und daher

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} = 1 + \sum_{k=2}^{n} \frac{1}{\sqrt{k}} \leq 1 + \sum_{k=2}^{n} \int_{k-1}^{k} \frac{1}{\sqrt{x}}\, dx =$$
$$= 1 + \int_{1}^{n} \frac{1}{\sqrt{x}}\, dx = 1 + 2(\sqrt{n} - 1) < 2\sqrt{n}.$$

(14.8) Bemerkung: Wird der Algorithmus von Lehman auf eine natürliche Zahl $m > 100$ angewandt, so benötigt er im Schritt (Lehman 1) höchstens $\lfloor m^{1/3} \rfloor$ Test-Divisionen, und für die Anzahl N der in (Lehman 3) getesteten Paare $(k,d) \in \mathbb{N} \times \mathbb{N}$ gilt

$$N \leq \sum_{k=1}^{\lfloor m^{1/3} \rfloor} \left(\left\lfloor \frac{m^{1/6}}{4\sqrt{k}} \right\rfloor + 1 \right) \leq \sum_{k=1}^{\lfloor m^{1/3} \rfloor} \frac{m^{1/6}}{4\sqrt{k}} + \lfloor m^{1/3} \rfloor =$$
$$= \frac{1}{4} m^{1/6} \sum_{k=1}^{\lfloor m^{1/3} \rfloor} \frac{1}{\sqrt{k}} + \lfloor m^{1/3} \rfloor \leq \frac{1}{4} m^{1/6} \cdot 2\sqrt{\lfloor m^{1/3} \rfloor} + \lfloor m^{1/3} \rfloor \leq$$
$$\leq \frac{1}{2} m^{1/6} \sqrt{m^{1/3}} + m^{1/3} = \frac{3}{2} m^{1/3}.$$

Also erfordert der Algorithmus von Lehman im ungünstigsten Fall einen Aufwand, der zu $m^{1/3}$ proportional ist. Er ist somit für größere m dem Algorithmus PZ aus (2.20) deutlich überlegen.

(14.9) Aufgabe: Man schreibe eine MuPAD-Funktion, die nach dem Algorithmus aus (14.6) zu einer natürlichen Zahl $m > 100$ einen nichttrivialen Teiler von m findet oder feststellt, daß m eine Primzahl ist.

15 Unendliche Kettenbrüche

(15.1) In Paragraph 13 wurde gezeigt, daß man jede rationale Zahl durch einen endlichen regelmäßigen Kettenbruch darstellen kann und daß sich dieser mit Hilfe des Euklidischen Algorithmus berechnen läßt. In diesem Paragraphen werden unendliche regelmäßige Kettenbrüche erklärt, und es wird bewiesen, daß man jede irrationale reelle Zahl durch einen solchen unendlichen Kettenbruch darstellen kann. Bereits Euklid kommt diesem Ergebnis recht nahe: Er wußte, daß sein Algorithmus der "Wechselwegnahme", der bei Anwendung auf zwei ganze Zahlen deren größten gemeinsamen Teiler liefert, nicht zu terminieren braucht und daß dann die reellen Zahlen, auf die er angewandt wird,

F. Schwarz, *Einführung in die Elementare Zahlentheorie*

in seiner Sprechweise inkommensurabel sind, d.h. daß ihr Quotient irrational ist (vgl. [32], Buch X, 2; hier spricht Euklid selbstverständlich nicht von reellen Zahlen, sondern von Größen, d.h. von Längen von Strecken). Das im Beweis von (15.5) beschriebene Verfahren zur Berechnung der Kettenbruchentwicklung einer irrationalen reellen Zahl α ist letztlich Euklids Algorithmus, angewandt auf die beiden Zahlen α und 1, und so liegt es nahe, daß manche Mathematikhistoriker zu der Meinung kamen, die griechischen Mathematiker hätten unendliche Kettenbrüche gekannt und mit ihrer Hilfe rationale Approximationen von Quadratwurzeln aus natürlichen Zahlen berechnet (vgl. (15.8)). Die eigentliche Geschichte der unendlichen Kettenbrüche beginnt allerdings – jedenfalls in Europa – wesentlich später, nämlich mit R. Bombelli (1526 – 1572) und P. A. Cataldi. Eine ausführliche Geschichte der Kettenbrüche und ihrer Anwendungen, zusammen mit einem überaus umfangreichen Literaturverzeichnis, findet man in dem Buch [15] von C. Brezinski.

(15.2) Satz: *Es sei a_0 eine ganze Zahl, und es sei $(a_n)_{n\geq 1}$ eine Folge in $\mathbb{N}$. Die Folge*

$$\left([a_0, a_1, \ldots, a_n]\right)_{n\geq 0}$$

konvergiert, und ihr Grenzwert ist eine irrationale reelle Zahl.

