(13.8) Bemerkung: Das klassische Werk über Kettenbrüche ist das Buch [77] von O. Perron (1880 – 1975). Eine neuere Darstellung der Zahlentheorie der Kettenbrüche ist das Buch [92] von A. M. Rockett und P. Szüsz.

(13.9) Aufgaben:

Aufgabe 1: Man schreibe eine MuPAD-Funktion, die zu einer rationalen Zahl q mit Hilfe der im Beweis von (13.5) verwendeten Methode den Kettenbruch für die Zahl q berechnet.

Aufgabe 2: (a) Man schreibe eine MuPAD-Funktion, die zu einer Liste aus einer ganzen Zahl a_0, aus natürlichen Zahlen $a_1, \ldots, a_{n-1}$ und aus einer natürlichen Zahl $a_n \geq 2$ die Liste der Näherungsbrüche des Kettenbruchs $[a_0, a_1, \ldots, a_n]$ berechnet. Man richte diese Funktion so ein, daß sie bei Aufruf mit einem zweiten Argument $k \in \{0, 1, \ldots, n\}$ nur den k-ten Näherungsbruch dieses Kettenbruchs ausgibt.

(b) Man schreibe eine MuPAD-Funktion, die zu einer Liste aus einer ganzen Zahl a_0, aus natürlichen Zahlen $a_1, \ldots, a_{n-1}$ und aus einer natürlichen Zahl $a_n \geq 2$ nur den Wert des Kettenbruchs $[a_0, a_1, \ldots, a_n]$ berechnet.

14 Der Algorithmus von R. S. Lehman

(14.1) In diesem Paragraphen wird ein Faktorisierungsalgorithmus für natürliche Zahlen vorgestellt, der mehr leistet als das in (2.20) beschriebene naive Verfahren; zu seiner Begründung werden die im letzten Paragraphen behandelten Kettenbruchentwicklungen von rationalen Zahlen verwendet.

(14.2) Es seien a, $b \in \mathbb{N}$, und es gelte $b < a$ und $b \nmid a$.
(1) Es sei $a/b = [a_0, a_1, \ldots, a_n]$ die Kettenbruchentwicklung von a/b. Wegen $b < a$ ist $a_0 = \lfloor a/b \rfloor \in \mathbb{N}$, und wegen $b \nmid a$ gilt $n \geq 1$ und daher $a_n \geq 2$. Es gilt

$$\frac{b}{a} = 0 + \frac{1}{a/b} = \left\lfloor \frac{b}{a} \right\rfloor + \frac{1}{[a_0, a_1, \ldots, a_n]} = [0, a_0, a_1, \ldots, a_n].$$

Wegen $a_0, a_1, \ldots, a_n \in \mathbb{N}$ und wegen $a_n \geq 2$ ist dies der Kettenbruch für b/a.
(2) Es seien $r_0/s_0, r_1/s_1, \ldots, r_n/s_n$ die $n+1$ Näherungsbrüche des Kettenbruchs $a/b = [a_0, a_1, \ldots, a_n]$. Für jedes $j \in \{0, 1, \ldots, n\}$ gilt

$$\frac{r_j}{s_j} = [a_0, a_1, \ldots, a_j]$$

und

$$[0, a_0, a_1, \ldots, a_j] = 0 + \frac{1}{[a_0, a_1, \ldots, a_j]} = \frac{1}{r_j/s_j} = \frac{s_j}{r_j},$$

und somit sind $0/1$, s_0/r_0, $s_1/r_1, \ldots$, s_n/r_n die $n+2$ Näherungsbrüche für den Kettenbruch $b/a = [0, a_0, a_1, \ldots, a_n]$. Aus (13.6)(2) folgt daher: Für jedes $j \in \{0, 1, \ldots, n-1\}$ gilt

$$\left| \frac{a}{b} - \frac{r_j}{s_j} \right| \leq \frac{1}{s_j s_{j+1}} \quad \text{und} \quad \left| \frac{b}{a} - \frac{s_j}{r_j} \right| \leq \frac{1}{r_j r_{j+1}}.$$

