universität
wien

# DIPLOMARBEIT

Titel der Diplomarbeit

„Die Vermutung von Zaremba“

Verfasser

Johannes Puttinger

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag.rer.nat.)

Wien, im April 2010

| | |
|---|---|
| Studienkennzahl lt. Studienblatt: | A 405 |
| Studienrichtung lt. Studienblatt: | Mathematik |
| Betreuer: | Ao. Univ.-Prof. Dr. Christoph Baxa |

# Abstract

## Zusammenfassung

In dieser Diplomarbeit wird eine Vermutung behandelt, die im Jahr 1972 in einer Arbeit von S. K. Zaremba [15] veröffentlicht wurde. Es geht dabei um die Frage, ob es für jedes natürliche $m$ eine zu $m$ teilerfremde natürliche Zahl $a$ gibt, sodass in der regelmäßigen Kettenbruchentwicklung von $\frac{a}{m}$ alle Teilnenner durch eine von $a$ und $m$ unabhängige Schranke $b$ beschränkt sind. Numerische Berechnungen legen die Vermutung nahe, dass für alle $m \in \mathbb{N}$ der Wert $b = 5$, für hinreichend große $m$ sogar $b = 3$ genügt.

Im ersten Kapitel geben wir eine Einführung in die Theorie der (regelmäßigen) Kettenbrüche. Dabei werden sowohl endliche als auch unendliche Kettenbrüche behandelt. Insbesondere wird die Konvergenz unendlicher Kettenbrüche, sowie die Eindeutigkeit der Kettenbruchentwicklung bewiesen. Weiters wird durch Sätze von Euler und Lagrange die Rolle der periodischen Kettenbrüche vollständig geklärt. Außerdem beschreiben wir die in gewisser Hinsicht bestmögliche Approximation reeller Zahlen durch Näherungsbrüche. Dann führen wir Kontinuanten ein, die später mehrere Beweise vereinfachen werden.

Im zweiten Kapitel wird die Vermutung von Zaremba für Kettenbrüche und Kontinuanten formuliert und ihr Ursprung in einem Problem der numerischen Mathematik erläutert. Tatsächlich beschäftigte sich Zaremba in der anfangs erwähnten Arbeit mit einer speziellen Methode zur mehrdimensionalen numerischen Integration, der Methode der „guten Gitterpunkte".

In Kapitel 3 wird zuerst das sogenannte „Faltungslemma" bewiesen, mit dessen Hilfe die Richtigkeit der Vermutung für die Potenzen von 2, 3, 5 und 6 gezeigt wird. Weiters wird für positives $x \in \mathbb{R}$ eine untere Schranke für die Anzahl der Zahlen kleiner als $x$, die die Vermutung erfüllen, gegeben. Abschließend wird gezeigt, dass die folgende Abschwächung der Vermutung korrekt ist: Zu jedem $m \in \mathbb{N}$ existiert ein zu $m$ teilerfremdes $a$, sodass die Teilnenner von $\frac{a}{m}$ durch $B \cdot \log m \cdot (\log \log m)^2$ beschränkt sind (für ein gewisses $B > 0$, das von $m$ nicht abhängt).

## Summary

This thesis is devoted to a conjecture published by S. K. Zaremba [15] in 1972. It deals with the following question: given a positive integer $m$, does there exist a positive integer $a$, relatively prime to $m$, such that in the regular continued fraction expansion of $\frac{a}{m}$ all partial quotients are smaller or equal than a bound $b$, which is independent of $a$ and $m$. Numerical experiments suggest that for all $m \in \mathbb{N}$ the value $b = 5$, and for sufficiently large $m$ even $b = 3$ suffice.

In the first chapter we give a short introduction to the theory of (regular) continued fractions, dealing with both the finite and the infinite case. In particular, convergence of infinite continued fractions and uniqueness of continued fraction expansions are proved. Periodic continued fractions are discussed as well as the importance of convergents as best approximations (in a certain sense) of real numbers. Furthermore, we introduce continuants in order to simplify several proofs later on.

In chapter 2 Zaremba's conjecture is stated in terms of continued fractions as well as in terms of continuants, and its historic origin is described. In fact, in his paper mentioned earlier, Zaremba discussed a method of numerical integration, the "method of good lattice points".

The third chapter's starting point is the so-called "folding lemma", which allows us to confirm the validity of the conjecture for powers of 2, 3, 5 and 6. In addition, we give a lower bound for the number of positive integers smaller than $x > 0$ which satisfy the conjecture. Finally, it is shown that the following weakening of the conjecture holds: let $m \in \mathbb{N}$, then there exists some $a \in \mathbb{N}$, relatively prime to $m$, such that the partial quotients of the regular continued fraction expansion of $\frac{a}{m}$ are smaller or equal than $B \cdot \log m \cdot (\log \log m)^2$ (where $B > 0$ does not depend on $m$).

# Danksagung

Zuallererst möchte ich mich bei meinem Diplomarbeitsbetreuer Prof. Christoph Baxa bedanken, von dem die Idee zu dieser Arebeit kommt, und der sich viel Zeit für mich genommen hat.
Außerdem will ich mich bei meinen Eltern, der ganzen Familie, Freundinnen und Freunden bedanken, die mich in jeder Hinsicht bei meinem Studium und insbesondere während des Verfassens der Diplomarbeit unterstützt haben.

# Inhaltsverzeichnis

# 1 Kettenbrüche

## 1.1 Endliche Kettenbrüche

In Teil 1.1 folgen wir im Wesentlichen [6, S. 24-26] und [1, S. 24].

**Definition 1.** Sei $a_0 \in \mathbb{Z}, a_1, \ldots, a_n \in \mathbb{N}$. Dann nennt man

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

einen *endlichen regelmäßigen Kettenbruch* . Die $a_i$ $(0 \leq i \leq n)$ heißen *Elemente* oder *Teilnenner* des Kettenbruchs.
Für den Kettenbruch mit den Elementen $a_0, a_1, \ldots, a_n$ verwendet man auch die platzsparende Schreibweise $[a_0; a_1, \ldots, a_n]$, die auf Oskar Perron zurückgeht [11, S. 23].

*Bemerkung* 1. Weil alle $a_i \in \mathbb{N}$ $(1 \leq i \leq n)$, ist keiner der auftretenden Nenner gleich 0, der Ausdruck also wohldefiniert.

*Bemerkung* 2. Ein Ausdruck der Form

$$a_0 + \cfrac{c_1}{a_1 + \cfrac{c_2}{a_2 + \cfrac{c_3}{\ddots + \cfrac{c_n}{a_n}}}}$$

bei dem nicht alle $c_i$ $(1 \leq i \leq n)$ notwendig gleich 1 sind, heißt *allgemeiner endlicher Kettenbruch*. Da im weiteren nur *regelmäßige* endliche Kettenbrüche behandelt werden, werden wir ab jetzt den Zusatz *regelmäßig* weglassen, und nur von *endli-*

*chen Kettenbrüchen* schreiben (im Gegensatz zu *unendlichen Kettenbrüchen*, die im nächsten Kapitel vorgestellt werden).

**Satz 1.** *Für jedes* $r \in \mathbb{Q}$ *gibt es ein* $a_0 \in \mathbb{Z}$ *und* $a_1, \ldots, a_j \in \mathbb{N}$ *mit* $r = [a_0; a_1, \ldots, a_j]$.

*Beweis.* Es sei $r = \frac{a}{b}$, mit $a, b \in \mathbb{Z}, b > 0$. Man verwendet den Euklidischen Algorithmus:
Wähle $a_0, a_1, \ldots, a_j \in \mathbb{Z}, \quad r_1 := b, r_2, \ldots, r_{j+1} \in \mathbb{Z}$, sodass

$$\begin{aligned} a &= a_0 r_1 + r_2 && 0 \leq r_2 < r_1 && \text{und} \\ r_i &= a_i r_{i+1} + r_{i+2} && 0 \leq r_{i+2} < r_{i+1} && (1 \leq i \leq j) \end{aligned} \tag{1.1}$$

Dabei sei $j$ derart, dass $0 = r_{j+2} < r_{j+1}$, der Algorithmus breche also im $j+2$-ten Schritt ab.
Ist $i \geq 1$, so ist $r_{i+2} < r_i \overset{(1.1)}{\Rightarrow} a_i > 0$. Es ist $r = \frac{a}{r_1} = a_0 + \frac{r_2}{r_1}$.
Es sei schon gezeigt, dass

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{i-1} + \cfrac{r_{i+1}}{r_i}}}}}.$$

Aus $\frac{r_i}{r_{i+1}} = a_i + \frac{r_{i+2}}{r_{i+1}}$ folgt

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{i-1} + \cfrac{1}{a_i + \cfrac{r_{i+2}}{r_{i+1}}}}}}}.$$

Setzt man nun $i = j$, so ist die Behauptung gezeigt. □

*Bemerkung* 3. Man kann den Begriff des Kettenbruchs auch folgendermaßen einführen:

Für eine Folge von Unbestimmten $X_0, X_1, \ldots$ definiere rekursiv:

$$[X_0] := X_0 \tag{1.2}$$

$$[X_0; X_1, \ldots, X_i] := \left[X_0; X_1, \ldots, X_{i-2}, X_{i-1} + \frac{1}{X_i}\right] \quad \text{für } i \geq 1 \tag{1.3}$$

*Bemerkung* 4. Es sei nun $r = \frac{a}{b}$ und wie im Beweis zu Satz 1 seien $a_0, a_1, \ldots, a_j$ und $r_1, \ldots, r_{j+1}$ aus dem Euklidischen Algorithmus gewonnen. Es gilt dann $r = [a_0; a_1, \ldots, a_j]$, wobei dieser Ausdruck im Sinne der Definition in Bemerkung 3 zu verstehen ist, also (noch) nicht als Perrons Schreibweise aufgefasst werden soll.
Für den Beweis dieser Behauptung wird $a$ zu $r_0$ umbenannt und (wie schon im Beweis zu Satz 1) ist $b = r_1$. Mit dieser Bezeichnung wird zunächst

$$\frac{r_0}{r_1} = \left[a_0; a_1, \ldots, a_{i-1}, \frac{r_i}{r_{i+1}}\right] \tag{1.4}$$

für $i = 0, \ldots, j$ behauptet. Für $i = 0$ folgt das direkt aus (1.2).
Wenn $j > 0$ und (1.4) für $0 \leq i < j$ schon gezeigt ist, so folgt der Induktionsschritt aus

$$\frac{r_0}{r_1} = \left[a_0; a_1, \ldots, a_{i-1}, \frac{r_i}{r_{i+1}}\right] \overset{(1.1)}{=} \left[a_0; a_1, \ldots, a_{i-1}, a_i + \frac{r_{i+2}}{r_{i+1}}\right] \overset{(1.3)}{=} \left[a_0; a_1, \ldots, a_{i-1}, a_i, \frac{r_{i+1}}{r_{i+2}}\right]$$

Dadurch ist (1.4) gezeigt. Aus (1.4) erhält man nun für $i = j$, dass

$$r = \frac{r_0}{r_1} = [a_0; a_1, \ldots, a_j].$$

Das heißt das in Bemerkung 3 eingeführte Symbol $[X_0; X_1, \ldots, X_j]$ stimmt mit der Schreibweise von Perron überein.

*Bemerkung* 5. Für einen Bruch $\frac{a}{b}$ kann man also die Teilnenner aus dem Euklidischen Algorithmus ablesen. Deshalb folgt $a_j \geq 2$, da $a_j = \frac{r_j}{r_{j+1}}$ gilt, mit $r_j > r_{j+1}$.

*Bemerkung* 6. Die Darstellung von $r = [a_0; a_1, \ldots, a_j]$ ist nicht eindeutig, da wegen $a_j = (a_j - 1) + \frac{1}{1}$ für $a_j \geq 2$ auch $r = [a_0; a_1, \ldots, a_{j-1} - 1, 1]$ gilt.
Es wird später gezeigt, dass die Darstellung als Kettenbruch bis auf dieses Umschreiben eindeutig ist.

## 1.2 Unendliche Kettenbrüche

Für diesen Abschnitt wurde, wenn nicht anders angegeben, [1, S. 222-236] verwendet.

### 1.2.1 Der Kettenbruchalgorithmus

Wenn man $\alpha_i := \frac{r_i}{r_{i+1}}$ mit $i = 0, \ldots, j$ setzt, ist der Euklidische Algorithmus mit den Bezeichnungen aus dem Beweis zu Satz 1 äquivalent zu

$$\begin{aligned} \alpha_0 &= a_0 + \alpha_1^{-1} \\ \alpha_1 &= a_1 + \alpha_2^{-1} \\ &\vdots \\ \alpha_{j-1} &= a_{j-1} + \alpha_j^{-1} \\ \alpha_j &= a_j \end{aligned}$$

mit $\alpha_1, \ldots, \alpha_j > 1$. Es gilt $a_i = \lfloor \alpha_i \rfloor$ für $i = 0, \ldots, j$, beziehungsweise $\alpha_{i+1} = \{\alpha_i\}^{-1}$ für $i = 0, \ldots, j-1$, wobei für $x \in \mathbb{R}$ der Ausdruck $\lfloor x \rfloor$ die größte ganze Zahl $\leq x$ bezeichnet und $x = \lfloor x \rfloor + \{x\}$.
Die Bezeichnung $\lfloor x \rfloor$ heißt auch Gaußklammer von $x$, $\{x\}$ der Bruchteil von $x$.

In dieser Form ist der Algorithmus auch auf $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ anwendbar:
Setze $\alpha_0 := \alpha, \quad a_0 := \lfloor \alpha_0 \rfloor$, und weil $\alpha_0 \notin \mathbb{Q}$, ist $0 < \{\alpha_0\} < 1$.
Setze weiters $\alpha_1 := \{\alpha_0\}^{-1}$.
Es ist $a_0 \in \mathbb{Z}$, $\alpha_0 = a_0 + \alpha_1^{-1}$, $\alpha_1 > 1$ und $\alpha_1 \notin \mathbb{Q}$. Fahre induktiv fort: Für $i \geq 1$ seien bereits

$$\begin{gathered} \alpha_j = a_j + \alpha_{j+1}^{-1} \quad \text{für } j = 0, \ldots, i-1 \\ \text{mit } a_0 \in \mathbb{Z},\ a_1, \ldots, a_{i-1} \in \mathbb{N} \text{ und } \alpha_j > 1,\ \alpha_j \notin \mathbb{Q} \quad \text{für } j = 1, \ldots, i \end{gathered} \tag{1.5}$$

gefunden.
Dann definiert man $a_i := \lfloor \alpha_i \rfloor (\in \mathbb{N})$; es ist dann $0 < \{\alpha_i\} < 1$ und $\alpha_i$ ist irrational, also ist $\alpha_{i+1} := \{\alpha_i\}^{-1}$ größer als 1 und irrational und es gilt $\alpha_i = a_i + \alpha_{i+1}^{-1}$.
Somit ist (1.5) für alle $i \in \mathbb{N}$ gültig.

Unter Beachtung von Bemerkung 3 erhält man nun:

$$\alpha = [a_0; a_1, \ldots, a_{i-1}, \alpha_i] \quad \text{für} \quad i = 0, 1, \ldots \tag{1.6}$$

Das ist leicht zu sehen: Der Fall $i = 0$ folgt sofort aus $\alpha = \alpha_0$ und (1.2) .
Wenn die Gleichung in (1.6) für ein $i \geq 0$ schon gilt, ersetze $\alpha_i$ durch $a_i + \frac{1}{\alpha_{i+1}}$ und (1.3) ergibt den Induktionsschritt von $i$ auf $i + 1$.
Der Algorithmus ordnet jedem $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ eine wohldefinierte unendliche Folge

$$a_0, a_1, a_2, \ldots$$

ganzer Zahlen zu, wobei $a_i > 0 \quad \forall i > 0$.

**Definition 2.** Mit den vorangegangenen Bezeichnungen nennt man $[a_0; a_1, a_2 \ldots]$ einen *unendlichen (regelmäßigen) Kettenbruch*. Der Zusatz *regelmäßig* wird wieder weggelassen, da andere Kettenbrüche nicht Gegenstand dieser Arbeit sind.