Beweis: Es seien $(r_n)_{n\geq -2}$ und $(s_n)_{n\geq -2}$ die Folgen in $\mathbb{Z}$ mit

$$\begin{aligned} r_{-2} &:= 0,\ r_{-1} := 1 \text{ und } r_n := a_n r_{n-1} + r_{n-2} \quad \text{für jedes } n \in \mathbb{N}_0,\\ s_{-2} &:= 1,\ s_{-1} := 0 \text{ und } s_n := a_n s_{n-1} + s_{n-2} \quad \text{für jedes } n \in \mathbb{N}_0. \end{aligned}$$

Aus (13.2) und (13.3) ergibt sich: Für jedes $n \in \mathbb{N}$ gilt

$$s_0 = 1 \leq s_1 = a_1 \leq s_n < s_{n+1}$$

und daher $s_n \geq n$, und für jedes $n \in \mathbb{N}_0$ gilt

$$[a_0, a_1, \ldots, a_n] = \frac{r_n}{s_n} \quad \text{und} \quad r_n s_{n-1} - r_{n-1} s_n = (-1)^{n+1}.$$

Für jedes $n \in \mathbb{N}_0$ gilt daher

$$\frac{r_{n+1}}{s_{n+1}} - \frac{r_n}{s_n} = \frac{r_{n+1}s_n - r_n s_{n+1}}{s_n s_{n+1}} = \frac{(-1)^n}{s_n s_{n+1}}$$

und

$$\begin{aligned} \frac{r_{n+2}}{s_{n+2}} - \frac{r_n}{s_n} &= \left(\frac{r_{n+1}}{s_{n+1}} - \frac{r_n}{s_n}\right) + \left(\frac{r_{n+2}}{s_{n+2}} - \frac{r_{n+1}}{s_{n+1}}\right) = \\ &= (-1)^n \left(\frac{1}{s_n s_{n+1}} - \frac{1}{s_{n+1} s_{n+2}}\right) = (-1)^n \frac{s_{n+2} - s_n}{s_n s_{n+1} s_{n+2}} = \\ &= (-1)^n \frac{a_{n+2} s_{n+1}}{s_n s_{n+1} s_{n+2}} = (-1)^n \frac{a_{n+2}}{s_n s_{n+2}}. \end{aligned}$$

Also gilt für jedes $k \in \mathbb{N}_0$

$$(*) \qquad \frac{r_{2k}}{s_{2k}} < \frac{r_{2k+2}}{s_{2k+2}} < \frac{r_{2k+3}}{s_{2k+3}} < \frac{r_{2k+1}}{s_{2k+1}}$$

und

$$(**) \qquad 0 < \frac{r_{2k+1}}{s_{2k+1}} - \frac{r_{2k}}{s_{2k}} = \frac{1}{s_{2k}s_{2k+1}} \le \frac{1}{2k\,(2k+1)}.$$

Aus $(*)$ folgt, daß die Folgen $(r_{2k}/s_{2k})_{k\ge 0}$ und $(r_{2k+1}/s_{2k+1})_{k\ge 0}$ konvergieren, und aus $(**)$ folgt, daß beide denselben Grenzwert besitzen. Damit ist gezeigt, daß die Folge

$$\left(\frac{r_n}{s_n}\right)_{n\ge 0} = \big([\,a_0, a_1, \ldots, a_n\,]\big)_{n\ge 0}$$

konvergiert. Für ihren Grenzwert α gilt wegen $(*)$: Für jedes $k \in \mathbb{N}_0$ ist

$$[\,a_0, a_1, \ldots, a_{2k}\,] = \frac{r_{2k}}{s_{2k}} < \alpha < \frac{r_{2k+1}}{s_{2k+1}} = [\,a_0, a_1, \ldots, a_{2k+1}\,].$$

Angenommen, α ist eine rationale Zahl. Dann gibt es ein $a \in \mathbb{Z}$ und ein $b \in \mathbb{N}$ mit $\alpha = a/b$, und weil die Folge $(s_n)_{n\ge 1}$ streng monoton wächst, gibt es ein $k \in \mathbb{N}$ mit $s_{2k+1} > b$. Es gilt

$$0 < \frac{a}{b} - \frac{r_{2k}}{s_{2k}} < \frac{r_{2k+1}}{s_{2k+1}} - \frac{r_{2k}}{s_{2k}} = \frac{1}{s_{2k}s_{2k+1}},$$

also

$$0 < as_{2k} - br_{2k} < \frac{b}{s_{2k+1}} < 1,$$

im Widerspruch dazu, daß $as_{2k} - br_{2k}$ eine ganze Zahl ist.

(15.3) Bemerkung: Es sei a_0 eine ganze Zahl, es sei $(a_n)_{n\ge 1}$ eine Folge in $\mathbb{N}$, und es sei $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ der Grenzwert der Folge $([\,a_0, a_1, \ldots, a_n\,])_{n\ge 0}$. Man schreibt

$$\alpha = [\,a_0, a_1, \ldots, a_n, a_{n+1}, \ldots\,].$$

(1) Es seien $(r_n)_{n\ge -2}$ und $(s_n)_{n\ge -2}$ wie im Beweis des Satzes in (15.2) die Folgen in $\mathbb{Z}$ mit

$$\begin{aligned} r_{-2} &:= 0,\ r_{-1} := 1 \text{ und } r_n := a_n r_{n-1} + r_{n-2} \quad \text{für jedes } n \in \mathbb{N}_0,\\ s_{-2} &:= 1,\ s_{-1} := 0 \text{ und } s_n := a_n s_{n-1} + s_{n-2} \quad \text{für jedes } n \in \mathbb{N}_0. \end{aligned}$$

Für jedes $n \in \mathbb{N}_0$ gilt $r_n \in \mathbb{Z}$ und $s_n \in \mathbb{N}$, sowie $r_n s_{n-1} - r_{n-1}s_n = (-1)^{n+1}$, und daher sind r_n und s_n teilerfremd. Für jedes $n \in \mathbb{N}$ ist $s_n < s_{n+1}$.