(14.3) Hilfssatz: *Es sei $m \in \mathbb{N}$, und es gelte: Es gibt Primzahlen p und q mit $m = pq$ und mit $m^{1/3} < p \leq q < m^{2/3}$. Dann gibt es natürliche Zahlen r und s, für die gilt: Es ist*

$$rs < m^{1/3} \quad \text{und} \quad |pr - qs| \leq m^{1/3}.$$

Beweis: (1) Gilt $p = q$, so kann man $r := 1$ und $s := 1$ setzen.
(2) Es gelte $p < q$. Es gibt ein $n \in \mathbb{N}$ und $a_0, a_1, \ldots, a_n \in \mathbb{N}$ mit $a_n \geq 2$ und mit $q/p = [a_0, a_1, \ldots, a_n]$. Es seien r_0/s_0, $r_1/s_1, \ldots$, r_n/s_n die Näherungsbrüche für diesen Kettenbruch. Es gilt $r_0 = a_0$ und $s_0 = 1$ und daher

$$(*) \qquad r_0 s_0 = a_0 = \left\lfloor \frac{q}{p} \right\rfloor \leq \frac{q}{p} < \frac{m^{2/3}}{m^{1/3}} = m^{1/3}.$$

Es gilt $r_n/s_n = [a_0, a_1, \ldots, a_n] = q/p$ und daher $r_n = q$ und $s_n = p$, denn es gilt $\mathrm{ggT}(r_n, s_n) = 1$ und $\mathrm{ggT}(q, p) = 1$. Also gilt

$$(**) \qquad r_n s_n = pq = m > m^{1/3}.$$

Wegen $(*)$ und $(**)$ folgt: Es gibt ein $j \in \{0, 1, \ldots, n-1\}$ mit $r_j s_j < m^{1/3}$ und mit $r_{j+1} s_{j+1} \geq m^{1/3}$. Ist $q/p \geq r_{j+1}/s_{j+1}$, so gilt $p/s_{j+1} \leq q/r_{j+1}$ und daher

$$|pr_j - qs_j| = ps_j \left| \frac{r_j}{s_j} - \frac{q}{p} \right| \leq \frac{ps_j}{s_j s_{j+1}} = \frac{p}{s_{j+1}} = \sqrt{\frac{p}{s_{j+1}}} \sqrt{\frac{p}{s_{j+1}}} \leq$$

$$\leq \sqrt{\frac{p}{s_{j+1}}} \sqrt{\frac{q}{r_{j+1}}} = \frac{\sqrt{pq}}{\sqrt{r_{j+1} s_{j+1}}} = \frac{\sqrt{m}}{\sqrt{r_{j+1} s_{j+1}}} \leq \frac{m^{1/2}}{m^{1/6}} = m^{1/3}.$$

Ist $q/p < r_{j+1}/s_{j+1}$, so gilt $q/r_{j+1} < p/s_{j+1}$ und daher

$$|pr_j - qs_j| = qr_j \left| \frac{p}{q} - \frac{s_j}{r_j} \right| \leq \frac{qr_j}{r_j r_{j+1}} = \frac{q}{r_{j+1}} = \sqrt{\frac{q}{r_{j+1}}} \sqrt{\frac{q}{r_{j+1}}} \leq$$

$$\leq \sqrt{\frac{p}{s_{j+1}}} \sqrt{\frac{q}{r_{j+1}}} = \frac{\sqrt{pq}}{\sqrt{r_{j+1} s_{j+1}}} = \frac{\sqrt{m}}{\sqrt{r_{j+1} s_{j+1}}} \leq \frac{m^{1/2}}{m^{1/6}} = m^{1/3}.$$

Man kann also in jedem Fall $r := r_j$ und $s := s_j$ setzen.

(14.4) Hilfssatz: *Es sei $m \in \mathbb{N}$, und es gelte: Es gibt Primzahlen p und q mit $m = pq$ und mit $m^{1/3} < p < q < m^{2/3}$. Es gibt natürliche Zahlen k und d mit den folgenden Eigenschaften: Es gilt*

$$k \leq \lfloor m^{1/3} \rfloor \quad \text{und} \quad d \leq \left\lfloor \frac{m^{1/6}}{4\sqrt{k}} \right\rfloor + 1,$$

und die Zahl

$$\left(\lfloor \sqrt{4km} \rfloor + d\right)^2 - 4km$$

ist eine Quadratzahl.

Beweis: Nach (14.3) gibt es $r, s \in \mathbb{N}$ mit $rs < m^{1/3}$ und mit $|\, pr - qs \,| \leq m^{1/3}$. Für $k := rs$ und $d := pr + qs - \lfloor \sqrt{4km} \rfloor$ gilt $1 \leq k = rs \leq \lfloor m^{1/3} \rfloor$ und

$$(pr + qs)^2 \geq (pr + qs)^2 - (pr - qs)^2 = 4pqrs = 4km$$

und daher

$$d = pr + qs - \lfloor \sqrt{4km} \rfloor \geq \sqrt{4km} - \lfloor \sqrt{4km} \rfloor > 0,$$