## 1.2.2 Konvergenz von Kettenbrüchen

Es soll nun die Konvergenz von Kettenbrüchen untersucht werden. Das wird parallel für endliche und unendliche Kettenbrüche passieren.
Sei allgemein $a_0, a_1, a_2, \ldots, a_k(, \ldots)$ eine Folge ganzer Zahlen mit $a_i \in \mathbb{N} \quad \forall i > 0$. Sollte die Folge endlich sein, so sei $a_k$ das letzte Glied. Im Folgenden wird im endlichen Fall immer $i \leq k$ vorausgesetzt.
Es werden zwei neue Folgen $(p_i)_{i\geq -2}$ und $(q_i)_{i\geq -2}$ rekursiv definiert:

$$\begin{aligned} p_{-2} &:= 0 \quad p_{-1} := 1 \quad p_i := a_i p_{i-1} + p_{i-2} \\ q_{-2} &:= 1 \quad q_{-1} := 0 \quad q_i := a_i q_{i-1} + q_{i-2} \end{aligned} \tag{1.7}$$

für $i = 0, 1, \ldots, k(, \ldots)$.
Für alle $i \geq 0$ gilt dann $p_i \in \mathbb{Z}$ und $q_i \in \mathbb{N}$. Weil $q_0 = 1$ und $q_i \geq q_{i-1} + q_{i-2}$ sieht man, dass $q_i \geq i$ für $i \geq 1$ . Daher ist $(q_i)_{i\geq 1}$ streng monoton wachsend und im unendlichen Fall unbeschränkt.
Zum Beweis des zentralen Satzes dieses Abschnitts, über die Konvergenz von unendlichen Kettenbrüchen, werden ein paar Hilfsresultate benötigt:

**Lemma 1.** *Für alle vorkommenden $i \geq 0$ und die Unbestimmte $X$ ist*

$$[a_0; a_1, \ldots, a_{i-1}, X] = \frac{p_{i-1}X + p_{i-2}}{q_{i-1}X + q_{i-2}}$$

*Beweis.* Der Beweis erfolgt mittels Induktion nach $i$.
Für $i = 0$ ergeben (1.2) und (1.7) die Aussage.

Sei das Ergebnis für $i \geq 0$ schon gezeigt. Dann gilt:

$$[a_0;a_1,\ldots,a_i,X] \overset{(1.3)}{=} \left[a_0;a_1,\ldots,a_{i-1},a_i+\frac{1}{X}\right]$$
$$= \frac{p_{i-1}(a_i+\frac{1}{X})+p_{i-2}}{q_{i-1}(a_i+\frac{1}{X})+q_{i-2}} \overset{(1.7)}{=} \frac{p_iX+p_{i-1}}{q_iX+q_{i-1}}$$

□

Wenn man nun $a_i$ für $X$ einsetzt in Lemma 1 , so erhält man

$$[a_0;a_1,\ldots,a_i] = \frac{p_i}{q_i} =: A_i.$$

**Definition 3.** Für $i \geq 0$ (und wenn notwendig $i \leq k$) heißt $A_i$ der *$i$-te Näherungsbruch* des möglicherweise endlichen Kettenbruchs $[a_0;a_1,\ldots,a_k,\ldots]$. Dabei werden $p_i$ der *$i$-te Näherungszähler* und $q_i$ der *$i$-te Näherungsnenner* genannt.

**Lemma 2.** *1. Für $i \geq -1$ gilt*

$$p_{i-1}q_i - p_iq_{i-1} = (-1)^i. \tag{1.8}$$

*Insbesondere gelten* $\mathrm{ggT}(p_i,q_i) = 1$ *für $i \geq -2$ und*

$$A_{i-1} - A_i = \frac{(-1)^i}{q_{i-1}q_i} \quad \textit{für} \quad i \geq 1. \tag{1.9}$$

*2. Für $i \geq 0$ gilt*

$$p_{i-2}q_i - p_iq_{i-2} = (-1)^{i-1}a_i. \tag{1.10}$$

*Insbesondere gilt für $i \geq 2$*

$$A_i - A_{i-2} = \frac{(-1)^i a_i}{q_{i-2}q_i}. \tag{1.11}$$

*Beweis.* 1. Der Beweis erfolgt mit Induktion nach $i$.

Für $i = -1$ folgt die Behauptung sofort aus (1.7).

Sei nun (1.8) für ein $i \geq -1$ richtig. Dann berechnet man

$$p_iq_{i+1} - p_{i+1}q_i \overset{(1.7)}{=} p_i(a_{i+1}q_i + q_{i-1}) - (a_{i+1}p_i + p_{i-1})q_i$$
$$= p_iq_{i-1} - p_{i-1}q_i \overset{\text{Induktionsannahme}}{=} (-1)^{i+1}$$

Die restlichen Behauptungen von Punkt 1 folgen trivialerweise aus (1.8).

2. Berechne dafür

$$\begin{aligned} p_{i-2}q_i - p_iq_{i-2} &\overset{(1.7)}{=} p_{i-2}(a_iq_{i-1} + q_{i-2}) - (a_ip_{i-1} + p_{i-2})q_{i-2} \\ &= a_i(p_{i-2}q_{i-1} - p_{i-1}q_{i-2}) \overset{(1.8)}{=} a_i(-1)^{i-1}. \end{aligned}$$

Damit ist die erste Behauptung in diesem Punkt gezeigt. Der Zusatz folgt daraus trivialerweise.

□

**Lemma 3.** *Die (möglicherweise endlichen) Folgen der Näherungsbrüche $A_0, A_2, A_4, \ldots$ beziehungsweise $A_1, A_3, A_5, \ldots$ sind streng monoton wachsend beziehungsweise streng monoton fallend.*
*Jedes Glied der ersten Folge ist kleiner als jedes Glied der zweiten Folge.*

*Beweis.* Sei zuerst $i \geq 2$ gerade. Dann folgt $A_i > A_{i-2}$ aus (1.11), das heißt die erste Folge ist monoton wachsend.
Wenn $i \geq 3$ ungerade, folgt wieder aus (1.11), dass $A_i < A_{i-2}$, das heißt die zweite Folge ist streng monoton fallend.
Wenn man jetzt für irgendwelche $s, t \in \mathbb{N}_0$ die Näherungsbrüche $A_{2s}$ und $A_{2t+1}$ vergleicht, so gilt

- für $s \leq t$:

$$A_{2s} \leq A_{2t} < A_{2t+1}.$$

  Die letzte Ungleichung folgt aus (1.9), wenn man $i = 2t + 1$ setzt.

- für $s > t$ gilt wegen der obigen Überlegungen

$$A_{2s} < A_{2s+1} < A_{2t+1}$$

□

Nach diesen Vorbereitungen sind wir nun in der Lage, den wichtigen Konvergenzsatz für Kettenbrüche zu zeigen.

**Satz 2** (Konvergenzsatz)**.** *Gegeben sei ein unendlicher Kettenbruch $[a_0; a_1, a_2, \ldots]$ mit $a_0 \in \mathbb{Z}$ und $a_1, a_2, \ldots \in \mathbb{N}$. Die unendliche Folge $(A_i)_{i\geq 0}$ der Näherungsbrüche konvergiert.*

*Sei $\alpha$ der Grenzwert. Dann gilt:*

$$A_0 < A_2 < \ldots < \alpha < \ldots < A_3 < A_1 \quad \textit{und} \quad \alpha \notin \mathbb{Q} \tag{1.12}$$

*Beweis.* Aufgrund von Lemma 3 ist die Folge $A_0, A_2, A_4, \ldots$ streng monoton wachsend und nach oben beschränkt, zum Beispiel durch $A_1$. Sie konvergiert also gegen einen Wert $\alpha^- \in \mathbb{R}$.
Genauso ist die Folge $A_1, A_3, A_5, \ldots$ streng monoton fallend und nach unten beschränkt, zum Beispiel durch $A_0$. Sie konvergiert daher gegen ein $\alpha^+ \in \mathbb{R}$ und es gilt $\alpha^- \leq \alpha^+$.
Es gilt nun $\forall s \geq 1$

$$0 \leq \alpha^+ - \alpha^- < A_{2s-1} - A_{2s} \overset{(1.9)}{=} \frac{1}{q_{2s-1}q_{2s}} \leq \frac{1}{(2s-1)(2s)} \tag{1.13}$$

Für die letzte Ungleichung wurde verwendet, dass $q_i \geq i$ für $i \geq 1$, was schon früher angemerkt wurde.
Wenn man in (1.13) $s \to \infty$ gehen läßt, folgt $\alpha^+ = \alpha^- =: \alpha$.
Für den Beweis der Irrationalität von $\alpha$, nehme indirekt an, dass $\alpha \in \mathbb{Q}$, also

$$\alpha = \frac{a}{b} \quad (a \in \mathbb{Z}, b \in \mathbb{N}).$$

Für alle $i \geq 0$ gilt $A_i \neq \alpha$ und daher

$$\frac{1}{bq_i} \leq |\alpha - A_i| < |A_{i+1} - A_i| \overset{(1.9)}{=} \frac{1}{q_i q_{i+1}}$$

Das heißt $q_{i+1} < b$ für alle $i \geq 0$, im Widerspruch zur Unbeschränktheit der Folge $(q_i)_{i \geq -2}$. □

### 1.2.3 Eindeutigkeit der Kettenbruchentwicklung

Im Kapitel über endliche Kettenbrüche wurde bereits bemerkt, dass man endliche Kettenbrüche immer auf mindestens zwei Arten schreiben kann:

$$[a_0; a_1, \ldots, a_j] = [a_0; a_1, \ldots, a_{j-1}, a_j - 1, 1] \quad (a_j \geq 2)$$

Der folgende Satz klärt die Frage der Eindeutigkeit für endliche und unendliche Kettenbrüche und liefert darüberhinaus ein Kriterium (notwendig und hinreichend) für die Irrationalität reeller Zahlen.

**Satz 3.** *Jedes $\alpha \in \mathbb{R}$ läßt sich in eindeutiger Weise in einen Kettenbruch entwickeln. Dieser ist endlich genau dann wenn $\alpha$ rational ist.*
*Im endlichen Fall muss man dabei verbieten, dass das letzte Element gleich* 1 *ist, falls es einen positiven Index hat.*

*Beweis.* **Existenz:** Die Existenz der Kettenbruchentwicklung für rationale Zahlen wurde schon im Kapitel über endliche Kettenbrüche in Satz 1 behandelt.
Für $\alpha \notin \mathbb{Q}$ gilt für alle $i \geq 0$ wegen (1.5) und (1.6) die Gleichung

$$\alpha = [a_0; a_1, a_2, \ldots, a_i, \alpha_{i+1}],$$

wobei $\alpha_{i+1} > 1$ und irrational ist.
Nach Lemma 1 ist für $i \geq 0$

$$\alpha = \frac{p_i \alpha_{i+1} + p_{i-1}}{q_i \alpha_{i+1} + q_{i-1}}$$

also folgt

$$\begin{aligned} \alpha - \frac{p_i}{q_i} &= \frac{q_i(p_i\alpha_{i+1} + p_{i-1}) - p_i(q_i\alpha_{i+1} + q_{i-1})}{q_i(q_i\alpha_{i+1} + q_{i-1})} \\ &\overset{(1.8)}{=} \frac{(-1)^i}{q_i(q_i\alpha_{i+1} + q_{i-1})} \qquad \forall i \geq 0 \end{aligned} \tag{1.14}$$

Das ergibt $|\alpha - A_i| < \frac{1}{q_i^2}$, also $\alpha = \lim_{i\to\infty} A_i$.

Das heißt die Zahl $\alpha$ aus dem Algorithmus aus Kapitel 1.2.1 für unendliche Kettenbrüche stimmt mit dem Grenzwert $\alpha$ aus dem Konvergenzsatz überein und somit liefert der besagte Algorithmus tatsächlich eine Entwicklung des irrationalen $\alpha$ in einen unendlichen Kettenbruch.

**Eindeutigkeit:** Angenommen $\alpha \in \mathbb{R}$ habe zwei Entwicklungen

$$[a_0; a_1, a_2, \ldots] = \alpha = [a_0'; a_1', a_2', \ldots] \tag{1.15}$$

Es ist klar, dass die Entwicklungen entweder beide endlich (also $\alpha \in \mathbb{Q}$), oder beide unendlich (also $\alpha \notin \mathbb{Q}$) sind.
Sei nun $i \geq 0$ und $a_l = a_l'$ für $l = 0, 1, \ldots, i-1$ bereits gezeigt. Im endlichen Fall wird natürlich vorausgesetzt, dass die Kettenbrüche in (1.15) mindestens $i+1$ Elemente haben.

Wenn man $\alpha_i := [a_i; a_{i+1}, a_{i+2}, \ldots]$ und $\alpha_i^{'} := [a_i^{'}; a_{i+1}^{'}, a_{i+2}^{'}, \ldots]$ setzt, dann folgt aus Lemma 1 und (1.15)

$$\frac{p_{i-1}\alpha_i + p_{i-2}}{q_{i-1}\alpha_i + q_{i-2}} = [a_0; a_1, \ldots, a_{i-1}, \alpha_i] = \alpha = [a_0^{'}; a_1^{'}, \ldots, a_{i-1}^{'}, \alpha_i^{'}] = \frac{p_{i-1}\alpha_i^{'} + p_{i-2}}{q_{i-1}\alpha_i^{'} + q_{i-2}}.$$

Vergleicht man die beiden Brüche, so erhält man nach kurzer Rechnung

$$\alpha_i \underbrace{(p_{i-1}q_{i-2} - p_{i-2}q_{i-1})}_{\neq 0 \text{ nach (1.8)}} = \alpha_i^{'} \underbrace{(p_{i-1}q_{i-2} - p_{i-2}q_{i-1})}_{\neq 0 \text{ nach (1.8)}}$$

also $\alpha_i = \alpha_i^{'}$.
Wenn die beiden Kettenbrüche unendlich sind, erhält man $a_i + \frac{1}{\alpha_{i+1}} = a_i^{'} + \frac{1}{\alpha_{i+1}^{'}}$, also $|a_i - a_i^{'}| = |\frac{1}{\alpha_{i+1}} - \frac{1}{\alpha_{i+1}^{'}}| < 1$, weil $\alpha_{i+1}, \alpha_{i+1}^{'} > 1$. Daher gilt $a_i = a_i^{'}$.
Dieselbe Schlussfolgerung zieht man für endliche Kettenbrüche mit mindestens $i + 2$ Gliedern. Hier wird die Voraussetzung, dass das letzte Element $\neq 1$ sein muss, benutzt.
Wenn beide Kettenbrüche die Länge $k + 1$ haben, so ist

$$a_k^{'} = \alpha_k^{'} = \alpha_k = a_k$$

Indirekt angenommen, die Kettenbrüche in (1.15) hätten verschiedene Länge, zum Beispiel die rechte Seite in (1.15) die Länge $k+1$, die linke Seite mindestens die Länge $k + 2$, dann ist

$$a_k^{'} - a_k = \frac{1}{\alpha_{k+1}} \in (0, 1) \qquad \text{weil} \quad \alpha_{k+1} > 1$$

Das steht im Widerspruch zur Ganzzahligkeit von $a_k$ und $a_k^{'}$, wobei man wiederum benutzt, dass das letzte Element $\neq 1$ ist.

□

### 1.2.4 Periodische Kettenbrüche

In diesem Abschnitt werden wir uns genauer mit speziellen unendlichen Kettenbrüchen beschäftigen, nämlich den periodischen.