(2) Wie im Beweis von (15.2) gezeigt wurde, gilt für jedes $n \in \mathbb{N}_0$

$$\frac{r_{n+1}}{s_{n+1}} - \frac{r_n}{s_n} = \frac{(-1)^n}{s_n s_{n+1}} \quad \text{und} \quad \frac{r_{n+2}}{s_{n+2}} - \frac{r_n}{s_n} = (-1)^n \frac{a_{n+2}}{s_n s_{n+2}},$$

und für jedes $k \in \mathbb{N}_0$ gilt

$$\frac{r_{2k}}{s_{2k}} < \frac{r_{2k+2}}{s_{2k+2}} < \alpha < \frac{r_{2k+3}}{s_{2k+3}} < \frac{r_{2k+1}}{s_{2k+1}}.$$

Für jedes $k \in \mathbb{N}_0$ gilt daher

$$\frac{a_{2k+2}}{s_{2k}\, s_{2k+2}} = \frac{r_{2k+2}}{s_{2k+2}} - \frac{r_{2k}}{s_{2k}} < \alpha - \frac{r_{2k}}{s_{2k}} < \frac{r_{2k+1}}{s_{2k+1}} - \frac{r_{2k}}{s_{2k}} = \frac{1}{s_{2k} s_{2k+1}}$$

und

$$\frac{a_{2k+3}}{s_{2k+1} s_{2k+3}} = \frac{r_{2k+1}}{s_{2k+1}} - \frac{r_{2k+3}}{s_{2k+3}} < \frac{r_{2k+1}}{s_{2k+1}} - \alpha < \frac{r_{2k+1}}{s_{2k+1}} - \frac{r_{2k+2}}{s_{2k+2}} = \frac{1}{s_{2k+1} s_{2k+2}}.$$

(3) Für jedes $n \in \mathbb{N}_0$ gilt $a_{n+2} s_{n+1} < a_{n+2} s_{n+1} + s_n = s_{n+2}$ und daher wegen (2)

$$\frac{a_{n+2}}{s_n s_{n+2}} < \left| \alpha - \frac{r_n}{s_n} \right| < \frac{1}{s_n s_{n+1}}.$$

(4) Es gilt $r_0 = a_0$, $s_0 = 1$, $r_1 = a_0 a_1 + 1$ und $s_1 = a_1$, und aus (3) folgt

$$a_0 = \frac{r_0}{s_0} < \alpha < \frac{r_1}{s_1} = \frac{a_0 a_1 + 1}{a_1} = a_0 + \frac{1}{a_1} \leq a_0 + 1,$$

also $a_0 = \lfloor \alpha \rfloor$. Für jedes $n \in \mathbb{N}$ gilt

$$[\, a_0, a_1, \ldots, a_n \,] = a_0 + \frac{1}{[\, a_1, a_2, \ldots, a_n \,]},$$

und daher gilt für

$$\alpha_1 := [\, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots \,] = \lim_{n\to\infty} \big([\, a_1, a_2, \ldots, a_n \,] \big) \in \mathbb{R} \setminus \mathbb{Q} :$$

Es ist

$$\alpha = \lim_{n\to\infty} \big([\, a_0, a_1, \ldots, a_n \,] \big) = a_0 + \frac{1}{\lim_{n\to\infty} \big([\, a_1, a_2, \ldots, a_n \,] \big)} = a_0 + \frac{1}{\alpha_1}.$$

(15.4) Hilfssatz: *Es seien a_0 und b_0 ganze Zahlen, es seien $(a_n)_{n\geq 1}$ und $(b_n)_{n\geq 1}$ Folgen in $\mathbb{N}$, und es gelte*

$$[\,a_0, a_1, \ldots, a_n, a_{n+1}, \ldots\,] \;=\; [\,b_0, b_1, \ldots, b_n, b_{n+1}, \ldots\,].$$

Dann gilt: Für jedes $n \in \mathbb{N}_0$ ist $a_n = b_n$.

Beweis: Für $\alpha := [\,a_0, a_1, \ldots, a_n, \ldots\,]$ und $\alpha_1 := [\,a_1, a_2, \ldots, a_n, \ldots\,]$ und für $\beta := [\,b_0, b_1, \ldots, b_n, \ldots\,]$ und $\beta_1 := [\,b_1, b_2, \ldots, b_n, \ldots\,]$ gilt nach (15.3)(4): Es ist $a_0 = \lfloor\alpha\rfloor$ und $\alpha = a_0 + 1/\alpha_1$, und es ist $b_0 = \lfloor\beta\rfloor$ und $\beta = b_0 + 1/\beta_1$. Wegen $\alpha = \beta$ folgt zunächst $a_0 = b_0$ und dann $\alpha_1 = \beta_1$, und daraus folgt auf dieselbe Weise $a_1 = b_1$ und $[\,a_2, a_3, \ldots, a_n, \ldots\,] = [\,b_2, b_3, \ldots, b_n, \ldots\,]$. Die Fortsetzung des Verfahrens liefert $a_n = b_n$ für jedes $n \in \mathbb{N}_0$.