denn wegen $k < m^{1/3} < m = pq$ ist $4km = 4kpq$ keine Quadratzahl, und daher ist $\lfloor \sqrt{4km} \rfloor < \sqrt{4km}$. Da d eine ganze Zahl ist, folgt $d \in \mathbb{N}$. Wegen

$$\begin{aligned} m^{2/3} &\geq (pr - qs)^2 = (pr + qs)^2 - 4km = \\ &= \left((pr + qs) - \sqrt{4km}\right)\left((pr + qs) + \sqrt{4km}\right) \geq \\ &\geq \left((pr + qs) - \sqrt{4km}\right) \cdot 2\sqrt{4km} > \\ &> 2\left((pr + qs) - (\lfloor \sqrt{4km} \rfloor + 1)\right) \cdot \sqrt{4km} = 2(d-1)\sqrt{4km} \end{aligned}$$

folgt

$$d < \frac{m^{2/3}}{2\sqrt{4km}} + 1 = \frac{m^{1/6}}{4\sqrt{k}} + 1,$$

also

$$d \leq \left\lfloor \frac{m^{1/6}}{4\sqrt{k}} \right\rfloor + 1.$$

Außerdem ist $\left(\lfloor \sqrt{4km} \rfloor + d\right)^2 - 4km = (pr + qs)^2 - 4km = (pr - qs)^2$ eine Quadratzahl.

(14.5) Bemerkung: Für jede natürliche Zahl $m > 100$ gilt

$$2m^{2/3} + \frac{m^{1/6}}{4} + 1 < \frac{m}{2}.$$

Beweis: Es sei $f\colon \mathbb{R} \to \mathbb{R}$ die Funktion mit

$$f(t) := \frac{t^6}{2} - 2t^4 - \frac{t}{4} - 1 \quad \text{für jedes } t \in \mathbb{R}.$$

Für jedes $t \in \mathbb{R}$ gilt

$$f'(t) = 3t^5 - 8t^3 - \frac{1}{4} \quad \text{und} \quad f''(t) = 15t^4 - 24t^2 = 15t^2\left(t^2 - \frac{8}{5}\right).$$

Für jedes $t \in \mathbb{R}$ mit $t \geq 2$ gilt $f''(t) > 0$, und daher ist f' im Intervall $[2, \infty[$ streng monoton wachsend. Also gilt für jede reelle Zahl $t \geq 2$: Es ist $f'(t) \geq f'(2) = 31.75 > 0$, und daher ist f in $[2, \infty[$ streng monoton wachsend. Für jedes $m \in \mathbb{N}$ mit $m > 100$ gilt $m^{1/6} > 100^{1/6} = 2.154\ldots > 2.1$ und daher

$$\frac{m}{2} - 2m^{2/3} - \frac{m^{1/6}}{4} - 1 = f(m^{1/6}) > f(2.1) = 2.461\ldots > 0.$$

(14.6) Der Algorithmus von R. S. Lehman: (1) Es sei m eine natürliche Zahl mit $m > 100$. Der folgende Algorithmus findet entweder einen Primteiler $p < m$ von m oder stellt fest, daß m eine Primzahl ist.

(Lehman 1) Man stellt fest, ob m einen Primteiler $\leq \lfloor m^{1/3} \rfloor$ besitzt (wie im Algorithmus PZ in (2.20) mit Hilfe einer geeigneten Folge $(d_i)_{i \geq 1}$). Findet man dabei einen Primteiler p von m, so bricht man ab. Findet man dabei keinen Primteiler $\leq \lfloor m^{1/3} \rfloor$ von m, so ist m entweder eine Primzahl oder das Quadrat einer Primzahl, oder es gibt Primzahlen p und q mit $m = pq$ und mit $m^{1/3} < p < q < m^{2/3}$.

(Lehman 2) Ist m eine Quadratzahl, so bricht man ab: Es ist $p := \sqrt{m}$ ein Primteiler $< m$ von m.

(Lehman 3) Man sucht ein Paar (k, d) natürlicher Zahlen mit $k \leq \lfloor m^{1/3} \rfloor$ und mit $d \leq \lfloor m^{1/6}/(4\sqrt{k}) \rfloor + 1$, für das $(\lfloor \sqrt{4km} \rfloor + d)^2 - 4km$ eine Quadratzahl ist. Hat man ein solches Paar (k, d) gefunden, so setzt man

$$a := \lfloor \sqrt{4km} \rfloor + d \quad \text{und} \quad b := \sqrt{a^2 - 4km}$$

und hat mit $m_1 := \mathrm{ggT}(a + b, m)$ einen Primteiler $< m$ von m ermittelt. Wenn man in dem angegebenen Bereich kein Paar (k, d) findet, für das die Zahl $(\lfloor \sqrt{4km} \rfloor + d)^2 - 4km$ eine Quadratzahl ist, so ist m eine Primzahl.