**Definition 4.** Ein unendlicher Kettenbruch $[a_0; a_1, a_2, \ldots]$ heißt *periodisch*, wenn die Folge $a_1, a_2, \ldots$ natürlicher Zahlen periodisch ist, das heißt, $\exists l \in \mathbb{N}_0$ und $\exists h \in \mathbb{N}$,

sodass

$$a_i = a_{i+h} \qquad \forall i > l \tag{1.16}$$

Die Zahlen $a_1, \ldots, a_l$ heißen *Vorperiode*, wenn $l$ minimal gewählt ist, sodass (1.16) gilt. Die nichtnegative ganze Zahl $l$ heißt dann die *Vorperiodenlänge*.
Das minimale $h$ für das (1.16) gilt, heißt *Periodenlänge*. Die Zahlen $a_{l+1}, \ldots, a_{l+h}$ heißen die *Periode*.
Ist also $[a_0; a_1, a_2, \ldots]$ periodisch mit Vorperiodenlänge $l$ und Periodenlänge $h$, so schreibt man den Kettenbruch auch als

$$[a_0; a_1, \ldots, a_l, \overline{a_{l+1}, \ldots, a_{l+h}}]$$

*Beispiel* 1. Die reelle Zahl $\sqrt{2}$ ist irrational und hat deshalb eine unendliche Kettenbruchdarstellung. Zur Berechnung dieser betrachte $(\sqrt{2}-1)(\sqrt{2}+1) = 1$, woraus

$$\sqrt{2} = 1 + \frac{1}{1+\sqrt{2}}$$

folgt. In der rechten Seite der letzten Gleichung kann man für $\sqrt{2}$ die ganze rechte Seite einsetzen:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{1+\sqrt{2}}} = [1; 2, 1+\sqrt{2}]$$

Fortgesetztes Anwenden führt zu der Kettenbruchdarstellung von

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

Dieses Beispiel ist Spezialfall der allgemeineren Tatsache:

**Proposition 1.** *Für $D \in \mathbb{N}$ gilt $(1+D)^{\frac{1}{2}} = [D; 2D, 2D, 2D, \ldots]$.*

*Beweis.* Setze $\alpha := [2D; 2D, 2D, 2D, \ldots]$.
Dann gilt $\alpha = 2D + \alpha^{-1}$ beziehungsweise durch einfache Umformungen

$$\alpha^2 - 2D\alpha - 1 = 0.$$

Die quadratische Gleichung hat eine einzige positive Lösung für $\alpha$, nämlich

$$D + (1+D^2)^{\frac{1}{2}}.$$

Daraus folgt die Behauptung. □

Die folgenden beiden Sätze klären die Struktur der periodischen Kettenbrüche vollständig auf. Es gilt nämlich nach einem Satz von Euler, dass ein unendlicher periodischer Kettenbruch eine reell-quadratische Irrationalzahl definiert. Die Umkehrung dieses Resultats ist auch richtig und als Satz von Lagrange bekannt.
Zuerst beweisen wir ein Lemma, das im Beweis des Satzes von Euler benötigt wird:

**Lemma 4.** *Für $j \neq k \in \mathbb{N}_0$ gilt stets $q_j q_{k-1} \neq q_{j-1} q_k$*

*Beweis.* O.B.d.A. sei $k > j \geq 0$. Für $j = 0$ ist $q_{j-1} q_j = q_{-1} q_k = 0$, aber $q_j q_{k-1} \neq 0$.
Sei nun $k > j \geq 1$. Dann sind alle vorkommenden $q_i$ nicht null.
Nehme nun indirekt an, es wäre $q_j q_{k-1} = q_{j-1} q_k$. Da $q_j$ die linke Seite der Gleichung teilt, teilt es auch die rechte Seite. Aus (1.8) folgt, dass $q_j$ und $q_{j-1}$ teilerfremd sind, deshalb gilt $q_j | q_k$.
Mit der analogen Begründung gilt auch $q_k | q_j$.
Weil beide positiv sind, folgt $q_j = q_k$, im Widerspruch zum streng monotonen Wachstum der Folge $(q_i)_{i \geq 1}$. □

**Satz 4** (Euler)**.** *Der Wert eines unendlichen periodischen Kettenbruchs ist eine reell-quadratische Irrationalzahl.*

*Beweis.* Es sei der periodische Kettenbruch $[a_0; a_1, \ldots, a_l, \overline{a_{l+1}, \ldots, a_{l+h}}]$ gegeben und $\alpha$ sein Wert.
Setze $\alpha_i := [a_i; a_{i+1}, a_{i+2} \ldots]$ für $i \geq 0$ (also insbesondere $\alpha_0 = \alpha$).
Aus Lemma 1 ergibt sich dann für $i \geq 0$

$$\alpha = [a_0; a_1, a_2, \ldots, a_{i-1}, \alpha_i] = \frac{p_{i-1}\alpha_i + p_{i-2}}{q_{i-1}\alpha_i + q_{i-2}}. \tag{1.17}$$

Nach einer leichten Umformung erhält man daraus

$$\alpha_i = \frac{p_{i-2} - q_{i-2}\alpha}{q_{i-1}\alpha - p_{i-1}} \qquad \text{für} \quad i \geq 0 \tag{1.18}$$

wobei der Nenner nicht verschwindet, weil $\alpha$ irrational ist.

Aus $a_{i+h} = a_i$ für alle $i > l$ folgt $\alpha_{i+h} = \alpha_i$ für alle $i > l$. Daher folgt aus (1.18):

$$\frac{p_{i+h-2} - q_{i+h-2}\alpha}{\alpha q_{i+h-1} - p_{i+h-1}} = \frac{p_{i-2} - \alpha q_{i-2}}{\alpha q_{i-1} - p_{i-1}} \qquad \text{für} \quad i > l \tag{1.19}$$

Umformung von (1.19) ergibt für $i > l$: Die Zahl $\alpha$ erfüllt die quadratische Gleichung $R_i\alpha^2 + S_i\alpha + T_i = 0$, wobei

$$\begin{aligned} R_i &:= q_{i+h-1}q_{i-2} - q_{i+h-2}q_{i-1} \\ S_i &:= p_{i+h-2}q_{i-1} + p_{i-1}q_{i+h-2} - p_{i-2}q_{i+h-1} - p_{i+h-1}q_{i-2} \\ T_i &:= p_{i+h-1}p_{i-2} - p_{i-1}p_{i+h-2} \end{aligned}$$

Anwendung des gerade bewiesenen Lemma 4 mit $j = i - 1, \quad k = i + h - 1$ (und dadurch $j, k \geq 0$ für $i > 0$ und verschieden, weil $h \geq 1$) ergibt, dass $R_i \neq 0$ für $i > 0$. Insbesondere ist $R_i \neq 0$ für $i > l$ und $\alpha$ ist algebraisch vom Grad höchstens 2. Wegen der Unendlichkeit der Kettenbruchentwicklung ist $\alpha$ irrational, sein Grad also tatsächlich gleich 2. □

**Satz 5** (Lagrange)**.** *Die Kettenbruchentwicklung einer reel-quadratischen Irrationalzahl ist periodisch.*

*Beweis.* Sei $\alpha \in \mathbb{R}$ eine reell-quadratische Irrationalzahl und $[a_0; a_1, a_2, \ldots]$ ihre (nach dem Eindeutigkeitssatz 3) unendliche Kettenbruchentwicklung.
Nach Voraussetzung gibt es ein Polynom $P(X) := RX^2 + SX + T \in \mathbb{Z}[X]$, $P$ nicht das Nullpolynom, mit $\alpha$ als Wurzel. Da $\alpha$ irrational ist, gilt $R \neq 0$ und die Diskriminante $S^2 - 4RT$ ist positiv, aber keine Quadratzahl.

Wegen (1.17) gilt für alle $i \geq 0$:

$$R(p_{i-1}\alpha_i + p_{i-2})^2 + S(p_{i-1}\alpha_i + p_{i-2})(q_{i-1}\alpha_i + q_{i-2}) + T(q_{i-1}\alpha_i + q_{i-2})^2 = 0$$

Daraus ergibt sich mit den Bezeichnungen

$$\begin{aligned} R_i^* &:= Rp_{i-1}^2 + Sp_{i-1}q_{i-1} + Tq_{i-1}^2 \\ S_i^* &:= 2Rp_{i-1}p_{i-2} + S(p_{i-1}q_{i-2} + p_{i-2}q_{i-1}) + 2Tq_{i-1}q_{i-2} \\ T_i^* &:= R_{i-1}^* \end{aligned}$$

dass $\alpha_i$ Wurzel von $P_i := R_i^*X^2 + S_i^*X + T_i^* \in \mathbb{Z}[X]$ ist, wobei $i \geq 0$. Eine leichte Rechnung zeigt die Gültigkeit der Matrizengleichung

$$\begin{pmatrix} 2R_i^* & S_i^* \\ S_i^* & 2T_i^* \end{pmatrix} = \begin{pmatrix} p_{i-1} & q_{i-1} \\ p_{i-2} & q_{i-2} \end{pmatrix} \begin{pmatrix} 2R & S \\ S & 2T \end{pmatrix} \begin{pmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{pmatrix}.$$

Vergleich der Determinanten ergibt

$$4R_i^*T_i^* - S_i^{*2} = (\underbrace{p_{i-1}q_{i-2} - p_{i-2}q_{i-1}}_{=(-1)^i \text{ nach (1.8)}})(4RT - S^2)(\underbrace{p_{i-1}q_{i-2} - p_{i-2}q_{i-1}}_{=(-1)^i \text{ nach (1.8)}}),$$

also für alle $i \geq 0$:

$$S_i^{*2} - 4R_i^*T_i^* = S^2 - 4RT \tag{1.20}$$

Anwendung von (1.14) mit $i-1$ statt $i$ ergibt

$$|q_{i-1}\alpha - p_{i-1}| = \frac{1}{q_{i-1}\alpha_i + q_{i-2}} < \frac{1}{q_{i-1}a_i + q_{i-2}} = \frac{1}{q_i} \qquad \text{für} \quad i \geq 1$$

Daher existiert für alle $i \geq 0$ ein $\vartheta_i \in \mathbb{R}, \quad 0 < |\vartheta_i| < 1$:

$$p_{i-1} = \alpha q_{i-1} + \vartheta_i q_i^{-1}$$

Setzt man das in die Definition von $R_i^*$ ein, so erhält man

$$R_i^* = q_{i-1}^2(\underbrace{R\alpha^2 + S\alpha + T}_{=P(\alpha)}) + (2R\alpha + S)\vartheta_i\frac{q_{i-1}}{q_i} + R\vartheta_i^2 q_i^{-2}$$

Da $P(\alpha) = 0$, kann man $R_i^*$ wie folgt abschätzen:

$$|R_i^*| \leq |2R\alpha + S| \cdot \underbrace{|\vartheta_i\frac{q_{i-1}}{q_i}|}_{\leq 1} + |R| \cdot \underbrace{|\vartheta_i^2 q_i^{-2}|}_{\leq 1} \leq |2R\alpha + S| + |R|$$

für alle $i \geq 0$.
Das heißt, $(R_i^*)_{i\geq 0}$ und damit auch $(T_i^*)_{i\geq 0}$ sind beschränkte Folgen ganzer Zahlen. Wegen (1.20) ist dasselbe für $(S_i^*)_{i\geq 0}$ richtig.
Daher muss es (nach dem Schubfachprinzip) ein $(R^*, S^*, T^*) \in \mathbb{Z}^3$ geben, sodass

$$S^{*2} - 4R^*T^* = S^2 - 4RT$$

und für unendlich viele Indizes $i$ gilt

$$R_i^* = R^*$$
$$S_i^* = S^*$$
$$T_i^* = T^*$$

Weil $S^2 - 4RT$ kein Quadrat ist, ist auch $S^{*2} - 4R^*T^*$ keines, und daher $R^* \cdot T^* \neq 0$. Daher hat das Polynom $P^*(X) := R^*X^2 + S^*X + T^*$ zwei unterschiedliche reelle Wurzeln.
Andererseits ist $P^*(\alpha_i) = 0$ für unendlich viele Indizes $i$. Also existieren verschiedene $j, k \in \mathbb{N}_0$, o.B.d.A. $j < k$, mit $\alpha_k = \alpha_j$, das heißt

$$[a_k; a_{k+1}, a_{k+2}, \ldots] = [a_j; a_{j+1}, a_{j+2}, \ldots].$$

Wegen der Eindeutigkeit der Kettenbruchentwicklung ist mit $h := k - j \in \mathbb{N}$

$$a_{i+h} = a_i \quad \text{für alle } i \geq j.$$

Also hat $\alpha$ tatsächlich eine periodische Kettenbruchentwicklung. □

*Bemerkung* 7. Bis jetzt haben wir folgende Tatsachen gezeigt:

- $\alpha$ ist vom Grad 1 (also rational) genau dann, wenn seine Kettenbruchentwicklung endlich ist.
- $\alpha$ ist vom Grad 2 genau dann, wenn seine unendliche Kettenbruchentwicklung periodisch ist.

Eine vergleichbare Aussage für algebraische $\alpha \in \mathbb{R}$ von höherem Grad ist nicht bekannt.

### 1.2.5 Approximation reeller Zahlen durch rationale; Beste Näherungen

Für die Folge der Näherungsbrüche $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}, \ldots$ von $\alpha$ (für $\alpha \in \mathbb{Q}$ soll diese Folge immer mit $\frac{p_k}{q_k}$ enden), ergibt (1.14) bei Übergang zum Betrag

$$\left|\alpha - \frac{p_i}{q_i}\right| = \frac{1}{q_i(\alpha_{i+1}q_i + q_{i-1})} \tag{1.21}$$

und daraus folgt

$$\frac{1}{q_i(q_{i+1} + q_i)} < \left|\alpha - \frac{p_i}{q_i}\right| \leq \frac{1}{q_i q_{i+1}} \tag{1.22}$$

wobei für rationales $\alpha$ die Bedingung $i < k$ verlangt werden muss.
Rechts tritt Gleichheit genau dann auf, wenn $\alpha \in \mathbb{Q}$ und $i = k - 1$. Dann ist nämlich $\alpha_{i+1} = \alpha_k = a_k$.

Die Ungleichung (1.22) bietet eine Möglichkeit, eine reelle Zahl $\alpha$ durch rationale Zahlen zu approximieren und gleichzeitig eine gute Abschätzung für den Approximationsfehler zu geben. Dabei wird $\alpha$ durch die Näherungsbrüche seiner Kettenbruchentwicklung angenähert.
In diesem Kapitel soll gezeigt werden, dass diese Methode der Annäherung in einem bestimmten Sinn optimal ist, wenn man von wenigen (explizit angebbaren) Spezialfällen absieht, für die das nicht zutrifft.
Wir werden ab nun Abschätzungen der Größe $|b\alpha - a|$ statt $|\alpha - \frac{a}{b}|$ betrachten. In welcher Beziehung diese Varianten der Abschätzung zueinander stehen, wird in einer Bemerkung am Ende dieses Abschnitts erklärt.

Das folgende Lemma wird für die weiteren Aussagen benötigt:

**Lemma 5.** *1. Bei $\alpha \in \mathbb{Q}$ gilt für $c \in \mathbb{Z}$, $d \in \mathbb{N}$ die Ungleichung*

$$|q_k\alpha - p_k| \leq |d\alpha - c|$$

*mit Gleichheit genau für $\frac{c}{d} = \frac{p_k}{q_k} (= \alpha)$.*

*2. Wenn $\alpha \in \mathbb{Q}$ und $q_k > 1$, dann gilt für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $d < q_k$ die Ungleichung*

$$|q_{k-1}\alpha - p_{k-1}| \leq |d\alpha - c|$$

*mit Gleichheit genau dann, wenn $(c, d) = (p_{k-1}, q_{k-1})$ beziehungsweise $(c, d) = (p_k - p_{k-1}, q_k - q_{k-1})$.*

*3. Wenn $\alpha \in \mathbb{Q}$, $0 \leq i \leq k-2$ beziehungsweise $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, $i \geq 0$, aber nicht gleichzeitig $i = 0$ und $a_1 = 1$ gilt, dann hat man für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $d < q_{i+1}$ die Ungleichung*

$$|q_i\alpha - p_i| \leq |d\alpha - c|$$

*mit Gleichheit genau für $c = p_i$ und $d = q_i$*

*Bemerkung* 8. **ad 2:** In diesem Fall ist (wegen $q_k > 1$) $k \geq 1$ und aus (1.7) folgt

$$q_k = \underbrace{a_k}_{\geq 2} q_{k-1} + q_{k-2} \geq 2q_{k-1}$$

Setzt man nun $(c, d) := (p_{k-1}, q_{k-1})$ oder davon verschieden $(c, d) := (p_k - p_{k-1}, q_k - q_{k-1})$, so gilt in beiden Fällen die Bedingung $0 < d < q_k$.

Dass in beiden Fällen in der Ungleichung dann Gleichheit auftritt, ist wegen $q_k\alpha = p_k$ evident.

**ad 3:** Der Fall, dass $\alpha \in \mathbb{Q}$ kann offensichtlich nur bei $k \geq 2$ auftreten.
Außerdem gilt für $i \geq 0$ immer $q_i \leq q_{i+1}$ mit Gleichheit genau für $i = 0$ und $a_1 = 1$, was in 3. aber explizit ausgeschlossen ist. Also ist in 3. immer $q_i < q_{i+1}$ und so kommt hier $(p_i, q_i)$ unter den zugelassenen Paaren $(c, d)$ vor.

*Beweis.* (des Lemmas)

1. ist trivial.

   Zum Beweis von 2 und 3 geht man wie folgt vor:
   Betrachte das lineare Gleichungssystem:

$$\begin{aligned} p_iX + p_{i+1}Y &= c \\ q_iX + q_{i+1}Y &= d \end{aligned} \tag{1.23}$$

   Die Koeffizientenmatrix hat nach (1.8) die Determinante $(-1)^{i+1}$ und das Gleichungssystem besitzt daher eine Lösung $(x, y) \in \mathbb{Z}^2$.
   Dabei ist $x \neq 0$, weil sonst aus der zweiten Gleichung $q_{i+1}|d$ folgen würde, entgegen den Voraussetzungen $d < q_{i+1}$ in 2. (hier mit $i := k - 1$) und 3.