(15.5) Satz: *Es sei α eine irrationale reelle Zahl. Es gibt eine eindeutig bestimmte ganze Zahl a_0 und eine eindeutig bestimmte Folge $(a_n)_{n\geq 1}$ in $\mathbb{N}$ mit*

$$\alpha \;=\; \lim_{n\to\infty}\big([\,a_0, a_1, \ldots, a_n\,]\big) \;=\; [\,a_0, a_1, \ldots, a_n, a_{n+1}, \ldots\,].$$

Beweis: (1) Man setzt $\alpha_0 := \alpha$ und $a_0 := \lfloor\alpha_0\rfloor$. Wegen $\alpha_0 \in \mathbb{R}\setminus\mathbb{Q}$ und $a_0 \in \mathbb{Z}$ gilt $a_0 < \alpha_0 < a_0+1$, also $0 < \alpha_0 - a_0 < 1$, und daher gilt $\alpha_1 := 1/(\alpha_0 - a_0) > 1$ und $a_1 := \lfloor\alpha_1\rfloor \in \mathbb{N}$. Wegen $\alpha_1 \in \mathbb{R}\setminus\mathbb{Q}$ kann man dieses Verfahren fortsetzen: Man erhält so Folgen $(\alpha_n)_{n\geq 0}$ in $\mathbb{R}\setminus\mathbb{Q}$ und $(a_n)_{n\geq 0}$ in $\mathbb{Z}$, für die gilt: Es gilt $\alpha_0 = \alpha$, $a_0 = \lfloor\alpha_0\rfloor = \lfloor\alpha\rfloor \in \mathbb{Z}$, und für jedes $n \in \mathbb{N}$ gilt $\alpha_n > 1$, $a_n = \lfloor\alpha_n\rfloor \in \mathbb{N}$ und

$$\alpha_n \;=\; \frac{1}{\alpha_{n-1} - a_{n-1}} \quad \text{und daher} \quad \alpha_{n-1} \;=\; a_{n-1} + \frac{1}{\alpha_n}.$$

(2) Für jedes $n \in \mathbb{N}_0$ gilt

$$\alpha \;=\; [\,a_0, a_1, \ldots, a_{n-1}, \alpha_n\,],$$

denn es ist $\alpha = \alpha_0 = [\,\alpha_0\,]$, und ist n eine natürliche Zahl, für die bereits bewiesen ist, daß $\alpha = [\,a_0, a_1, \ldots, a_{n-2}, \alpha_{n-1}\,]$ gilt, so folgt

$$\begin{aligned}\alpha \;&=\; [\,a_0, a_1, \ldots, a_{n-2}, \alpha_{n-1}\,] \;=\\ &=\; \left[\,a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{\alpha_n}\,\right] \;=\; [\,a_0, a_2, \ldots, a_{n-1}, \alpha_n\,].\end{aligned}$$

(3) Es seien $(r_n)_{n\geq -2}$ und $(s_n)_{n\geq -2}$ die zur Folge $(a_n)_{n\geq 0}$ wie in (15.3)(1) definierten Folgen in $\mathbb{Z}$. Dann gilt für jedes $n \in \mathbb{N}$: Es ist wegen (13.2)(4)

$$\alpha \;=\; [\,a_0, a_2, \ldots, a_{n-1}, a_n, \alpha_{n+1}\,] \;=\; \frac{\alpha_{n+1}r_n + r_{n-1}}{\alpha_{n+1}s_n + s_{n-1}}$$

und daher

$$\begin{aligned}\alpha - \frac{r_n}{s_n} &= \frac{\alpha_{n+1} r_n + r_{n-1}}{\alpha_{n+1} s_n + s_{n-1}} - \frac{r_n}{s_n} = \\ &= \frac{r_{n-1} s_n - r_n\, s_{n-1}}{s_n(\alpha_{n+1} s_n + s_{n-1})} = \frac{(-1)^n}{s_n(\alpha_{n+1} s_n + s_{n-1})},\end{aligned}$$

also

$$\left| \alpha - \frac{r_n}{s_n} \right| = \frac{1}{s_n(\alpha_{n+1} s_n + s_{n-1})} < \frac{1}{s_n^2} \leq \frac{1}{n^2},$$

denn es ist $\alpha_{n+1} > 1$, und $(s_n)_{n \geq 1}$ ist eine streng monoton wachsende Folge natürlicher Zahlen. Also konvergiert die Folge $(r_n/s_n)_{n \geq 0}$ gegen α, und es ist

$$\alpha = \lim_{n \to \infty} \left(\frac{r_n}{s_n} \right) = \lim_{n \to \infty} ([\, a_0, a_1, \ldots, a_n\,]) = [\, a_0, a_1, \ldots, a_n, a_{n+1}, \ldots\,].$$

Daß dadurch die Folge $(a_n)_{n \geq 0}$ eindeutig bestimmt ist, folgt unmittelbar aus dem Hilfssatz in (15.4).

