix} q_k \\ 1 \end{pmatrix} = \left(M_1\begin{pmatrix} c_{k-2}' \\ d_{k-2}' \end{pmatrix}, M_1\begin{pmatrix} c_{k-3}' \\ d_{k-3}' \end{pmatrix}\right)\cdot\begin{pmatrix} q_k \\ 1 \end{pmatrix} = \begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix}\begin{pmatrix} q_k \\ 1 \end{pmatrix}$$

↪ ⊛ ✓ □

4.12 Lemma: Mit den Bezeichnungen 4.9/4.11 gilt: (1) $M_{k+1} = M_k \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$, $k = 0, 1, 2, \ldots$,
(2) $M_{k+1} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$, $k = 0, 1, 2, \ldots$
(3) $d_k c_{k-1} - c_k d_{k-1} = (-1)^k$ für $k \ge -1$

Bew.: (1) ✓
(2): $M_k \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c_{k-1} & c_{k-2} \\ d_{k-1} & d_{k-2} \end{pmatrix}\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c_k & c_{k-1} \\ d_k & d_{k-1} \end{pmatrix} = M_{k+1}$, $k = 0, 1, \ldots$, $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightsquigarrow$ (2) ✓
(3): $c_k d_{k-1} - c_{k-1} d_k = \det(M_{k+1}) \overset{(2)}{=} \underbrace{\det\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}}_{=-1} \cdots \underbrace{\det\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}}_{=-1} = (-1)^{k+1}$, $k \ge 0 \rightsquigarrow$ (3) ✓ □

4.13 Korollar: Die NBe eines KBs lassen sich nicht kürzen, d.h. $(c_k, d_k) = 1$ für $k \ge -2$.
Bew.: $d_k c_{k-1} - c_k d_{k-1} = (-1)^k$ für $k \ge -1$ nach Lemma 4.12 (3), also $(c_{k-1}, d_{k-1}) = 1$. □

4.14 Bem.: Ist $\alpha \in \mathbb{Q}$, so hat α die Darstellung $\alpha = [q_0; q_1, \ldots, q_m]$ als endl. KB, oder, falls $m \ge 1$, mit einem $q_m \ge 2$ endet.
1. Bew.: Für $\alpha \in \mathbb{Z}$ ist $\alpha = [q_0] = q_0$ ✓, für $\alpha \notin \mathbb{Z}$ liefert der endl. Algo. die KB darstellung mit $m \ge 1$ und $q_m = \frac{r_{m-1}}{r_m} \ge 2$.
2. Bew.: Sei $\alpha = [q_0; q_1, \ldots, q_m]$, $m \ge 1$, $q_m = 1$. Für $m = 1$ ist $\alpha = q_0 + \frac{1}{q_1} = q_0 + 1 \in \mathbb{Z}$, also $\alpha = [q_0 + 1]$. ✓
Für $m \ge 2$ ist $s_{m-1} = q_{m-1} + \frac{1}{q_m} = q_{m-1} + 1 \in \mathbb{Z}_{\ge 2}$, also $\alpha = [q_0; q_1, \ldots, q_{m-2}, s_{m-1}] = [q_0; q_1, \ldots, q_{m-2}, q_{m-2} + 1]$.

4.15. **Def.:** Ein (endl.) KB, der nicht mit 1 endet, falls er nicht von der Form $[q_0]$ ist, heißt ein (endl.) normierter KB.

4.16. **Bem.:** Sind $[q_0; q_1, \dots, q_m]$ und $[q_0'; q_1', \dots, q_n']$ mit $n \geq m$ beide normiert vom selben Wert α, so folgt $m = n$ und $q_i' = q_i$ für alle i.

Bew.: Sei $n > 0$. Dann ist $\alpha = q_0 + \frac{\wedge}{s_1}$ und $s_1 > 1$ wegen Normiertheit. Also ist $\alpha \notin \mathbb{Z}$. Daher ist auch $m > 0$. Dann ist $q_0 + \frac{\wedge}{s_1} = q_0' + \frac{\wedge}{s_1'}$ mit $s_1' > 1$. Es folgt $q_0 = \lfloor \alpha \rfloor = q_0'$, also $s_1 = s_1'$. Dann Induktion. Im Fall $n = 0$ ist $m = 0$ und Beh. klar. □

4.17. **Bsp.:** $1 + \frac{\wedge}{2} = 1 + \frac{\wedge}{1 + \frac{\wedge}{1}}$ sind zwei KB-Darstellungen von $\frac{3}{2}$, der zweite KB ist nicht normiert.