2. Setzt man in (1.23) $i := k - 1$, so erhält man nach Multiplikation der zweiten Gleichung mit $\alpha$ und anschließender Subtraktion der ersten Gleichung:

$$x(q_{k-1}\alpha - p_{k-1}) = d\alpha - c$$

   Bei $|x| \geq 2$ erhält man wegen $\frac{p_{k-1}}{q_{k-1}} \neq \alpha$ die gewünschte Ungleichung $|d\alpha - c| > |q_{k-1}\alpha - p_{k-1}|$ in 2.
   Andererseits ist $|x| = 1$ äquivalent zu

$$cq_k - dp_k = \varepsilon \qquad \text{mit einem} \quad \varepsilon \in \{1, -1\} \tag{1.24}$$

   Das sieht man durch Elimination von $y$ in (1.23) und unter Beachtung von (1.8).
   Die lineare diophantische Gleichung (1.24) mit den Unbekannten $c$ und $d$ ist

lösbar und hat die Lösungsmenge

$$(\varepsilon c_0 + tp_k, \varepsilon d_0 + tq_k) \qquad t \in \mathbb{Z}$$

wobei $(c_0, d_0) \in \mathbb{Z}^2$ eine spezielle Lösung von $cq_k - dp_k = 1$ ist, zum Beispiel $c_0 = (-1)^k p_{k-1}$ und $d_0 = (-1)^k q_{k-1}$. Hierbei wurde auch beachtet, dass $p_k q_k \neq 0$: Dass $q_k > 0$ ist klar, weil $k \geq 1$. Indirekt angenommen es wäre $p_k = 0$. Dann wäre wegen (1.24) $q_k = 1$, also $k = 1$. Somit nach (1.7) $a_1 = 1$, was nicht geht, da das letzte Element eines Kettenbruchs einer rationalen, nicht ganzen Zahl größer als 1 sein muss.
Die Gleichung $|d\alpha - c| = |q_{k-1}\alpha - p_{k-1}|$ tritt also genau für die Paare $(c, d)$ der Gestalt

$$c = \varepsilon' p_{k-1} + tp_k \qquad\qquad d = \varepsilon' q_{k-1} + tq_k$$

auf, wobei $\varepsilon' \in \{1, -1\}$ und $t \in \mathbb{Z}$ so zu wählen sind, dass $0 < d < q_k$ gilt. Das ist erfüllt, wenn entweder $t = 0$ und $\varepsilon' = 1$ oder $t = 1$ und $\varepsilon' = -1$. Das sind genau die in 2. genannten Fälle für Gleichheit.

3. Für Paare $(c, d)$ der Form $(\lambda p_i, \lambda q_i)$ mit $\lambda = 2, 3, 4, \ldots$ ist wegen $q_i \neq \alpha p_i$ (wobei $i \leq k - 2$ im endlichen Fall) die strenge Ungleichung klar.
Sei jetzt also $(c, d)$ von allen $(\lambda p_i, \lambda q_i)$ verschieden ($\lambda = 1, 2, 3, \ldots$), das heißt $\frac{c}{d} \neq \frac{q_i}{p_i}$.
Dann gilt für die Lösung $(x, y)$ von (1.23), dass $xy < 0$:
Denn $y = 0$ würde zu $\frac{p_i}{q_i} = \frac{c}{d}$ führen. Wäre andererseits $xy > 0$, also $x, y > 0$ oder $x, y < 0$, würde das wegen $0 < d < q_{i+1}$ der zweiten Gleichung in (1.23) widersprechen.

Nach (1.14) haben auch $q_i\alpha - p_i$ und $q_{i+1}\alpha - p_{i+1}$ verschiedenes Vorzeichen und verschwinden beide auch im Fall $\alpha \in \mathbb{Q}$ nicht, da $i < k - 2$.
Daher haben die Ausdrücke $x(q_i\alpha - p_i)$ und $y(q_{i+1}\alpha - p_{i+1})$ gleiches Vorzeichen.
Aus den Gleichungen (1.23) folgt dann:

$$\begin{aligned} |d\alpha - c| &= |x(q_i\alpha - p_i) + y(q_{i+1}\alpha - p_{i+1})| \\ &= \underbrace{|x|}_{\geq 1} \cdot |q_i\alpha - p_i| + \underbrace{|y|}_{\geq 1} \cdot \underbrace{|q_{i+1}\alpha - p_{i+1}|}_{>0} \\ &> |q_i\alpha - p_i| \end{aligned}$$

□

**Definition 5.** Eine rationale Zahl $\frac{a}{b}$ mit $a \in \mathbb{Z},\ b \in \mathbb{N}$ heißt eine *beste Näherung* für $\alpha \in \mathbb{R}$, wenn für alle $c \in \mathbb{Z},\ d \in \mathbb{N}$ mit $\frac{c}{d} \neq \frac{a}{b}$ und $d \leq b$ gilt:

$$|d\alpha - c| > |b\alpha - a|$$

.

**Satz 6.** *Jede beste Näherung $\frac{a}{b}$ für $\alpha$ ist ein Näherungsbruch von $\alpha$.*

*Beweis.* Indirekt angenommen, es sei $\frac{a}{b} \neq \frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_k}{q_k}, \ldots$, wobei im Fall $\alpha \in \mathbb{Q}$ die Folge wieder mit $\frac{p_k}{q_k}$ abbrechen möge.

**1. Fall:** Sei $\alpha \in \mathbb{Q}$ und $q_k \leq b$.

Dann wähle $c := p_k$ und $d := q_k$. Dann hat man $\frac{c}{d} \neq \frac{a}{b}$, $d \leq b$ und

$$0 = |q_k\alpha - p_k| = |d\alpha - c| < |b\alpha - a|$$

also ist $\frac{a}{b}$ keine beste Näherung für $\alpha$.

**2. Fall:** Entweder $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ oder es ist $\alpha \in \mathbb{Q}$ und $b < q_k$.

Fixiere $i$, sodass $q_i \leq b < q_{i+1}$ und erhalte:
$i < k$ und $1 < q_{i+1} \overset{(1.7)}{=} a_{i+1}q_i + q_{i-1}$, also ist entweder $i \geq 1$ oder aber $i = 0$ und $a_1 > 1$. Jetzt kann Lemma 5 verwendet werden, sodass

$$|q_i\alpha - p_i| \leq |b\alpha - a|.$$

Wenn man jetzt $c := p_i$ und $d := q_i$ wählt, dann ist $\frac{c}{d} \neq \frac{a}{b}$, $d \leq b$ und es gilt:

$$|d\alpha - c| \leq |b\alpha - a|$$

Also ist $\frac{a}{b}$ keine beste Näherung für $\alpha$.

□

Wie bereits angedeutet, gilt die Umkehrung des Satzes 6 mit wenigen Ausnahmen:

**Satz 7.** *Jeder Näherungsbruch von $\alpha \in \mathbb{R}$ ist eine beste Näherung für $\alpha$, wenn man für die $\alpha$ der Form $[a_0; 2]$, $[a_0; 1, a_2, \ldots, a_k]$ mit einem $k \geq 2$ und $[a_0; 1, a_2, a_3, \ldots]$ von den Näherungsbrüchen nullter Ordnung absieht.*
*Für diese Ausnahmen ist der nullte Näherungsbruch tatsächlich keine beste Näherung für $\alpha$.*

*Beweis.* Ist $\frac{p_i}{q_i}$ ein Näherungsbruch für $\alpha$ (mit $i \geq 1$ in den genannten Ausnahmefällen), dann ist für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $\frac{c}{d} \neq \frac{p_i}{q_i}$, $d \leq q_i$ die Ungleichung

$$|d\alpha - c| > |q_i\alpha - p_i|$$

zu zeigen.

Ist $\alpha \in \mathbb{Q}$ und $i = k$, dann folgt die Aussage aus Punkt 1 in Lemma 5.
Im Fall $\alpha \in \mathbb{Q}$ ist das gleichzeitige Auftreten von $k = 1$ und $a_k = 2$ in den Voraussetzungen des Satzes als Sonderfall ausgeschlossen. Daher ist $q_k - q_{k-1} > q_{k-1}$ und so gilt das gewünschte Resultat nach Punkt 2 von Lemma 5.
In den Fällen $\alpha \in \mathbb{Q}$, $0 \leq i \leq k-2$ beziehungsweise $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, $i \geq 0$ ist die Möglichkeit, dass gleichzeitig $i = 0$ und $a_1 = 1$ gilt, in den Voraussetzungen des Satzes als Spezialfall ausgeschlossen. Daher sind die Voraussetzungen für Punkt 3 von Lemma 5 erfüllt, was das gewünschte Resultat ergibt.

Betrachte abschließend die Spezialfälle:
Für den ersten Ausnahmefall $\alpha = a_0 + \frac{1}{2}$ ist $p_0 = a_0$, $q_0 = 1$, $p_1 = 2a_0 + 1$, $q_1 = 2$, daher

$$|q_0\alpha - p_0| = |(q_1 - q_0)\alpha - \underbrace{(p_1 - p_0)}_{\neq p_0}| \qquad \left(= \frac{1}{2}\right)$$

also ist hier $\frac{p_0}{q_0}$ keine beste Näherung für $\alpha$.
Im zweiten und dritten Ausnahmefall gilt für $\alpha \notin \mathbb{Q}$ beziehungsweise $\alpha \in \mathbb{Q}$ und $k \geq 3$:

$$\alpha - a_0 \overset{(1.12)}{>} \frac{p_2}{q_2} - a_0 = \left(1 + \frac{1}{a_2}\right)^{-1} \geq \frac{1}{2}$$

Weiters gilt für $\alpha \in \mathbb{Q}$ und $k = 2$:

$$\alpha - a_0 = \frac{p_2}{q_2} - a_0 = \left(1 + \frac{1}{a_2}\right)^{-1} \geq \frac{2}{3}$$

weil $a_2 \geq 2$. Insgesamt ist also im zweiten und dritten Ausnahmefall jedenfalls

$$\alpha - a_0 > \frac{1}{2},$$

oder anders geschrieben

$$\alpha - a_0 > (a_0 + 1) - \alpha \qquad (> 0)$$

Übergang zum Betrag zeigt, dass $\frac{p_0}{q_0}(=\frac{a_0}{1})$ wieder keine beste Näherung für $\alpha$ ist. □

**Definition 6.** Für $\alpha \in \mathbb{R}$ definiere $\|\alpha\|$ als den Abstand zur nächstgelegenen ganzen Zahl, also

$$\|\alpha\| := \min(\{\alpha\}, 1 - \{\alpha\}).$$

**Proposition 2.** *Für jedes reelle $\alpha$ gilt:*

$$\|q_0\alpha\| \geq \|q_1\alpha\| > \ldots > \|q_k\alpha\| > \ldots$$

*wobei im Fall, dass $\alpha = \frac{p_k}{q_k} \in \mathbb{Q}$ die Ungleichungskette mit $\|q_k\alpha\| = 0$ abbricht.*
*In der ersten Ungleichung tritt genau dann Gleichheit auf, wenn das Kettenbruchelement $a_1$ von $\alpha$ gleich 1 ist, was im Fall $\alpha \in \mathbb{Q}$ nur bei $k \geq 2$ eintreten kann.*

*Beweis.* Sei $\alpha \notin \mathbb{Z}$ (für ganze $\alpha$ ist die Aussage trivial), also etwa $\alpha = [a_0; a_1, \ldots, a_k, \ldots]$ mit $k \geq 1$ für rationale $\alpha$.
Nach dem letzten Satz ist $\frac{p_i}{q_i}$ für $i \geq 1$ eine beste Näherung für $\alpha$ und deshalb gilt, wegen $q_{i-1} \leq q_i$ und $\frac{p_{i-1}}{q_{i-1}} \neq \frac{p_i}{q_i}$ die Abschätzung

$$|q_{i-1}\alpha - p_{i-1}| > |q_i\alpha - p_i| \qquad \text{für } i \geq 1.$$

Ebenso sieht man, dass $|q_0\alpha - (p_0+1)| \geq |q_1\alpha - p_1|$, mit Gleichheit genau dann, wenn $a_1 = 1$. Das liefert

$$\min(|q_0\alpha - p_0|, |q_0\alpha - (p_0+1)|) \geq |q_1\alpha - p_1| > \ldots > |q_k\alpha - p_k| > \ldots \tag{1.25}$$

wobei die Ungleichungskette im Fall eines rationalen $\alpha$ mit $|q_k\alpha - p_k| = 0$ abbricht. Nach (1.21) gilt

$$|q_i\alpha - p_i| = \frac{1}{q_i\alpha_{i+1} + q_{i-1}} \leq \frac{1}{\alpha_{i+1}+1} < \frac{1}{2} \qquad \text{für } i \geq 1$$

wobei $i < k$ im rationalen Fall erfüllt sein muss.
Daraus folgt, dass für $i \geq 1$ immer $\|q_i\alpha\| = |q_i\alpha - p_i|$ gilt. Das Minimum im ersten Glied von (1.25) ist gleich $\|q_0\alpha\|$, daraus folgt die Behauptung. □

*Bemerkung* 9. Wenn $\frac{a}{b}$ eine beste Näherung für $\alpha \in \mathbb{R}$ ist, dann ist nach der Definition

$$\left|\alpha - \frac{a}{b}\right| = \frac{1}{b}\left|b\alpha - a\right| < \frac{1}{b}\left|d\alpha - c\right| = \underbrace{\frac{d}{b}}_{\leq 1} \cdot \left|\alpha - \frac{c}{d}\right| \leq \left|\alpha - \frac{c}{d}\right|$$

für alle rationalen $\frac{c}{d} \neq \frac{a}{b}$ mit $d \leq b$. Die Umkehrung gilt allerdings nicht. Das liefert die Erklärung für die Beziehung zwischen den verschiedenen Arten der Abschätzung, die am Beginn dieses Abschnitts angekündigt wurde.
Die letzten Resultate besagen also, dass wenn man $\alpha \in \mathbb{R}$ durch seinen $i$-ten Näherungsbruch ersetzt ($i \geq 1$), dann ist der Fehler absolut kleiner, als wenn man $\alpha$ durch irgendeine andere rationale Zahle, deren Nenner $q_i$ nicht übersteigt, ersetzt.

## 1.3 Kontinuanten

**Definition 7.** Es seien $a_1, \ldots, a_n \in \mathbb{N}$. Die Kontinuante $K_n(a_1, \ldots, a_n)$ ist definiert als die Determinante

$$K_n(a_1, \ldots, a_n) := \begin{vmatrix} a_1 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & -1 & a_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_{n-1} & 1 \\ & & & & -1 & a_n \end{vmatrix}$$

wobei alle Eintragungen abseits der Hauptdiagonale, sowie der ersten oberen und ersten unteren Nebendiagonale 0 sind.
Zusätzlich setzt man $K_0 := 1$ und $K_{-1} := 0$.

*Bemerkung* 10. Die grundlegenden Tatsachen über Kontinuanten findet man in [11].

Die folgende Proposition wird den Zusammenhang zwischen Kontinuanten und Kettenbrüchen erklären.