(15.6) Definition: Es sei α eine irrationale reelle Zahl, und es seien a_0 die eindeutig bestimmte ganze Zahl und $(a_n)_{n \geq 1}$ die eindeutig bestimmte Folge aus natürlichen Zahlen mit

$$(*) \qquad \alpha = [\, a_0, a_1, \ldots, a_n, a_{n+1}, \ldots\,].$$

Dann heißt $(*)$ die Kettenbruchentwicklung von α oder der Kettenbruch für α, genauer der unendliche regelmäßige Kettenbruch für α. Für jedes $n \in \mathbb{N}_0$ heißt a_n der n-te Teilnenner dieses Kettenbruchs. Sind $(r_n)_{n \geq -2}$ und $(s_n)_{n \geq -2}$ wie in (15.3)(1) die Folgen in $\mathbb{Z}$ mit

$$\begin{aligned} r_{-2} &:= 0, \; r_{-1} := 1 \text{ und } r_n := a_n r_{n-1} + r_{n-2} \quad \text{für jedes } n \in \mathbb{N}_0, \\ s_{-2} &:= 1, \; s_{-1} := 0 \text{ und } s_n := a_n s_{n-1} + s_{n-2} \quad \text{für jedes } n \in \mathbb{N}_0, \end{aligned}$$

so heißen für jedes $n \in \mathbb{N}_0$ die rationale Zahl r_n/s_n der n-te Näherungsbruch, die ganze Zahl r_n der n-te Näherungszähler und die natürliche Zahl s_n der n-te Näherungsnenner des Kettenbruchs für α. Für jedes $n \in \mathbb{N}_0$ heißt die irrationale Zahl

$$\alpha_n := [\, a_n, a_{n+1}, a_{n+2}, \ldots\,]$$

der n-te vollständige Quotient des Kettenbruchs für α.

(15.7) Beispiel: Für $\alpha := \sqrt{3}$ liefert das Verfahren aus dem Beweis des Satzes in (15.5)

$$\begin{aligned}
\alpha_0 &:= \sqrt{3}, & a_0 &:= \lfloor \alpha_0 \rfloor = 1,\\
\alpha_1 &:= \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}, & a_1 &:= \lfloor \alpha_1 \rfloor = 1,\\
\alpha_2 &:= \frac{2}{\sqrt{3}-1} = \sqrt{3}+1, & a_2 &:= \lfloor \alpha_2 \rfloor = 2,\\
\alpha_3 &:= \frac{1}{\sqrt{3}-1} = \alpha_1, & a_3 &:= \lfloor \alpha_3 \rfloor = \lfloor \alpha_1 \rfloor = a_1 = 1,
\end{aligned}$$

und daher gilt $\alpha_4 = \alpha_2$, $a_4 = a_2 = 2$, $\alpha_5 = \alpha_3 = \alpha_1$, $a_5 = a_1 = 1$ und so fort. Also gilt

$$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, 1, 2, 1, 2, \dots].$$

Der Kettenbruch für $\sqrt{3}$ ist also – nach der Vorperiode 1 – periodisch mit der Periode $(1, 2)$. Dahinter steht ein allgemeiner Satz, der im nächsten Paragraphen behandelt wird.

Die Folge $(r_n/s_n)_{n>0}$ der Näherungsbrüche dieses Kettenbruchs konvergiert gegen $\sqrt{3}$; man kann also Näherungsbrüche als rationale Approximationen für $\sqrt{3}$ verwenden. Nach (15.3)(2) gilt zum Beispiel

$$1.73205\,08075\,65499\ldots = \frac{716035}{413403} = \frac{r_{20}}{s_{20}} < \sqrt{3} <$$
$$< \frac{r_{21}}{s_{21}} = \frac{978122}{564719} = 1.73205\,08075\,69782\ldots\,.$$

Die Näherungsbrüche sind in einem noch zu präzisierenden Sinn besonders gute rationale Näherungen für $\sqrt{3}$. Davon wird am Anfang des übernächsten Paragraphen die Rede sein.

Rechnet man gemäß (15.5) mit gerundeten Dezimalbrüchen, so führen Rundungsfehler zu falschen Ergebnissen; so liefert ein Taschenrechner, der zehn Dezimalstellen ausgibt, zu $\alpha := \sqrt{3}$ der Reihe nach die Teilnenner

$$1,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 3,\ 2,\ 1,\ 2,\ 1,\ 4,\ 3,\ 4,\ \dots$$

und ein anderer die Teilnenner

$$1,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 1,\ 2,\ 1,\ 4,\ \dots\,.$$

Der Satz in (15.9) gibt Auskunft darüber, wie man zu einer reellen Zahl α aus den Kettenbrüchen für reelle Zahlen α' und α'' mit $\alpha' \le \alpha \le \alpha''$ den Anfang der Kettenbruchentwicklung von α gewinnen kann.

(15.8) Bemerkung: Archimedes (um 280 – 212) beweist in seiner Schrift über die Kreismessung (*Κύκλου μέτρησις*, vgl. [3], Band I; ins Deutsche übersetzt [4], S. 367–377), daß

$$\frac{223}{71} < \pi < \frac{22}{7}$$

gilt. Dazu zeigt er: Für den Umfang u_{96} eines einem Kreis vom Radius 1 einbeschriebenen und den Umfang U_{96} eines diesem Kreis umbeschriebenen regelmäßigen 96-Ecks gilt $u_{96} > 2 \cdot 223/71$ und $U_{96} < 2 \cdot 22/7$. Zum Beweis dieser Abschätzungen benötigt er rationale Näherungen für $\sqrt{3}$, und zwar gibt er an, daß