(2) Der Algorithmus leistet das Verlangte.

Beweis: Es sei $m \in \mathbb{N}$ mit $m > 100$.

(a) Wenn der Algorithmus in (Lehman 1) einen Primteiler $p \leq \lfloor m^{1/3} \rfloor$ von m findet, so ist p ein Primteiler $< m$ von m.

(b) Wenn der Algorithmus in (Lehman 2) feststellt, daß m eine Quadratzahl ist, so ist $p := \sqrt{m}$ ein Primteiler $< m$ von m.
(c) Es gelte: m ist keine Quadratzahl, und der Algorithmus ermittelt in (Lehman 1) keinen Primteiler $p \leq \lfloor m^{1/3} \rfloor$ von m und findet in (Lehman 3) ein Paar $(k,d) \in \mathbb{N} \times \mathbb{N}$ mit $k \leq \lfloor m^{1/3} \rfloor$ und $d \leq \lfloor m^{1/6}/(4\sqrt{k}) \rfloor + 1$, für das $(\lfloor \sqrt{4km} \rfloor + d)^2 - 4km$ eine Quadratzahl ist. Dann gilt $a := \lfloor \sqrt{4km} \rfloor + d \in \mathbb{N}$, $b := \sqrt{a^2 - 4km} \in \mathbb{N}_0$ und $b < a$ und daher $1 \leq a - b \leq a \leq a + b < 2a$, und es ist

$$a = \lfloor \sqrt{4km} \rfloor + d \leq \sqrt{4km} + d \leq \sqrt{4 \lfloor m^{1/3} \rfloor \cdot m} + \left\lfloor \frac{m^{1/6}}{4\sqrt{k}} \right\rfloor + 1 \leq$$
$$\leq \sqrt{4\, m^{1/3} \cdot m} + \frac{m^{1/6}}{4\sqrt{k}} + 1 \leq 2m^{2/3} + \frac{m^{1/6}}{4} + 1 \leq \frac{1}{2} m$$

(nach (14.5) wegen $m > 100$). Also gilt $1 \leq a - b \leq a + b < 2a \leq m$. Für $m_1 := \mathrm{ggT}(a+b, m)$ und $m_2 := m/m_1$ gilt $m = m_1 m_2$. Wäre $m_1 = 1$, so wären $a+b$ und m teilerfremd, und wegen $(a+b)(a-b) = a^2 - b^2 = 4km$ wäre daher m ein Teiler von $a - b$, aber wegen $1 \leq a - b < m$ ist dies nicht möglich. Wäre $m_2 = 1$, so wäre $m = m_1 = \mathrm{ggT}(a+b, m)$ ein Teiler von $a + b$, aber wegen $1 \leq a + b < m$ ist auch dies nicht möglich. Also ist m_1 ein nichttrivialer Teiler von m und somit ein Primteiler $< m$ von m.
(d) Ist m keine Primzahl, so besitzt m entweder einen Primteiler $\leq \lfloor m^{1/3} \rfloor$, oder m ist das Quadrat einer Primzahl, oder es gibt Primzahlen p und q mit $m = pq$ und mit $m^{1/3} < p < q < m^{2/3}$. Im ersten und im zweiten Fall findet der Algorithmus in (Lehman 1) bzw. in (Lehman 2) einen Primteiler p von m, im dritten Fall gibt es nach (14.4) ein Paar (k,d) natürlicher Zahlen mit $k \leq \lfloor m^{1/3} \rfloor$ und $d \leq \lfloor m^{1/6}/(4\sqrt{k}) \rfloor + 1$, für das $(\lfloor \sqrt{4km} \rfloor + d)^2 - 4km$ eine Quadratzahl ist, und hieraus lassen sich, wie in (c) gezeigt wurde, die Primteiler p und q von m berechnen.
(3) Der in diesem Abschnitt behandelte Faktorisierungsalgorithmus wurde 1974 von R. S. Lehman in [60] veröffentlicht. Zu der hier beschriebenen Version vergleiche man auch den Aufsatz [110] von M. Voorhoeve.

(14.7) Hilfssatz: *Für jedes $n \in \mathbb{N}$ gilt*

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} < 2\sqrt{n}.$$

Beweis: Ist $n = 1$, so ist nichts zu beweisen, und ist $n \geq 2$, so gilt

$$\frac{1}{\sqrt{k}} \leq \int_{k-1}^{k} \frac{1}{\sqrt{x}}\, dx \quad \text{für jedes } k \in \{2, 3, \ldots, n\}$$

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,