**Proposition 3.** *Es sei der endliche Kettenbruch*

$$[a_0; a_1, \ldots, a_m] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}}}$$

*gegeben und $p_m$, $q_m$ aus (1.7) berechnet, also $\frac{p_m}{q_m} = [a_0; a_1, \ldots, a_m]$.*
*Dann gilt: $q_m = K_m(a_1, \ldots, a_m)$.*

*Beweis.* Aus (1.7) erhält man für $0 \leq k < m$:

$$q_{k+1} = a_{k+1}q_k + q_{k-1}$$

mit den Startwerten $q_{-1} = 0$ und $q_0 = 1$. Daraus erhält man das lineare Gleichungssytem:

$$\begin{aligned} q_0 &= 1 \\ a_1q_0 - q_1 &= 0 \\ q_0 + a_2q_1 - q_2 &= 0 \\ q_1 + a_3q_2 - q_3 &= 0 \\ &\vdots \\ q_{m-2} + a_mq_{m-1} - q_m &= 0 \end{aligned}$$

Das System kann man auch als Matrizengleichung schreiben:

$$\begin{pmatrix} 1 & & & & & \\ a_1 & -1 & & & & \\ 1 & a_2 & -1 & & & \\ & 1 & a_3 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & a_m & -1 \end{pmatrix} \cdot \begin{pmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ \vdots \\ q_m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Es soll nun $q_m$ mit Hilfe der Cramer'schen Regel berechnet werden. Es gilt

$$\begin{vmatrix} 1 & & & & & \\ a_1 & -1 & & & & \\ 1 & a_2 & -1 & & & \\ & 1 & a_3 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & a_m & -1 \end{vmatrix} = (-1)^m.$$

Daraus erhält man:

$$q_m = (-1)^m \begin{vmatrix} 1 & & & & & & 1 \\ a_1 & -1 & & & & & 0 \\ 1 & a_2 & -1 & & & & 0 \\ & 1 & a_3 & -1 & & & 0 \\ & & \ddots & \ddots & \ddots & & \vdots \\ & & & 1 & a_{m-1} & -1 & 0 \\ & & & & 1 & a_m & 0 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 1 & & & & & \\ 0 & a_1 & -1 & & & & \\ 0 & 1 & a_2 & -1 & & & \\ \vdots & & 1 & a_3 & -1 & & \\ \vdots & & & \ddots & \ddots & \ddots & \\ \vdots & & & & 1 & a_{m-1} & -1 \\ 0 & & & & & 1 & a_m \end{vmatrix} = \begin{vmatrix} a_1 & -1 & & & & \\ 1 & a_2 & -1 & & & \\ & 1 & a_3 & -1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & a_{m-1} & -1 \\ & & & & 1 & a_m \end{vmatrix}$$

$$\overset{\text{Transponieren}}{=} \begin{vmatrix} a_1 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & -1 & a_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_{m-1} & 1 \\ & & & & -1 & a_m \end{vmatrix} = K_m(a_1, \ldots, a_m)$$

□

*Bemerkung* 11. Aus der Proposition folgt, dass $K_m(a_1, \ldots, a_m) \in \mathbb{N}$ für $m \geq 0$. Das kann man auch durch direktes Berechnen der Determinante sehen.

Im nächsten Lemma werden ein paar nützliche Eigenschaften von Kontinuanten bewiesen:

**Lemma 6.** *1. Es gilt stets:*

$$K_m(a_1, a_2, \ldots, a_{m-1}, a_m) = K_m(a_m, a_{m-1}, \ldots, a_2, a_1) \tag{1.26}$$

2. *Wenn $a_m \geq 2$, dann gilt*

$$K_m(a_1, \ldots, a_m) = K_{m+1}(a_1, \ldots, a_{m-1}, a_m - 1, 1) \tag{1.27}$$

3. *Für $0 \leq m \leq n$ gilt:*

$$\begin{aligned} K_n(a_1, \ldots, a_n) = {} & K_m(a_1, \ldots, a_m) K_{n-m}(a_{m+1}, \ldots, a_n) \\ & + K_{m-1}(a_1, \ldots, a_{m-1}) K_{n-m-1}(a_{m+2}, \ldots, a_n) \end{aligned} \tag{1.28}$$

*Beweis.* 1. Sei $\sigma \in S_m$ die Permutation $\sigma = \begin{pmatrix} 1 & 2 & \ldots & m-1 & m \\ m & m-1 & \ldots & 2 & 1 \end{pmatrix}$. Dann ist

$$\begin{aligned} & K_m(a_1, \ldots, a_m) \\ & = \begin{vmatrix} a_1 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & -1 & a_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_{m-1} & 1 \\ & & & & -1 & a_m \end{vmatrix} = \operatorname{sgn}\sigma \cdot \begin{vmatrix} & & & & 1 & a_1 \\ & & & 1 & a_2 & -1 \\ & & \iddots & \iddots & \iddots & \\ 1 & a_{m-1} & -1 & & & \\ a_m & -1 & & & & \end{vmatrix} \\ & \overset{\text{Transponieren}}{=} \operatorname{sgn}\sigma \cdot \begin{vmatrix} & & & & 1 & a_m \\ & & & 1 & a_{m-1} & -1 \\ & & 1 & a_{m-2} & -1 & \\ & \iddots & \iddots & \iddots & & \\ 1 & a_2 & -1 & & & \\ a_1 & -1 & & & & \end{vmatrix} \\ & = \underbrace{(\operatorname{sgn}\sigma)^2}_{=1} \cdot \begin{vmatrix} a_m & 1 & & & & \\ -1 & a_{m-1} & 1 & & & \\ & -1 & a_{m-2} & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_2 & 1 \\ & & & & -1 & a_1 \end{vmatrix} = K_m(a_m, \ldots, a_1) \end{aligned}$$

2. Da für Kettenbrüche gilt $[a_0; a_1, \ldots, a_m] = [a_0; a_1 \ldots, a_{m-1}, a_m - 1, 1]$, folgt das Ergebnis auch für Kontinuanten aus Proposition 3.

3. Zeige die Behauptung mit Induktion nach $n - m$:

- $n - m = 0$:

$$\begin{aligned} K_n(a_1, \dots a_n) &= K_n(a_1, \dots a_n) \cdot 1 + K_{n-1}(a_1, \dots, a_{n-1}) \cdot 0 \\ &= K_n(a_1, \dots a_n) \cdot K_0 + K_{n-1}(a_1, \dots, a_{n-1}) \cdot K_{-1} \end{aligned}$$

- $n - m = 1$ :
  Entwicklung der Determinante nach der letzten Zeile ergibt:

$$\begin{aligned} &K_n(a_1, \dots a_n) \\ &= \begin{vmatrix} a_1 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & -1 & a_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_{n-1} & 1 \\ & & & & -1 & a_n \end{vmatrix} = \underbrace{a_n}_{=K_1(a_n)} \cdot \begin{vmatrix} a_1 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & -1 & a_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_{n-2} & 1 \\ & & & & -1 & a_{n-1} \end{vmatrix} \\ &\qquad + (-1) \cdot (-1) \begin{vmatrix} a_1 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & \ddots & \ddots & \ddots & & \\ & & -1 & a_{n-3} & 1 & \\ & & & -1 & a_{n-2} & 0 \\ & & & & -1 & 1 \end{vmatrix} \\ &\qquad = K_1(a_n) \cdot K_{n-1}(a_1, \dots, a_{n-1}) + K_0 \cdot K_{n-2}(a_1, \dots, a_{n-2}) \end{aligned}$$

- Sei nun $n - m \geq 2$.

$$\begin{aligned} &K_n(a_1, \dots, a_n) = a_n K_{n-1}(a_1, \dots, a_{n-1}) + K_{n-2}(a_1, \dots, a_{n-2}) \\ &\overset{\text{Induktionsvoraussetzung}}{=} a_n(K_m(a_1, \dots, a_m) K_{n-m-1}(a_{m+1}, \dots, a_{n-1}) \\ &+ K_{m-1}(a_1, \dots, a_{m-1}) K_{n-m-2}(a_{m+2}, \dots, a_{n-1})) + K_m(a_1, \dots, a_m) \\ &\times K_{n-m-2}(a_{m+1}, \dots, a_{n-2}) + K_{m-1}(a_1, \dots, a_{m-1}) K_{n-m-3}(a_{m+2}, \dots, a_{n-2}) \\ &= K_m(a_1, \dots, a_m) \cdot (a_n K_{n-m-1}(a_{m+1}, \dots, a_{n-1}) + K_{n-m-2}(a_{m+1}, \dots, a_{n-2})) \end{aligned}$$

$$
\begin{aligned}
&+ K_{m-1}(a_1, \ldots, a_{m-1}) \cdot (a_n K_{n-m-2}(a_{m+2}, \ldots, a_{n-1}) \\
&+ K_{n-m-3}(a_{m+2}, \ldots, a_{n-2})) \\
&\overset{\text{Induktionsvoraussetzung}}{=} K_m(a_1, \ldots, a_m) K_{n-m}(a_{m+1}, \ldots, a_n) \\
&+ K_{m-1}(a_1, \ldots, a_{m-1}) K_{n-m-1}(a_{m+2}, \ldots, a_n)
\end{aligned}
$$

□

*Bemerkung* 12. Die Formel (1.28) wird bei O. Perron [11, S. 11] aufgrund ihrer Wichtigkeit als „Fundamentalformeln" bezeichnet. Perron beweist dort das entsprechende Resultat für Kontinuanten, die aus allgemeinen (also nicht notwendig regelmäßigen) Kettenbrüchen abgeleitet werden. Man erhält dadurch zwei äquivalente Formeln, daher der Plural in „Fundamentalformeln".

*Bemerkung* 13. Die „Fundamentalformel" (1.28) enthält als Spezialfall $n = m + 1$ die Rekursionsrelation zur Bildung der $q_i$, vergleiche (1.7):

$$q_{m+1} = a_{m+1} q_m + q_{m-1}$$

In der Definition der Kontinuante darf keines der $a_i$ gleich 0 sein. Später wird es aber nützlich sein, in gewissen Fällen $a_i = 0$ zuzulassen. Betrachte also die Determinante aus der Definition der Kontinuante und setze ein $a_i$ gleich 0.
Dann folgt das Ergebnis:

**Proposition 4.** *Für $n \in \mathbb{N}$ gilt:*

*1.*

$$
\begin{vmatrix}
a_1 & 1 & & & & \\
-1 & a_2 & 1 & & & \\
 & -1 & a_3 & 1 & & \\
 & & \ddots & \ddots & \ddots & \\
 & & & -1 & a_{n-1} & 1 \\
 & & & & -1 & 0
\end{vmatrix}
=: K_n(a_1, \ldots, a_{n-1}, 0) = K_{n-2}(a_1, \ldots, a_{n-2}) \tag{1.29}
$$

*und*

$$\begin{vmatrix} 0 & 1 & & & & \\ -1 & a_2 & 1 & & & \\ & -1 & a_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & -1 & a_{n-1} & 1 \\ & & & & -1 & a_n \end{vmatrix} =: K_n(0, a_2, \ldots, a_n) = K_{n-2}(a_3, \ldots, a_n)$$

*2. Für $1 < m < n$ gilt:*

$$\begin{aligned} &\begin{vmatrix} a_1 & 1 & & & & & & & \\ -1 & a_2 & 1 & & & & & & \\ & \ddots & \ddots & \ddots & & & & & \\ & & -1 & a_{m-1} & 1 & & & & \\ & & & -1 & 0 & 1 & & & \\ & & & & -1 & a_{m+1} & 1 & & \\ & & & & & \ddots & \ddots & \ddots & \\ & & & & & & -1 & a_{n-1} & 1 \\ & & & & & & & -1 & a_n \end{vmatrix} \\ &=: K_n(a_1, \ldots, a_{m-1}, 0, a_{m+1}, \ldots, a_n) \\ &= K_{n-2}(a_1, \ldots, a_{m-2}, a_{m-1} + a_{m+1}, a_{m+2}, \ldots, a_n) \end{aligned} \tag{1.30}$$

*Beweis.* 1. Die erste Aussage folgt einfach durch Entwicklung der Determinante nach der letzten Zeile.
Die zweite Aussage wird vollkommen analog gezeigt.

2. Da man im Beweis von (1.28) vom vorigen Lemma nur allgemeine Eigenschaften von Determinanten benutzt hat, insbesondere also nicht verwendet hat, dass alle Einträge auf der Hauptdiagonale natürliche Zahlen sind, kann man die Aussage auch für Kontinuanten, bei denen ein $a_i = 0$ ist, verwenden.
Wende also die Gleichung (1.28) für $K(\ldots, x, 0, y, \ldots)$ an, für die linke Seite der

zu beweisenden Gleichung:

$$\begin{aligned}
&K_n(a_1,\dots,a_{m-1},0,a_{m+1},\dots,a_n)\\
&\quad= K_m(a_1,\dots,a_{m-1},0)K_{n-m}(a_{m+1},\dots,a_n)\\
&\qquad+ K_{m-1}(a_1,\dots,a_{m-1})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\quad\overset{(1.29)}{=} K_{m-2}(a_1,\dots,a_{m-2})K_{n-m}(a_{m+1},\dots,a_n)\\
&\qquad+ K_{m-1}(a_1,\dots,a_{m-1})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\quad\overset{(1.28)}{=} K_{m-2}(a_1,\dots,a_{m-2})\cdot(a_{m+1}K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\qquad+ K_{n-m-2}(a_{m+3},\dots,a_n))+(a_{m-1}K_{m-2}(a_1,\dots,a_{m-2})\\
&\qquad+ K_{m-3}(a_1,\dots,a_{m-3}))\cdot K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\quad= a_{m+1}K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\qquad+ K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-2}(a_{m+3},\dots,a_n))\\
&\qquad+ a_{m-1}K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\qquad+ K_{m-3}(a_1,\dots,a_{m-3})K_{n-m-1}(a_{m+2},\dots,a_n)
\end{aligned}$$

Andererseits ergibt die Berechnung der Kontinuante auf der rechten Seite der Gleichung:

$$\begin{aligned}
&K_{n-2}(a_1,\dots,a_{m-2},a_{m-1}+a_{m+1},a_{m+2},\dots,a_n)\\
&\quad\overset{(1.28)}{=} K_{m-1}(a_1,\dots,a_{m-2},a_{m-1}+a_{m+1})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\quad+ K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-2}(a_{m+3},\dots,a_n)\\
&\quad\overset{(1.28)}{=} ((a_{m+1}+a_{m-1})K_{m-2}(a_1,\dots,a_{m-2})+K_{m-3}(a_1,\dots,a_{m-3}))\\
&\quad\times K_{n-m-1}(a_{m+2},\dots,a_n)+K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-2}(a_{m+3},\dots,a_n))\\
&\quad= (a_{m+1}+a_{m-1})K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\quad+ K_{m-3}(a_1,\dots,a_{m-3})K_{n-m-1}(a_{m+2},\dots,a_n)\\
&\quad+ K_{m-2}(a_1,\dots,a_{m-2})K_{n-m-2}(a_{m+3},\dots,a_n)
\end{aligned}$$

Also stimmen beide Seiten überein.

□

**Proposition 5.** *Wenn* $\frac{p_n}{q_n}=[a_0;a_1,\dots,a_n]$. *Dann gilt für* $1\le i\le n$*:*

$$\frac{q_{i-1}}{q_i}=[0;a_i,a_{i-1}\dots,a_1]$$

*Insbesondere gilt für $i = n$:*

$$\frac{K_{n-1}(a_1, \ldots, a_{n-1})}{K_n(a_1, \ldots, a_n)} = [0; a_n, \ldots, a_1] \tag{1.31}$$

*Beweis.* Induktion nach $i$.
Für $i = 1$ gilt $\frac{q_0}{q_1} = \frac{1}{a_1} = [0; a_1]$.
Sei die Behauptung für $i - 1$ richtig. Dann berechne

$$\frac{q_{i-1}}{q_i} \overset{(1.7)}{=} \frac{q_{i-1}}{a_i q_{i-1} + q_{i-2}} = \frac{1}{a_i + \dfrac{q_{i-2}}{q_{i-1}}}$$

$$\overset{\text{Induktionsvoraussetzung}}{=} \cfrac{1}{a_i + \cfrac{1}{a_{i-1} + \cfrac{1}{a_{i-2} + \cfrac{1}{\ddots + \cfrac{1}{a_1}}}}} = [0; a_i, \ldots, a_1]$$

□

# 2 Vermutung von Zaremba

## 2.1 Formulierung für Kettenbrüche

**Vermutung 1** (Zaremba [15])**.** *Es gibt eine natürliche Zahl $b$ mit der Eigenschaft, dass es für alle natürlichen Zahlen $m$ ein ganzes $a$ mit $0 < a < m$ und $\mathrm{ggT}(a, m) = 1$ gibt, sodass die Kettenbruchentwicklung*

$$\frac{a}{m} = [0; a_1, \ldots, a_n]$$

*die folgende Eigenschaft hat: $a_i \leq b$ für $1 \leq i \leq n$.*

*Bemerkung* 14. Numerische Auswertungen legen folgende Präzisierungen der Vermutung nahe:

- Die Vermutung von Zaremba ist mit $b = 5$ erfüllt.
- Für hinreichend große $m$ ist die Vermutung mit $b = 3$ erfüllt.

Die ersten derartigen numerischen Experimente wurden von I. Borosh in den 70er Jahren des 20. Jahrhunderts durchgeführt, allerdings nie publiziert. Die einzigen beiden $m$, für die die Schranke $b = 5$ erreicht wird, die dabei gefunden wurden, sind 54 und 150. Weiters wurden 25 Zahlen gefunden, für die $b = 4$ erreicht wird. Die größte dieser Zahlen ist 6234.