$$(*) \qquad \frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

gilt, ohne einen Hinweis darauf, wie er diese Abschätzungen gewonnen hat. Weil 265/153 der achte und 1351/780 der elfte Näherungsbruch des Kettenbruchs für $\sqrt{3}$ sind, schlossen manche Mathematikhistoriker darauf, daß Archimedes über unendliche Kettenbrüche verfügte oder wenigstens den Anfang des Kettenbruchs für $\sqrt{3}$ und die ersten zugehörigen Näherungsbrüche berechnen konnte. Dieser Schluß scheint aber nicht zwingend, schon weil 265/153 und 1351/780 nicht aufeinanderfolgende Näherungsbrüche des Kettenbruchs für $\sqrt{3}$ sind. Es gibt manche andere Versuche, die Überlegungen, die Archimedes zu (*) führten, zu rekonstruieren (vgl. (15.12), Aufgabe 2). K. Vogel beschreibt in [109] die folgende Methode als eine, die Archimedes zu Verfügung gehabt haben könnte: Daß 5/3 eine erste brauchbare Näherung für $\sqrt{3}$ ist, ist wegen

$$3 - \left(\frac{5}{3}\right)^2 = \frac{2}{9}$$

leicht zu sehen. Das nach dem griechischen Mathematiker Heron (um 100 n. Chr. Geb.) benannte Verfahren, näherungsweise Quadratwurzeln zu berechnen, das schon vor ihm im vorderen Orient und sicher auch in der griechischen Welt bekannt war, liefert zum Startwert $c_1 := 5/3$ die gegen $\sqrt{3}$ konvergente Folge $(c_n)_{n\geq 1}$ mit

$$c_{n+1} := c_n - \frac{c_n^2 - 3}{2c_n} = \frac{1}{2}\left(c_n + \frac{3}{c_n}\right) \quad \text{für jedes } n \in \mathbb{N},$$

und es gilt $c_3 = 1351/780$ und $1351^2 > 3 \cdot 780^2$. (Wie man sieht, ist $(c_n)_{n\geq 1}$ auch die Folge, die das Newton-Verfahren der Numerik bei Anwendung auf die Funktion $x \mapsto x^2 - 3 :]0, \infty[\to \mathbb{R}$ und auf den Startwert 5/3 liefert). Die Abschätzung $\sqrt{3} > 265/153$ könnte Archimedes mit Hilfe einer vielleicht naheliegenden Variante des Heronschen Verfahrens aus den ersten Termen der Folge $(c_n)_{n\geq 1}$ gewonnen haben: Die Folge $(d_n)_{n\geq 1}$ mit

$$d_1 := c_1 = \frac{5}{3} \quad \text{und} \quad d_{n+1} := c_n - \frac{c_n^2 - 3}{c_n + c_{n+1}} \quad \text{für jedes } n \in \mathbb{N}$$

konvergiert ebenfalls gegen $\sqrt{3}$, und es gilt $d_2 = 265/153$ und $265^2 < 3 \cdot 153^2$. Die "Kreismessung" liefert somit wohl keinen zwingenden Beweis dafür, daß Archimedes über Kettenbrüche für Quadratwurzeln aus natürlichen Zahlen verfügte. Eine mit einiger Sicherheit von ihm stammende Aufgabe, das sog. Rinderproblem, erlaubt aber vielleicht doch, sich vorzustellen, daß Archimedes mit solchen Kettenbrüchen und ihren Näherungsbrüchen umgehen konnte (vgl. dazu (17.15) und [100]).

(15.9) Satz: *Es seien α, α' und α'' reelle Zahlen, für die $\alpha' \leq \alpha \leq \alpha''$ gilt, und es seien*

$$\begin{aligned} \alpha &= [a_0, a_1, \dots, a_n, \dots], \\ \alpha' &= [a'_0, a'_1, \dots, a'_n, \dots] \quad \text{und} \\ \alpha'' &= [a''_0, a''_1, \dots, a''_n, \dots] \end{aligned}$$

die (endlichen oder unendlichen) Kettenbrüche für α, α' und α''. Wenn es ein $k \in \mathbb{N}_0$ mit $a'_i = a''_i$ für jedes $i \in \{0, 1, \dots, k\}$ gibt, so gilt: Für jedes $i \in \{0, 1, \dots, k\}$ ist $a_i = a'_i = a''_i$.

Beweis: Wegen $\alpha' \leq \alpha \leq \alpha''$ gilt $a'_0 = \lfloor \alpha' \rfloor \leq \lfloor \alpha \rfloor \leq \lfloor \alpha'' \rfloor = a''_0$, und daher gilt: Ist $a'_0 = a''_0$, so ist $a_0 = \lfloor \alpha \rfloor = a'_0 = a''_0$. – Es sei $k \in \mathbb{N}$, es gelte $a'_i = a''_i$ für jedes $i \in \{0, 1, \dots, k\}$, und es sei bereits bewiesen, daß $a_i = a'_i = a''_i$ für jedes $i \in \{0, 1, \dots, k-1\}$ gilt. Die reellen Zahlen $\alpha_k := [a_k, a_{k+1}, \dots, a_n, \dots]$, $\alpha'_k := [a'_k, a'_{k+1}, \dots, a'_n, \dots]$ und $\alpha''_k := [a''_k, a''_{k+1}, \dots, a''_n, \dots]$ sind positiv, und es gilt $\alpha = [a_0, a_1, \dots, a_{k-1}, \alpha_k]$,

$$\begin{aligned} \alpha' &= [a'_0, a'_1, \dots, a'_{k-1}, \alpha'_k] = [a_0, a_1, \dots, a_{k-1}, \alpha'_k] \quad \text{und} \\ \alpha'' &= [a''_0, a''_1, \dots, a''_{k-1}, \alpha''_k] = [a_0, a_1, \dots, a_{k-1}, \alpha''_k]. \end{aligned}$$