Die Eindeutigkeit der Darstellung als KB gilt bei rationalen Zahlen nur mit normierten KBen. Der euklidische Algorithmus liefert die Darstellung mit dem normierten KB.

4.18. **Altes Bsp.:** $b = 133$, $a = 84$, Bestimmung der q_i:

$133 : 84 = 1$ q_0

$84 : 49 = 1$ q_1

$49 : 35 = 1$ q_2

$35 : 14 = 2$ q_3

$14 : 7 = 2$ (Rest 0) q_4 ↝ 7: letzter Rest $\neq 0$, ist ggT

Tabelle:

k		0	1	2	3	4
q_k		1	1	1	2	2
c	0 1	1	2	3	8	19
d	1 0	1	1	2	5	12
$\frac{c}{d}$		$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{8}{5}$	$\frac{19}{12}$

Zelle = vorletzte Zelle + letzter Zelle mal q_k-Wert darüber

= Rekursionen

↝ $n = 4$, $r_4 = 7$ → Haben $8 \cdot 84 - 5 \cdot 133 = 7$, wir können die Bézout-Elemente von a, b direkt ablesen (in der vorletzten Spalte, bis aufs VZ).

vorletzte Spalte

letzte Spalte: $\frac{c_n}{d_n} = \frac{r_n c_n}{r_n d_n} = \frac{b}{a}$

Mit $d_n c_{n-1} - c_n d_{n-1} = (-1)^n$ $\Leftrightarrow$ $d_n r_n \cdot c_{n-1} - c_n r_n \cdot d_{n-1} = (-1)^n r_n$

$\Leftrightarrow$ $a c_{n-1} - b d_{n-1} = (-1)^n r_n$

und $n = 4$: $a c_3 - b d_3 = + r_n$, wo $c_3 = 8$, $d_3 = 5$

+, da n gerade

↝ $8 \cdot 84 - 5 \cdot 133 = 7$ ✓

4.19. **Algorithmus zur Berechnung der Bézout-Elemente:**

Führe den erkl. Algo. und obiges Schema durch bis Schritt n, bei dem sich $\frac{a}{b} = \frac{c_n}{d_n}$, $(c_n, d_n)=1$ ergibt. In Spalte $n-1$ des Schemas stehen dann c_{n-1}, d_{n-1}, für die $c_{n-1}\,a - d_{n-1}\,b = (-1)^n r_n$ gilt, d.h. bis auf das VZ sind dies die Bézout-El.

Korrektheit:

Betr. $\frac{b}{a}$ mit $a>0$. Haben $\frac{b}{a} = \frac{r_n b'}{r_n a'}$, mit $\begin{matrix} b'=c_n, \\ a'=d_n \end{matrix}$ und dem letzten Rest $r_n \neq 0$, d.h. $r_n = (a,b)$.

Nach Lemma 4.12(3) gilt

$d_n c_{n-1} - c_n d_{n-1} = (-1)^n$, wegen $b'=c_n$, $a'=d_n$ also

$c_{n-1}\,a' - d_{n-1}\,b' = (-1)^n$, nach Multiplikation mit r_n folgt die Beh. □

4.20. **Bem.:** Das Rechenschema 4.19 ist auch als erweiterter/verallgemeinerter euklidischer Algorithmus bekannt.

Zuletzt noch eine bekannte Anwendung der Kettenbruchtheorie.

4.21. **Ein guter Kalender:**

Ein Sonnenjahr dauert 365 Tage, 5 Stunden, 48 Min. und 45,8 Sekunden, also etwa $\approx 365 + \underbrace{\frac{104\,629}{432\,000}}_{\approx 1/4}$ Tage. $(= 365.2425$ Tage$)$

Man bekommt den julianischen Kalender mit einem Schaltjahr alle 4 Jahre.

Die komplette KBE: $\frac{104\,629}{432\,000} = [0; 4, 7, 1, 3, 6, 2, 1, 170]$

Diese liefert etwa die Approximation $[0;4,7,1,3,6] = \frac{194}{801}$.

Dies führt auf unseren aktuellen gregorianischen Kalender:

Innerhalb von 800 Jahren müssen $6 = 200 - 194$ Schalttage ausfallen. Dies wurde so festgesetzt, dass dies für alle Jahre gilt, deren Jahreszahl durch 100, aber nicht durch 400 teilbar ist.

(Deswegen war 2000 ein Schaltjahr, nicht aber etwa 1900.)