*Beispiel* 2. Wenn $m = F_k$ eine Fibonacci-Zahl ist (wir verwenden als Definition der Fibonacci-Zahlen: $F_0 := 0,\ F_1 := 1,\ F_{n+2} := F_{n+1} + F_n$ für $n \geq 0$), ist die Vermutung für $m$ erfüllt. Man kann dann nämlich $a$ als die $(k-1)$-te Fibonacci-Zahl wählen.
Es gilt dann $\mathrm{ggT}(F_{k-1}, F_k) = 1$ und aus dem Euklidischen Algorithmus für $F_{k-1}$ und $F_k$ liest man die Kettenbruchentwicklung

$$\frac{F_{k-1}}{F_k} = [0; \underbrace{1, 1, \ldots, 1}_{k-3}, 2] \quad \text{für } k \geq 3$$

ab.

*Bemerkung* 15. Die Bedingung $a < m$ in der Vermutung ist keine wirkliche Einschränkung, da nur $a_1, \ldots, a_n$ betrachtet werden. Wenn man etwa für ein $m$ ein $a > m$ gefunden hat, sodass $\mathrm{ggT}(a, m) = 1$ und die Bedingung für $a_i$ $(1 \leq i \leq n)$ gilt, dann gilt die Vermutung auch für das $a'$ mit $0 < a' < m$ und $a' \equiv a \pmod{m}$.

## 2.2 Formulierung für Kontinuanten

**Vermutung 2.** *Es gibt eine natürliche Zahl $b$ mit der folgenden Eigenschaft: Für jede natürliche Zahl $m$ gibt es natürliche Zahlen $a_1, \ldots, a_n \leq b$, derart dass*

$$m = K_n(a_1, \ldots, a_n).$$

*Bemerkung* 16. Diese Formulierung der Vermutung ist äquivalent zur Formulierung für Kettenbrüche. Denn für ein $a$ mit $\mathrm{ggT}(a, m) = 1$ ist die Bedingung $a_i \leq b$ für $\frac{a}{m} = \frac{p_n}{q_n} = [0; a_1, \ldots a_n]$ in Vermutung 1 genau dann erfüllt, wenn sie auch für

$$[0; a_n, \ldots, a_1] = \frac{q_{n-1}}{q_n} = \frac{K_{n-1}(a_1, \ldots, a_{n-1})}{K_n(a_1, \ldots, a_n)}$$

in Vermutung 2 erfüllt ist.
Statt $K_{n-1}(a_1, \ldots a_{n-1})$ kann hier auch $K_{n-1}(a_2, \ldots, a_n)$ als Zähler gewählt werden.

Hier stört es nicht, $a_n = 1$ oder $a_1 = 1$ auch im entsprechenden Kettenbruch zuzulassen; dabei bleibt $a_i \leq b$ klarerweise aufrecht, eventuell kann dann $b$ sogar kleiner gewählt werden.

**Definition 8.** Es sei $k \in \mathbb{N}$. Dann definiere:

$$S_k := \{m \in \mathbb{N} : m = K_n(a_1, \ldots a_n) \quad \text{für gewisse } a_1, \ldots, a_n \leq k\}$$

*Bemerkung* 17.

- Die Vermutung 2 besagt also: Es gibt eine natürliche Zahl $b$, sodass $\mathbb{N} = S_b$
- Das Beispiel 2 zusammen mit (1.27) besagt, dass $\{F_n |\ n \in \mathbb{N}\} \subseteq S_1$. Aus $K_{-1} = F_0,\ K_0 = F_1$ und

  $$K_{n+2}(1, 1, \ldots, 1) = K_{n+1}(1, 1, \ldots, 1) + K_n(1, 1, \ldots, 1)$$

  für $n \geq 0$ folgt $\{F_n |\ n \in \mathbb{N}\} = S_1$.

- Genau wie bei Vermutung 1 wird auch bei Vermutung 2 der Wert $b = 5$ als möglicher Minimalwert für $b$ angenommen, sowie $b = 3$ für hinreichend große $m$.

## 2.3 Ursprung der Vermutung

Die Vermutung 1 tauchte erstmals in einem Gebiet auf, das nicht in erster Linie mit zahlentheoretischen Fragestellungen in Verbindung zu stehen scheint: Nämlich bei einer gewissen Methode zur numerischen Integration einer mehrdimensionalen Funktion.

In diesem Abschnitt sollen die Problemstellung und die historische Entwicklung der Lösungsmethoden, die zur Vermutung 1 führten, vorgestellt werden.

### 2.3.1 Problemstellung

In diesem Abschnitt folgen wir im Wesentlichen [5].

Es sei eine Riemann-integrierbare Funktion $f : \underbrace{Q^s}_{\subseteq \mathbb{R}^s} \to \mathbb{R}$ gegeben, wobei

$$Q^s := \{\mathbf{x} = (x_1, \ldots, x_s) : \ a_j \leq x_j \leq b_j \quad (1 \leq j \leq s)\}$$

ein Quader in $\mathbb{R}^s$ sei ($\mathbf{x}$ möge immer einen Punkt in $\mathbb{R}^s$ bezeichnen).
Es soll das Integral $\int_{Q^s} f(\mathbf{x})\, d\mathbf{x}$ numerisch angenähert werden.
Um die Problemstellung zu vereinfachen beziehungsweise übersichtlicher zu gestalten, können ohne Beschränkung der Allgemeinheit folgende Einschränkungen vorgenommen werden:

- Es wird angenommen, dass $f(\mathbf{x})$ auf $x_j = b_j \quad (1 \leq j \leq s)$ die selben Werte annimmt, wie für $x_j = a_j$.
  Ansonsten betrachte die Funktion

  $$f^*(\mathbf{x}) := f(b_1 - |x_1 - b_1|, \ldots, b_s - |x_s - b_s|)$$

  auf $Q^{*s} := \{\mathbf{x} \in \mathbb{R}^s : \quad a_j \leq x_j \leq 2b_j - a_j \quad (1 \leq j \leq s)\}$.
  Dann ist für $j \in \{1, \ldots, s\}$ tatsächlich

  $$f^*(x_1, \ldots, x_{j-1}, a_j, x_{j+1}, \ldots, x_s) = f^*(x_1, \ldots, x_{j-1}, 2b_j - a_j, x_{j+1}, \ldots, x_s)$$

  Weiters gilt: $\int_{Q^{*s}} f^*(\mathbf{x})\, d\mathbf{x} = 2^s \int_{Q^s} f(\mathbf{x})\, d\mathbf{x}$, da $f$ und $f^*$ auf $Q^s$ übereinstimmen

und $Q^{*s}$ sich aus $2^s$ Quadern $Q^s$ zusammensetzt.

- Außerdem wird angenommen, dass $Q^s$ der Einheitsquader

$$K^s := \{\mathbf{x} \in \mathbb{R}^s : \ 0 \leq x_j \leq 1 \ (1 \leq j \leq s)\}$$

ist. Sonst betrachte $f^{**} : \ K^s \to \mathbb{R}$,

$$f^{**}(t_1, \ldots, t_s) = f(a_1 + (b_1 - a_1)t_1, \ldots, a_s + (b_s - a_s)t_s)$$

Es gilt dann: $\int_{K^s} f^{**}(\mathbf{t})\, d\mathbf{t} = \frac{1}{\mathrm{Vol}(Q^s)} \int_{Q^s} f(\mathbf{x})\, d\mathbf{x}$, wobei $\mathrm{Vol}(Q^s)$ das Volumen von $Q^s$ ist.

Es kann also insgesamt angenommen werden, dass $f$ auf $K^s$ definiert ist und auf den Seiten $x_j = 0$ des Quaders den gleichen Wert annimmt wie auf den Seiten $x_j = 1$. Also kann $f$ auf ganz $\mathbb{R}^s$ periodisch fortgesetzt werden.

### 2.3.2 Lösungsmethoden

In diesem Abschnitt folgen wir, wenn nicht anders angegeben [5].

Im Eindimensionalen gibt es gute Näherungsformeln samt Fehlerabschätzung (zum Beispiel Trapez-Regel, Simpson-Formel, ...), die aber für $s \gg 1$ unbrauchbar sind. Ein Grund dafür ist, dass bei vorgegebener Genauigkeit die Anzahl der zu berechnenden Stützstellen exponentiell mit $s$ wächst.

Eine andere Möglichkeit, ein mehrdimensionales Integral zu approximieren, ist die sogenannte Monte-Carlo-Methode. Dabei wird eine (endliche) Folge von „Zufallszahlen“ (die in der Praxis deterministisch gewonnen wird, daher spricht man besser von Pseudo-Zufallszahlen) in $K^s$ erzeugt und die Funktion $f$ auf den Folgengliedern ausgewertet. Das arithmetische Mittel wird als brauchbare Näherung an das zu berechnende Integral aufgefaßt. Dabei beruft man sich auf das „Gesetz der großen Zahlen“.
Genauer gesagt, es sei $\otimes_{i=1}^{\infty} K_i^s \quad (K_i^s = K^s)$ der Raum der Folgen $\omega = (\mathbf{x_1}, \mathbf{x_2}, \ldots)$ mit den Folgengliedern aus $K^s$, $d\mu$ sei das Produktmaß zum Lebesgue-Maß auf $K^s$, dann ist für $\mu$-fast alle Folgen $\omega$:

$$\lim_{N \to \infty} \frac{1}{N} \sum_{j=1}^{N} f(\mathbf{x_j}) = \int_{K^s} f(\mathbf{x})\, d\mathbf{x}$$

Das heißt aber auch, dass wenn $\omega$ in einer Menge von Maß 0 bezüglich $\mu$ liegt, Konvergenz nicht garantiert ist.

Wenn man an $f$ bestimmte Regularitätsbedingungen stellt, erreicht man mit gewissen Quasi-Monte-Carlo-Verfahren (wo die $\mathbf{x_j}$ also nicht mehr (pseudo-) zufällig sind, sondern wo für $\omega$ spezielle Folgen, deren Elemente möglichst regelmäßig auf $K^s$ verteilt sind, gewählt werden) asymptotisch bessere Werte für den zu erwartenden Fehler.

Insbesondere sollen nun Funktionen von beschränkter Variation betrachtet werden.

### Beschränkte Variation nach Hardy und Krause

Die Definitionen dieses Abschnitts sind [10] entnommen.

**Der eindimensionale Fall.** Sei $f(x)$ eine reellwertige Funktion auf $[a,b]$ $(-\infty < a \leq b < +\infty)$.

**Definition 9.** Eine *Leiter* auf $[a,b]$ ist eine Menge $\mathcal{Y}$ die $a$ und höchstens endlich viele Punkte aus $(a,b)$ enthält. Der rechte Randpunkt $b$ des Intervalls ist nur dann enthalten, wenn $a = b$.
Jedes Element $y$ aus $\mathcal{Y}$ hat einen *Nachfolger* $y_+$:
Wenn $(y,+\infty) \cap \mathcal{Y} = \phi$, dann ist $y_+ = b$, sonst das kleinste Element in $(y,+\infty) \cap \mathcal{Y}$.
Sei $\mathbb{Y}$ die Menge aller Leitern auf $[a,b]$. Dann ist die *totale Variation* $V(f;a,b)$ von $f$ auf $[a,b]$ definiert als:

$$V(f;a,b) = \sup_{\mathcal{Y}\in\mathbb{Y}} \sum_{y\in\mathcal{Y}} |f(y_+) - f(y)| \tag{2.1}$$

Wenn $V(f;a,b) < \infty$, dann heißt $f$ eine *Funktion von beschränkter Variation*.
Die Menge der Funktionen von beschränkter Variation auf $[a,b]$ wird mit $BV[a,b]$ bezeichnet.

**Der mehrdimensionale Fall.** Für die Verallgemeinerung von (2.1) gibt es mehrere Möglichkeiten. Wir werden hier die Definitionen von Vitali sowie von Hardy und Krause angeben.

Zuerst werden wir ein paar Notationen für die Definitionen festlegen.

- Für $\mathbf{x} \in \mathbb{R}^s$ sei $x_j$ die $j$-te Komponente.
- Für $\mathbf{a}, \mathbf{b} \in \mathbb{R}^s$ schreibe $\mathbf{a} \leq \mathbf{b}$, wenn $a_j \leq b_j$ für alle $1 \leq j \leq s$ gilt.
- Für $\mathbf{a} \leq \mathbf{b}$ ist der Quader $[\mathbf{a}, \mathbf{b}]$ definiert als

$$[\mathbf{a}, \mathbf{b}] := \{\mathbf{x} \in \mathbb{R}^s | \mathbf{a} \leq \mathbf{x} \leq \mathbf{b}\}.$$

- Für beliebige $\mathbf{a}, \mathbf{b} \in \mathbb{R}^s$ sei $\mathrm{rect}[\mathbf{a}, \mathbf{b}]$ der Quader $[\tilde{\mathbf{a}}, \tilde{\mathbf{b}}]$, wobei $\tilde{a}_j = \min(a_j, b_j)$ und $\tilde{b}_j = \max(a_j, b_j)$.
- Für $j, k \in \{1, \ldots, s\}$ mit $j \leq k$ sei $j : k := \{j, j+1, \ldots, k-1, k\}$.
- Für $u \subseteq 1 : s$ sei $-u$ das Komplement von $u$ in $1 : s$.
- Für $\mathbf{x} \in \mathbb{R}^s$ und $u \subseteq 1 : s$ bezeichne $\mathbf{x}^u$ das $|u|$-Tupel, repräsentiert durch die Komponenten $x_j$ mit $j \in u$.
- Seien $u, v \subseteq 1 : s$ mit $u \cap v = \phi$ und $\mathbf{x}, \mathbf{z} \in [\mathbf{a}, \mathbf{b}]$. Dann bezeichne $\mathbf{x}^u : \mathbf{z}^v$ den Punkt $\mathbf{y} \in [\mathbf{a}^{u \cup v}, \mathbf{b}^{u \cup v}]$ mit $y_j = x_j$ für $j \in u$ und $y_j = z_j$ für $j \in v$.
- Sei $u \subseteq 1 : s$ , $\mathbf{y}^{-u} \in [\mathbf{a}^{-u}, \mathbf{b}^{-u}]$ und $f$ eine reellwertige Funktion auf $[\mathbf{a}, \mathbf{b}]$. Dann kann man eine Funktion $g$ definieren durch $g(\mathbf{x}^u) := f(\mathbf{x}^u : \mathbf{y}^{-u})$. Man schreibt dann für die Funktion $g$ auch $f(\mathbf{x}^u; \mathbf{y}^{-u})$, mit der Variablen $\mathbf{x}^u$ auf der linken Seite des Semikolon.

**Definition 10.** Sei $f : [\mathbf{a}, \mathbf{b}] \to \mathbb{R}$. Die *s-gefaltete alternierende Summe* von $f$ über $[\mathbf{a}, \mathbf{b}]$ ist definiert als

$$\Delta(f; \mathbf{a}, \mathbf{b}) := \sum_{v \subseteq 1:s} (-1)^{|v|} f(\mathbf{a}^v : \mathbf{b}^{-v})$$

*Bemerkung* 18. $\Delta(f; \mathbf{a}, \mathbf{b})$ ist wohldefiniert, auch wenn $\mathbf{a} \leq \mathbf{b}$ nicht gilt. Es ist

$$\Delta(f; \mathbf{a}, \mathbf{b}) = \pm \Delta(f; \mathrm{rect}[\mathbf{a}, \mathbf{b}]).$$

Das Minus tritt genau dann auf, wenn $a_j > b_j$ für eine ungerade Anzahl von $j \in 1 : s$.

**Definition 11.** Es sei $\mathbf{a} \leq \mathbf{b}$ und für alle $j \in 1 : s$, $\mathcal{Y}^j$ eine Leiter auf $[a_j, b_j]$. Eine *(mehrdimensionale) Leiter* $\mathcal{Y}$ auf $[\mathbf{a}, \mathbf{b}]$ hat die Form

$$\mathcal{Y} = \prod_{i=1}^{s} \mathcal{Y}^j.$$

Für $\mathbf{y} \in \mathcal{Y}$ erhält man den *Nachfolger* $\mathbf{y}_+$, indem man den Nachfolger in jeder Komponente $j$ nimmt.
Sei $\mathbb{Y}^j$ die Menge aller Leitern auf $[a_j, b_j]$, dann setzt man $\mathbb{Y} := \prod_{j=1}^{s} \mathbb{Y}^j$, die Menge aller Leitern auf $[\mathbf{a}, \mathbf{b}]$.