Es seien $r_{-2} := 0$, $r_{-1} := 1$ und $s_{-2} := 1$, $s_{-1} := 0$, und für jedes $i \in \{0, 1, \dots, k-1\}$ seien $r_i := a_i r_{i-1} + r_{i-2}$ und $s_i := a_i s_{i-1} + s_{i-2}$. Damit gilt nach (13.2)(4)

$$\alpha = \frac{\alpha_k r_{k-1} + r_{k-2}}{\alpha_k s_{k-1} + s_{k-2}}, \quad \alpha' = \frac{\alpha'_k r_{k-1} + r_{k-2}}{\alpha'_k s_{k-1} + s_{k-2}} \quad \text{und} \quad \alpha'' = \frac{\alpha''_k r_{k-1} + r_{k-2}}{\alpha''_k s_{k-1} + s_{k-2}}.$$

Die Funktion

$$f : [0, \infty[\; \to \mathbb{R} \quad \text{mit} \quad f(t) := \frac{t r_{k-1} + r_{k-2}}{t s_{k-1} + s_{k-2}} \quad \text{für jedes } t \in [0, \infty[$$

ist streng monoton, denn für jedes $t \in [0, \infty[$ ist nach (13.2)(5)

$$f'(t) = \frac{r_{k-1}s_{k-2} - r_{k-2}s_{k-1}}{(ts_{k-1} + s_{k-2})^2} = \frac{(-1)^k}{(ts_{k-1} + s_{k-2})^2};$$

sie besitzt somit eine streng monotone Umkehrfunktion. Wegen $\alpha' \leq \alpha \leq \alpha''$ gilt daher $\alpha'_k \leq \alpha_k \leq \alpha''_k$ oder $\alpha''_k \leq \alpha_k \leq \alpha'_k$, und daraus folgt $a'_k = \lfloor \alpha'_k \rfloor \leq a_k = \lfloor \alpha_k \rfloor \leq \lfloor \alpha''_k \rfloor = a''_k$ oder $a''_k = \lfloor \alpha''_k \rfloor \leq a_k = \lfloor \alpha_k \rfloor \leq \lfloor \alpha'_k \rfloor = a'_k$. In jedem Fall gilt also $a_k = a'_k = a''_k$.

(15.10) Beispiel: Es gilt

$$\alpha' := 3.14159\,26535\,89793\,23846 < \pi < 3.14159\,26535\,89794\,23847 =: \alpha'',$$

und das Verfahren aus dem Beweis in (13.5) liefert

$$\begin{aligned} \alpha' &= [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, \\ &\qquad 3, 9, 17, 1, 6, 3, 8, 5, 29, 4, 1, 1, 2, 1, 1, 1, 18] \qquad \text{und} \\ \alpha'' &= [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, \\ &\qquad 2, 1, 2, 4, 1, 1, 1, 2, 1, 3, 11, 2, 2, 1, 2, 1, 1, 1, 6, 13, 1, 1, 13, 4, 3]. \end{aligned}$$

Aus (15.9) folgt: Es ist

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, \ldots].$$

Die Näherungsbrüche

$$3, \quad \frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}, \quad \frac{103993}{33102}, \quad \frac{104348}{33215}, \quad \ldots$$

dieses Kettenbruchs sind rationale Näherungen für π. Daß 3 als Näherung für π betrachtet wurde, ist im Alten Testament erwähnt (1. Könige 7, 23; um 550 v. Chr. Geb.), die Näherung 22/7 fand Archimedes (vgl. (15.8)), und die Näherungen 333/106 und 355/113 wurden von A. Metius (1571 bis 1635) angegeben. Nach (15.3)(2), angewandt mit $k = 1$, ergibt sich die Fehlerabschätzung

$$0.266\ldots \cdot 10^{-6} = \frac{1}{113 \cdot 33215} < \frac{355}{113} - \pi < \frac{1}{113 \cdot 33102} = 0.267\ldots \cdot 10^{-6},$$

und es gilt

$$3.14159\,26530\ldots = \frac{103993}{33102} < \pi < \frac{104348}{33215} = 3.14159\,26539\ldots .$$

(15.11) Es seien a', $a'' \in \mathbb{Z}$ und b', $b'' \in \mathbb{N}$, es gelte $\mathrm{ggT}(a', b') = 1$ und $\mathrm{ggT}(a'', b'') = 1$, und es sei α eine reelle Zahl mit $a'/b' \leq \alpha \leq a''/b''$. Der folgende Algorithmus berechnet die ersten Teilnenner $a_0, a_1, \ldots, a_n$ des Kettenbruchs für α, soweit sie sich gemäß (15.9) aus den Kettenbrüchen für a'/b' und a''/b'' gewinnen lassen; er liefert außerdem Schranken für den ersten Teilnenner a_{n+1}, der sich nicht mehr exakt mit Hilfe von a'/b' und a''/b'' bestimmen läßt.