**Definition 12.** Sei $f : [\mathbf{a}, \mathbf{b}] \to \mathbb{R}$ und $\mathcal{Y}$ eine Leiter auf $[\mathbf{a}, \mathbf{b}]$. Die *Variation von $f$ über $\mathcal{Y}$* ist definiert als:

$$V_{\mathcal{Y}}(f) = \sum_{\mathbf{y} \in \mathcal{Y}} |\Delta(f; \mathbf{y}, \mathbf{y}_+)|$$

Die *Variation* von $f$ auf $[\mathbf{a}, \mathbf{b}]$ im Sinne von *Vitali* ist definiert als

$$V_{[\mathbf{a},\mathbf{b}]}(f) = \sup_{\mathcal{Y} \in \mathbb{Y}} V_{\mathcal{Y}}(f)$$

und $f$ heißt von *beschränkter Variation im Sinne von Vitali*, wenn $V_{[\mathbf{a},\mathbf{b}]}(f) < \infty$.

Die *Variation* von $f$ auf $[\mathbf{a}, \mathbf{b}]$ im Sinne von *Hardy und Krause* ist definiert als:

$$V_{HK}(f; \mathbf{a}, \mathbf{b}) = \sum_{u \subsetneq 1:s} V_{[\mathbf{a}^{-u}, \mathbf{b}^{-u}]} f(\mathbf{x}^{-u}; \mathbf{b}^u)$$

Wenn klar ist, welches $\mathbf{a}$ und $\mathbf{b}$ gemeint ist, dann schreibe für $V_{HK}(f; \mathbf{a}, \mathbf{b})$ kürzer $V_{HK}(f)$.
Die Funktion heißt von *beschränkter Variation im Sinne von Hardy und Krause*, wenn $V_{HK}(f; \mathbf{a}, \mathbf{b}) < \infty$.

Nach diesen Definitionen kann nun der folgende wichtige Satz, der als Koksma-Hlawka-Ungleichung bekannt ist, formuliert werden:

**Satz 8.** *Sei $f$ von beschränkter Variation im Sinne von Hardy und Krause auf $K^s$, $\omega = (\mathbf{x}_1, \ldots, \mathbf{x}_N)$ eine beliebige Folge in $K^s$ und*

$$D_N(\omega) := \sup_{Q \subset K^s} \left| \frac{1}{N} \sum_{j=1}^{N} \chi_Q(\mathbf{x}_j) - \mathrm{Vol}(Q) \right|$$

*wobei $\chi$ die charakteristische Funktion ist. Dann gilt:*

$$\left| \frac{1}{N} \sum_{j=1}^{N} f(\mathbf{x}_j) - \int_{K^s} f(\mathbf{x})\, d\mathbf{x} \right| \leq V_{HK}(f) \cdot D_N(\omega) \tag{2.2}$$

*Bemerkung* 19. In (2.2) wird also der Fehler durch ein Produkt einer Größe, die nur von der Funktion abhängt, und einer Größe, die nur von der gewählten Folge abhängt,

abgeschätzt. Der Ausdruck $D_N(\omega)$ heißt die *Diskrepanz* der Folge $\omega$. Sie ist klein, wenn $\omega$ möglichst gleichmäßig auf $K^s$ verteilt ist.
Man kann für die Diskrepanz die folgende Abschätzung zeigen, die Ungleichung von Erdös-Turan-Koksma genannt wird:
Für eine beliebige natürliche Zahl $M \geq 300$ ist immer

$$D_N(\omega) < 2^s \frac{300}{M} + 30^s \sum_{0<\|\mathbf{h}\|\leq M} |S_N(\mathbf{h},\omega)| R(\mathbf{h})^{-1}$$

wobei $\mathbf{h} \in \mathbb{Z}^s$, $\|\mathbf{h}\| := \max(|h_1|,\ldots,|h_s|)$, $R(\mathbf{h}) := \prod_{j=1}^s \max(|h_j|,1)$ und $S_N(\mathbf{h},\omega) = \frac{1}{N}\sum_{k=1}^N e^{2\pi i \mathbf{h}\cdot\mathbf{x}_k}$, wobei $\mathbf{h}\cdot\mathbf{x}_k$ das Skalarprodukt im $\mathbb{R}^s$ ist.

Betrachte nun folgende spezielle Folge $\omega^*$: Sei $p$ eine Primzahl, und für $1 \leq k \leq p-1$,

$$\mathbf{x}_k := \left(\frac{k}{p}, \frac{k^2}{p}, \ldots, \frac{k^s}{p}\right) \mod 1.$$

Dabei bedeutet mod 1 hier, dass in jeder Komponente modulo 1 reduziert wird, das heißt statt $x$ wird $\{x\}$ $(= x - \lfloor x \rfloor)$ genommen. Die Folge $\omega^*$ ist definiert durch

$$\omega^* = (\mathbf{x}_1, \ldots, \mathbf{x}_{p-1}).$$

E. Hlawka [5] konnte zeigen, dass für $\omega^*$ gilt: $D_N(\omega^*) < \frac{(70\log p)^s}{\sqrt{p}}$

**Methode der guten Gitterpunkte.** Folgen, die sehr genau approximieren, gewinnt man aus den „guten Gitterpunkten“.

**Definition 13** (E. Hlawka [5])**.** Es sei $p$ eine Primzahl, $\mathbf{g} \in \mathbb{Z}^s$. Dann heißt $\mathbf{g}$ ein *guter Gitterpunkt* mod $p$, wenn für alle $\mathbf{h} \in \mathbb{Z}^s \backslash \{0\}$ und $\mathbf{h}\cdot\mathbf{g} \equiv 0 \pmod p$

$$R(\mathbf{h}) \geq p(8\log p)^{-s}$$

E. Hlawka konnte zeigen [5, S. 147]:

**Satz 9.** *Es gibt immer gute Gitterpunkte* mod $p$ *.*

Sei $\mathbf{g}$ ein guter Gitterpunkt mod $p$. Definiere die Folge $\omega' = (\mathbf{x}_0, \ldots, \mathbf{x}_{p-1})$ durch

$$\mathbf{x}_k := \left(\frac{kg_1}{p}, \ldots, \frac{kg_s}{p}\right) \mod 1 \qquad (0 \leq k \leq p-1).$$

Für die Folge $\omega'$ gilt

$$D_N(\omega') < \frac{(1000 \log p)^{2s}}{p}$$

und daher für $f$ mit beschränkter Variation nach Hardy und Krause

$$\left| \frac{1}{p} \sum_{k=0}^{p-1} f(\mathbf{x}_k) - \int_{K^s} f(\mathbf{x})\, d\mathbf{x} \right| < V_{HK}(f) \frac{(1000 \log p)^{2s}}{p}.$$

Im Beweis dazu sieht man: Es gibt sogar einen guten Gitterpunkt, für den

$$\left| \frac{1}{p} \sum_{k=0}^{p-1} f(\mathbf{x}_k) - \int_{K^s} f(\mathbf{x})\, d\mathbf{x} \right| < V_{HK}(f) \frac{(80 \log p)^{s}}{p}$$

gilt.

Verlangt man von $f$ anstatt nur von beschränkter Variation zu sein, dass die partiellen Ableitungen bis zu einer bestimmten Ordnung existieren und durch eine gemeinsame Konstante beschränkt sind, kann man noch bessere Fehlerabschätzungen erreichen.

**Der zweidimensionale Fall.** Betrachte nun den zweidimensionalen Fall genauer. Die Formulierung von Definition 13 lautet für $s = 2$, wenn man eine neue Größe $\varrho(\mathbf{g})$ einführt:

**Definition 14.** Sei $p \in \mathbb{N}$, $\mathbf{g} \in \mathbb{Z}^2$ und

$$\varrho(\mathbf{g}) := \min_{\substack{\mathbf{h} \in \mathbb{Z}^2 \setminus \{0\} \\ \mathbf{g} \cdot \mathbf{h} \equiv 0 \pmod p}} R(\mathbf{h}) = \min_{\substack{\mathbf{h} \in \mathbb{Z}^2 \setminus \{0\} \\ \mathbf{g} \cdot \mathbf{h} \equiv 0 \pmod p}} (\max(1, |h_1|) \cdot \max(1, |h_2|)).$$

Dann heißt $\mathbf{g}$ ein *guter Gitterpunkt* mod $p$, wenn $\varrho(\mathbf{g}) \geq \frac{p}{(8 \log p)^2}$.

Zur Eignung von $\mathbf{g}$ für die Methode der guten Gitterpunkte soll also $\varrho(\mathbf{g})$ möglichst groß sein. Es soll nun eine Abschätzung von $\varrho(\mathbf{g})$ nach oben und nach unten gegeben werden. Dabei folgen wir im Wesentlichen [14].
Dazu sollen ohne Beschränkung der Allgemeinheit folgende Bedingungen an $\mathbf{g}$ und $p$ gestellt werden:

- Ohne Beschränkung der Allgemeinheit wird verlangt, dass $\mathrm{ggT}(g_1, g_2, p) = 1$.
  Das ist keine wesentliche Einschränkung, denn wenn man $\mathbf{g}$ und $p$ mit der glei-

chen Konstanten $k$ multipliziert, wird $\varrho(\mathbf{g})$ jedenfalls nicht größer. Denn

$$\mathbf{g}\cdot\mathbf{h}\equiv 0 \pmod{p} \quad\Leftrightarrow\quad k(\mathbf{g}\cdot\mathbf{h})\equiv 0 \pmod{k\cdot p}$$
$$\Rightarrow \{\mathbf{h}\in\mathbb{Z}^2\backslash\{0\}|\ \mathbf{g}\cdot\mathbf{h}\equiv 0 \pmod{p}\} = \{\mathbf{h}\in\mathbb{Z}^2\backslash\{0\}|\ k(\mathbf{g}\cdot\mathbf{h})\equiv 0 \pmod{k\cdot p}\}$$
$$\Rightarrow \varrho_p(\mathbf{g}) = \varrho_{k\cdot p}(k\cdot\mathbf{g})$$

wobei die Indizes an $\varrho$ die Abhängigkeit von $p$ beziehungsweise von $k\cdot p$ anzeigen soll.

- Weiters soll verlangt werden, dass mindestens eine der beiden Koordinaten von $\mathbf{g}$ teilerfremd mit $p$ ist, o.B.d.A. soll das $g_1$ sein.
  Wenn nämlich $g_1$ und $g_2$ verschiedene gemeinsame Teiler mit $p$ haben, muss mindestens einer davon $\geq 3$ sein. Wenn also o.B.d.A. $\mathrm{ggT}(g_1,p) < \underbrace{\mathrm{ggT}(g_2,p)}_{\geq 3}$ ist, kann $h_1 = 0$ und $h_2 = \frac{p}{\mathrm{ggT}(g_2,p)}$ gewählt werden, daraus folgt $\varrho(\mathbf{g}) \leq \frac{p}{\mathrm{ggT}(g_2,p)} \leq \frac{p}{3}$. Das ist aber kein guter Wert für $\varrho$ (was zum Beispiel die folgenden Resultate zeigen), daher soll eben $\mathrm{ggT}(g_1,p)=1$ gelten.
  Multiplikation von $\mathbf{g}$ mit dem reziproken Element $\bmod p$ von $g_1$ ändert die Menge $\{\mathbf{h}\in\mathbb{Z}^2\backslash\{0\}|\ \mathbf{g}\cdot\mathbf{h}\equiv 0 \pmod{p}\}$ nicht, deshalb auch nicht $\varrho(\mathbf{g})$. Daher sei o.B.d.A. $g_1 = 1$.

- Wie oben gezeigt, wäre $\varrho(\mathbf{g})$ im Fall $\mathrm{ggT}(g_2,p) > 2$ klein. Auch der Fall, dass $\mathrm{ggT}(g_2,p) = 2$ soll von den weiteren Betrachtungen ausgeschlossen werden, da er Nachteile in manchen Anwendungen hat und keine wesentliche Verbesserung von $\varrho(\mathbf{g})$ bringt.

Zusammenfassend soll also o.B.d.A. der Fall $g_1 = 1$, $\mathrm{ggT}(g_2,p) = 1$ betrachtet werden.

**Proposition 6.** *Es sei* $\mathbf{g} = (1,g_2) \in \mathbb{Z}^2$, $p\in\mathbb{N}$ *mit* $\mathrm{ggT}(g_2,p)=1$ *und* $A$ *das Maximum der Teilnenner in der Kettenbruchdarstellung von* $\frac{g_2}{p}$. *Dann gilt:*

$$\varrho(\mathbf{g}) \geq \frac{p}{A+2} \tag{2.3}$$

*Beweis.* Setze $H := \{\mathbf{h}\in\mathbb{Z}^2\backslash\{0\}|\ \mathbf{g}\cdot\mathbf{h}\equiv 0 \pmod{p}\}$
Für $\mathbf{h}\in H$, bei dem eine Koordinate verschwindet, ist $R(\mathbf{h})$ ein positives Vielfaches von $p$. Denn aus $h_1 + h_2 g_2 \equiv 0 \pmod{p}$ folgt für $h_1 = 0$, dass (wegen $\mathrm{ggT}(g_2,p)=1$) $h_2 = lp$ mit einem $l\in\mathbb{Z}\backslash\{0\}$. Das analoge Resultat folgt auch für $h_2 = 0$. Sollte $R$

also auf so einem $\mathbf{h}$ sein Minimum annehmen, dann ist (2.3) klarerweise erfüllt.
Für den Rest des Beweises kann man daher annehmen, dass $0 < |h_2| < p$.
Außerdem nehme o.B.d.A. an, dass $0 < g_2 < p$.
Sei $\frac{g_2}{p} = [0; a_1, a_2, \ldots, a_r]$.
Es seien hier $A_n$ die Zähler und $B_n$ $(0 \leq n \leq r)$ die Nenner der Näherungsbrüche an den Kettenbruch $[0; a_1, \ldots, a_r]$.
Dann existiert ein $m < r$, $m \in \mathbb{N}_0$, sodass

$$B_m \leq |h_2| < B_{m+1} \tag{2.4}$$

Die Kongruenz $\mathbf{g} \cdot \mathbf{h} \equiv 0 \pmod{p}$ ist äquivalent zur Existenz eines ganzen $b$ mit:

$$h_2 \frac{g_2}{p} - b = -\frac{h_1}{p}$$

Es folgt

$$\left|\frac{h_1}{p}\right| = \left|h_2 \frac{g_2}{p} - b\right| \overset{\text{Punkt 3 aus Lemma 5}}{\geq} \left|B_m \frac{g_2}{p} - A_m\right|$$

Außerdem gilt:

$$\left|\frac{g_2}{p} - \frac{A_m}{B_m}\right| \overset{(1.22)}{\geq} \frac{1}{B_m(B_m + B_{m+1})}$$

Daraus folgt: $|\frac{h_1}{p}| \geq \frac{1}{B_m + B_{m+1}}$ und mit (2.4):

$$|h_1 h_2| \geq \frac{pB_m}{B_m + B_{m+1}}$$

Aus der Definition von $B_m$ folgt

$$\begin{aligned} B_{m+1} &\leq (a_{m+1} + 1)B_m \leq (A+1)B_m \\ \Rightarrow \qquad |h_1| \cdot |h_2| &\geq \frac{p}{A+2} \end{aligned}$$

□

**Proposition 7.** *Wie in Proposition 6 seien* $\mathbf{g} = (1, g_2) \in \mathbb{Z}^2$, $p \in \mathbb{N}$ *mit* $\mathrm{ggT}(g_2, p) = 1$ *und* $A$ *das Maximum der Teilnenner in der Kettenbruchdarstellung von* $\frac{g_2}{p}$. *Dann gilt:*

$$\varrho(\mathbf{g}) \leq \frac{p}{A} \tag{2.5}$$

*Beweis.* Es seien $\frac{g_2}{p} = [0; a_1, \ldots, a_r]$ und $A_n$, $B_n$ und $H$ wie im Beweis zu Proposition 6.