(cFrac1) Ist $a'/b' = a''/b''$, so berechnet man den Kettenbruch für a'/b', gibt ihn aus und bricht ab.
(cFrac2) Man setzt $cF := [\ ]$.
(cFrac3) Man berechnet $q' := a' \operatorname{div} b'$, $r' := a' \bmod b'$ und $r'' := a'' - b''q'$. Gilt $r'' < 0$ oder $r'' \geq b''$, so setzt man $q'' := a'' \operatorname{div} b''$ und geht zu (cFrac5).
(cFrac4) Man fügt in die Liste cF als neuen letzten Eintrag q' ein und setzt $a' := b'$, $b' := r'$ und $a'' := b''$, $b'' := r''$. Ist $b' = 0$, so setzt man $q' := \infty$ und $q'' := a'' \operatorname{div} b''$ und geht zu (cFrac5); ist $b'' = 0$, so setzt man $q'' := \infty$ und $q' := a' \operatorname{div} b'$ und geht zu (cFrac5). Gilt $b' \neq 0$ und $b'' \neq 0$, so geht man zurück zu (cFrac3).
(cFrac5) Ist $q' < q''$, so fügt man in die Liste cF als neuen letzten Eintrag $q' \ldots q''$ ein, gibt cF aus und bricht ab; ist $q'' < q'$, so fügt man in die Liste cF als neuen letzten Eintrag $q'' \ldots q'$ ein, gibt cF aus und bricht ab.

(15.12) Aufgaben:

Aufgabe 1: Man überlege sich, daß der Algorithmus cFrac in (15.11) das Verlangte leistet, und schreibe dazu eine MuPAD-Funktion. Hier ist die Funktion `sharelib::rational` nützlich; sie verwandelt einen endlichen Dezimalbruch in einen Bruch mit demselben Wert; z.B. liefert `sharelib::rational(3.1415)` die Ausgabe `6283/2000`.

Aufgabe 2: Wie in (15.8) berichtet ist, hat Archimedes die Abschätzungen

$$(*) \qquad \frac{265}{153} < \pi < \frac{1351}{780}$$

angegeben.

(a) Wie kann man die beiden rationalen Zahlen in $(*)$ aus dem Kettenbruch für $\sqrt{27}$ gewinnen?

(b) Man beweise: Sind q und x_1 positive reelle Zahlen, so konvergiert die Folge $(x_n)_{n \geq 1}$ mit

$$x_{n+1} := x_n \cdot \frac{x_n^2 + 3q}{3x_n^2 + q} \quad \text{für jedes } n \in \mathbb{N}$$

gegen $\sqrt{q}$. Man stelle die Konvergenzordnung fest.

(c) Nach (b) konvergiert für jedes positive $x_1 \in \mathbb{R}$ die Folge $(x_n)_{n\geq 1}$ mit

$$x_{n+1} := x_n \cdot \frac{x_n^2+9}{3x_n^2+3} \quad \text{für jedes } n \in \mathbb{N}$$

gegen $\sqrt{3}$. Wie kann man jede der beiden von Archimedes angegebenen rationalen Näherungen an $\sqrt{3}$ mit Hilfe einer solchen Folge finden?

16 Periodische Kettenbrüche

(16.1) In diesem Paragraphen werden die Kettenbruchentwicklungen von irrationalen reellen Zahlen, die Nullstellen von quadratischen Polynomen mit rationalen Koeffizienten sind, behandelt. Zuerst wird gezeigt, daß diese Zahlen genau die Zahlen mit periodischer Kettenbruchentwicklung sind. Dann werden die Kettenbruchentwicklungen von Quadratwurzeln aus natürlichen Zahlen genauer untersucht; die dabei erzielten Ergebnisse werden im folgenden Paragraphen benötigt. Zwei der Resultate dieses Paragraphen stammen aus der ersten Publikation von E. Galois (1811 – 1832), die anderen gehen auf P. de Fermat, L. Euler und J. L. Lagrange zurück.

(16.2) Definition: Es sei $a_0 \in \mathbb{Z}$, und es sei $(a_n)_{n\geq 1}$ eine Folge in $\mathbb{N}$. Wenn es ein $k \in \mathbb{N}_0$ und ein $l \in \mathbb{N}$ mit

$$a_{k+l+i} = a_{k+i} \quad \text{für jedes } i \in \mathbb{N}_0$$

gibt, so nennt man den Kettenbruch $[a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$ periodisch und schreibt

$$[a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots] = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+l-1}}];$$

man nennt $(a_0, a_1, \ldots, a_{k-1})$ eine Vorperiode und $(a_k, a_{k+1}, \ldots, a_{k+l-1})$ eine Periode dieses Kettenbruchs. Der Kettenbruch $[a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$ heißt rein-periodisch, wenn es ein $l \in \mathbb{N}$ mit $a_{l+i} = a_i$ für jedes $i \in \mathbb{N}_0$ gibt, also wenn gilt: Es ist

$$[a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots] = [\overline{a_0, a_1, \ldots, a_{l-1}}].$$

(16.3) Bemerkung: Es sei $a_0 \in \mathbb{Z}$, es sei $(a_n)_{n\geq 1}$ eine Folge in $\mathbb{N}$, und es gelte: Der Kettenbruch $[a_0, a_1, a_2, \ldots, a_n, a_{n+1}, \ldots]$ ist periodisch. Eine Periode $(a_k, a_{k+1}, \ldots, a_{k+l-1})$ dieses Kettenbruchs heißt primitiv, wenn es nicht Zahlen $i, j \in \{k, k+1, \ldots, k+l-1\}$ mit $0 < j-i < l-1$ gibt, für die $(a_i, a_{i+1}, \ldots, a_j)$