Setze für $q \in \{1, \dots, r\}$

$$h_1 := A_{q-1}p - B_{q-1}g_2 \quad \text{und} \quad h_2 := B_{q-1}.$$

Dann ist $(h_1, h_2) \in H$. Nach (1.14) gilt

$$\left| \frac{A_{q-1}}{B_{q-1}} - \frac{g_2}{p} \right| = \frac{1}{B_{q-1}(B_{q-1}\xi + B_{q-2})},$$

wobei $\xi := [a_q; a_{q+1}, \dots, a_r] \geq a_q$.
Daher gilt:

$$|h_1 h_2| = B_{q-1}|A_{q-1}p - g_2 B_{q-1}| = \frac{p}{\xi + B_{q-2}B_{q-1}^{-1}}$$

Für $a_q = A$ ergibt sich dann:

$$\varrho(\mathbf{g}) \leq |h_1 h_2| \leq \frac{p}{A}$$

□

*Bemerkung* 20. Wenn $g_2 = F_{n-1}$ und $p = F_n$ als aufeinanderfolgende Fibonacci-Zahlen gewählt werden, ist $A$ minimal, nämlich (wenn man $a_r = 1$ zuläßt) $A = 1$. Man kann zeigen, dass dann $\varrho(\mathbf{g}) = F_{n-2}$ ist.

*Bemerkung* 21. Es wurde also gezeigt, dass $\frac{p}{A+2} \leq \varrho(\mathbf{g}) \leq \frac{p}{A}$.
Für gegebenes $p \in \mathbb{N}$ kann also die Güte von $\mathbf{g} = (1, g_2)$ überprüft werden, indem in der Kettenbruchdarstellung von $\frac{g_2}{p}$ der maximale Teilnenner $A$ ermittelt wird. Ist dieser „groß“, wird $\mathbf{g}$ kein guter Gitterpunkt sein.
Man kann sich nun die Frage stellen, ob man für beliebiges $p$ ein $g_2$ finden kann, sodass $A$ unter einer fixen, von $p$ unabhängigen Schranke bleibt.
Genau das ist der Inhalt von Vermutung 1.

# 3 Lösungsansätze

## 3.1 Lösung für bestimmte Zahlenmengen

In Beispiel 2 wurde gezeigt, dass die Vermutung für Fibonacci-Zahlen erfüllt ist. In diesem Kapitel wird gezeigt, dass sie auch für beliebige Potenzen einiger kleiner natürlicher Zahlen (insbesondere für 2) erfüllt ist.
Wir werden dabei hauptsächlich die Formulierung für Kontinuanten, also Vermutung 2, verwenden, da die Beweise dann einfacher und übersichtlicher werden. Es wurde schon erwähnt, dass die beiden Formulierungen der Vermutung äquivalent sind.

### 3.1.1 Faltungslemma

Das sogenannte Faltungslemma ist ein wichtiges Hilfsmittel zum Beweis der Vermutung von Zaremba für die Potenzen einiger niedriger Zahlen. Ich werde das Lemma für Kettenbrüche und Kontinuanten formulieren, aber nur für Kontinuanten beweisen (und verwenden). Ein Beweis der Version für Kettenbrüche kann in [9] nachgelesen werden.

#### Formulierung für Kettenbrüche

**Lemma 7** (Faltungslemma für Kettenbrüche)**.** *Es seien* $a_1, \ldots, a_n \in \mathbb{N}$, $b \in \mathbb{N}_0$, *und* $a_0 \in \mathbb{Z}$. *Wenn* $\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n]$, *dann gilt:*

$$[a_0; a_1, \ldots, a_n, b, 1, a_n - 1, a_{n-1}, \ldots, a_1] = \frac{p_n}{q_n} + \frac{(-1)^n}{(b+1)q_n^2}$$

#### Formulierung für Kontinuanten

**Lemma 8** (Faltungslemma für Kontinuanten)**.** *Es seien* $a_1, \ldots, a_n \in \mathbb{N}, \quad b \in \mathbb{N}_0$. *Dann gilt:*

$$K_{2n+2}(a_1, \ldots, a_n, b, 1, a_n - 1, a_{n-1}, \ldots, a_2, a_1) = (b+1)K_n(a_1, \ldots, a_n)^2$$

*Dabei ist für $b = 0$ beziehungsweise $a_n = 1$ die Regel (1.30) anzuwenden:*

$$K(\ldots, x, 0, y, \ldots) = K(\ldots, x + y, \ldots)$$

Die 3 Spezialfälle für $b = 0$ beziehungsweise $a_n = 1$ ergeben dann:

- $a_n = 1, b > 0$:

$$K_{2n}(a_1, \ldots, a_{n-1}, 1, b, a_{n-1} + 1, a_{n-2}, \ldots, a_1) = (b + 1)K_n(a_1, \ldots, a_{n-1}, 1)^2$$

- $a_n > 1, b = 0$:

$$K_{2n}(a_1, \ldots, a_{n-1}, a_n + 1, a_n - 1, a_{n-1}, \ldots, a_1) = K_n(a_1, \ldots, a_n)^2$$

- $a_n = 1, b = 0$:

$$K_{2n-2}(a_1, \ldots, a_{n-1}, a_{n-1} + 2, a_{n-2}, \ldots, a_1) = K_n(a_1, \ldots, a_{n-1}, 1)^2$$

*Beweis.* Es sind 4 Fälle einzeln zu beweisen.

- 1.Fall: $a_n > 1, b > 0$
  Aus einfachen Eigenschaften von Kontinuanten ergibt sich:

$$\begin{aligned} &K_{2n+2}(a_1, \ldots, a_n, b, 1, a_n - 1, a_{n-1}, \ldots, a_1) \\ &\quad \overset{(1.28) \text{ und } (1.26)}{=} K_{n+1}(a_1, \ldots, a_n, b)K_{n+1}(a_1, \ldots, a_{n-1}, a_n - 1, 1) \\ &\qquad + K_n(a_1, \ldots, a_n)K_n(a_1, \ldots, a_n - 1) \\ &\quad \overset{(1.28) \text{ und } (1.27)}{=} (bK_n(a_1, \ldots, a_n) + K_{n-1}(a_1, \ldots, a_{n-1}) \underbrace{K_0}_{=1})K_n(a_1, \ldots, a_n) \\ &\qquad + K_n(a_1, \ldots, a_n)K_n(a_1, \ldots, a_n - 1) \end{aligned} \tag{3.1}$$

  Die letzte Kontinuante kann man auch anders darstellen:

$$\begin{aligned} K_n(a_1, \ldots, a_n - 1) &= (a_n - 1)K_{n-1}(a_1, \ldots, a_{n-1}) + K_{n-2}(a_1, \ldots, a_{n-2}) \\ &= a_n K_{n-1}(a_1, \ldots, a_{n-1}) + K_{n-2}(a_1, \ldots, a_{n-2}) \\ &\quad - K_{n-1}(a_1, \ldots, a_{n-1}) \\ &\overset{(1.28)}{=} K_n(a_1, \ldots, a_n) - K_{n-1}(a_1, \ldots, a_{n-1}) \end{aligned}$$

Das ergibt, in die obere Gleichung eingesetzt:

$$\begin{aligned}
&K_{2n+2}(a_1,\ldots,a_n,b,1,a_n-1,a_{n-1},\ldots,a_1)\\
&\quad=(bK_n(a_1,\ldots,a_n)+K_{n-1}(a_1,\ldots,a_{n-1}))K_n(a_1,\ldots,a_n)\\
&\qquad+K_n(a_1,\ldots,a_n)(K_n(a_1,\ldots,a_n)-K_{n-1}(a_1,\ldots,a_{n-1}))\\
&\quad=bK_n(a_1,\ldots,a_n)^2+K_{n-1}(a_1,\ldots,a_{n-1})K_n(a_1,\ldots,a_n)\\
&\qquad+K_n(a_1,\ldots,a_n)^2-K_{n-1}(a_1,\ldots,a_{n-1})K_n(a_1,\ldots,a_n)\\
&\quad=(b+1)K_n(a_1,\ldots,a_n)^2
\end{aligned}$$

Somit ist der erste Fall bewiesen.

- 2.Fall: $a_n = 1, b > 0$

Die Regel $K(\ldots,x,0,y,\ldots)=K(\ldots,x+y,\ldots)$ ergibt:

$$\begin{aligned}
&K_{2n+2}(a_1,\ldots,a_{n-1},1,b,1,0,a_{n-1},\ldots,a_1)\\
&\quad=K_{2n}(a_1,\ldots,a_{n-1},1,b,a_{n-1}+1,a_{n-2},\ldots,a_1)\\
&\quad\overset{(1.26)}{=}K_{2n}(a_1,\ldots,a_{n-2},a_{n-1}+1,b,1,a_{n-1},\ldots,a_1)\\
&\quad\text{Weil } a_{n-1}+1>1 \text{ , kann man den 1. Fall anwenden:}\\
&\quad=(b+1)K_{n-1}(a_1,\ldots,a_{n-1}+1)^2\\
&\quad\overset{(1.27)}{=}(b+1)K_n(a_1,\ldots,a_{n-1},1)^2
\end{aligned}$$

Damit ist auch der 2. Fall bewiesen.

- 3. Fall: $a_n > 1, b = 0$

Für die Null verwendet man wieder die bekannte Additionsregel (1.30). Daraus ergibt sich:

$$\begin{aligned}
&K_{2n+2}(a_1,\ldots,a_n,0,1,a_n-1,a_{n-1},\ldots,a_1)\\
&\quad=K_{2n}(a_1,\ldots,a_n+1,a_n-1,a_{n-1},\ldots,a_1)\\
&\quad\overset{(1.28)\text{ und }(1.26)}{=}K_n(a_1,\ldots,a_{n-1},a_n+1)K_n(a_1,\ldots,a_{n-1},a_n-1)\\
&\qquad+K_{n-1}(a_1,\ldots,a_{n-1})^2
\end{aligned}$$

$$
\begin{aligned}
&\overset{(1.28)}{=} ((a_n+1)K_{n-1}(a_1,\ldots,a_{n-1}) + K_{n-2}(a_1,\ldots,a_{n-2}))\\
&\quad\times ((a_n-1)K_{n-1}(a_1,\ldots,a_{n-1}) + K_{n-2}(a_1,\ldots,a_{n-2}))\\
&\quad + K_{n-1}(a_1,\ldots,a_{n-1})^2\\
&= (\underbrace{a_nK_{n-1}(a_1,\ldots,a_{n-1}) + K_{n-2}(a_1,\ldots,a_{n-2})}_{=K_n(a_1,\ldots,a_n)} + K_{n-1}(a_1,\ldots,a_{n-1}))\\
&\quad\times (\underbrace{a_nK_{n-1}(a_1,\ldots,a_{n-1}) + K_{n-2}(a_1,\ldots,a_{n-2})}_{=K_n(a_1,\ldots,a_n)} - K_{n-1}(a_1,\ldots,a_{n-1}))\\
&\quad + K_{n-1}(a_1,\ldots,a_{n-1})^2\\
&= K_n(a_1,\ldots,a_n)^2 - K_{n-1}(a_1,\ldots,a_{n-1})^2 + K_{n-1}(a_1,\ldots,a_{n-1})^2\\
&= K_n(a_1,\ldots,a_n)^2
\end{aligned}
$$

Das ist gerade das gewünschte Ergebnis für den 3. Fall.

- 4. Fall: $a_n = 1, b = 0$

In diesem Fall ist die bereits bekannte Regel

$$K(\ldots,x,0,y,\ldots) = K(\ldots,x+y,\ldots)$$

zweimal anzuwenden:

$$
\begin{aligned}
&K_{2n+2}(a_1,\ldots,a_{n-1},1,0,1,0,a_{n-1},\ldots,a_1)\\
&\quad = K_{2n-2}(a_1,\ldots,a_{n-1},a_{n-1}+2,a_{n-2},\ldots,a_1)\\
&\quad \overset{(1.28)\text{ und }(1.26)}{=} K_{n-1}(a_1,\ldots,a_{n-1})K_{n-1}(a_1,\ldots,a_{n-1}+2) + K_{n-2}(a_1,\ldots,a_{n-2})^2\\
&\quad \overset{(1.28)}{=} K_{n-1}(a_1,\ldots,a_{n-1})((a_{n-1}+2)K_{n-2}(a_1,\ldots,a_{n-2}) + K_{n-3}(a_1,\ldots,a_{n-3}))\\
&\qquad + K_{n-2}(a_1,\ldots,a_{n-2})^2\\
&\quad = K_{n-1}(a_1,\ldots,a_{n-1})(a_{n-1}K_{n-2}(a_1,\ldots,a_{n-2}) + K_{n-3}(a_1,\ldots,a_{n-3})\\
&\qquad + 2K_{n-2}(a_1,\ldots,a_{n-2})) + K_{n-2}(a_1,\ldots,a_{n-2})^2\\
&\quad \overset{(1.28)}{=} K_{n-1}(a_1,\ldots,a_{n-1})(K_{n-1}(a_1,\ldots,a_{n-1}) + 2K_{n-2}(a_1,\ldots,a_{n-2}))\\
&\qquad + K_{n-2}(a_1,\ldots,a_{n-2})^2
\end{aligned}
$$

$$
\begin{aligned}
&= K_{n-1}(a_1, \ldots, a_{n-1})^2 + 2K_{n-1}(a_1, \ldots, a_{n-1})K_{n-2}(a_1, \ldots, a_{n-2}) \\
&\quad + K_{n-2}(a_1, \ldots, a_{n-2})^2 \\
&= (K_{n-1}(a_1, \ldots, a_{n-1}) + K_{n-2}(a_1, \ldots, a_{n-2}))^2 \\
&\overset{(1.28)}{=} K_n(a_1, \ldots, a_{n-1}, 1)^2
\end{aligned}
$$

Somit ist auch der 4. Fall gezeigt und das Lemma bewiesen.

□

### 3.1.2 Potenzen kleiner Zahlen

Zarembas Vermutung kann mit Hilfe des Faltungslemmas für die Potenzen einiger kleiner natürlicher Zahlen bewiesen werden.
Dafür sucht man für geeignete Startwerte gewisse Darstellungen als Kontinuanten, deren Struktur sich im Wesentlichen bei Anwendung des Faltungslemmas mit passend gewähltem $b$ nicht ändert.
Dann liefert vollständige Induktion das Resultat.

Es sei daran erinnert, dass $S_k$ definiert wurde als die Menge aller natürlichen Zahlen, die als Kontinuanten mit Eintragungen $\leq k$ dargestellt werden können.

Bei der Darstellung der Sätze 10, 11 und 12 folgen wir im Wesentlichen H. Niederreiter [9].

**Satz 10.** *Für alle Potenzen der Zahl* 2 *gilt Vermutung 1 mit* $b = 3$. *Anders formuliert:*

$$\{2^l : \quad l \geq 0\} \subseteq S_3$$

*Beweis.* Die Richtigkeit der Behauptung für $0 \leq l \leq 5$ kann leicht nachgerechnet werden:

$$
\begin{aligned}
1 &= K_1(1) \\
2 &= K_1(2) \\
4 &= K_2(1, 3) \\
8 &= K_3(2, 1, 2) \\
16 &= K_3(2, 3, 2) \\
32 &= K_5(3, 1, 1, 3, 1)
\end{aligned}
$$

Es wird nun behauptet, dass für $l \geq 6$ sogar mehr gilt, nämlich:
Sei $l \geq 6$ dann gibt es ein $n \in \mathbb{N}$, sodass man $2^l$ darstellen kann als

$$2^l = K_n(2, a_2, a_3, \ldots, a_{n-1}, 2)$$

wobei die $a_i \leq 3$ sind, für $2 \leq i \leq n-1$.
Für $6 \leq l \leq 11$ kann das leicht nachgeprüft werden:

$$\begin{aligned} 64 &= K_6(2,1,1,3,1,2) \\ 128 &= K_8(2,1,1,1,1,2,1,2) \\ 256 &= K_6(2,3,1,3,3,2) \\ 512 &= K_8(2,3,1,1,1,2,3,2) \\ 1024 &= K_8(2,3,1,1,3,2,3,2) \\ 2048 &= K_{10}(2,1,1,2,3,3,1,1,2,2) \end{aligned}$$

Für $l \geq 12$ zeigt man die Behauptung mit vollständiger Induktion: Es sei die Behauptung für alle $6 \leq k \leq l-1$ schon gezeigt.

- Sei zunächst $l \geq 12$ ungerade.
  Dann ist $\frac{l-1}{2} \geq 6$. Daher kann man laut Induktionsvoraussetzung $2^{\frac{l-1}{2}}$ darstellen als:
  $$2^{\frac{l-1}{2}} = K_m(2, a_2, \ldots, a_{m-1}, 2)$$
  wobei $a_i \leq 3$ für $2 \leq i \leq m-1$.
  Wendet man das Faltungslemma mit $b = 1$ darauf an, so erhält man:

  $$\begin{aligned} &K_{2m+2}(2, a_2, \ldots, a_{m-1}, 2, 1, 1, 1, a_{m-1}, \ldots, a_2, 2) \\ &\qquad = 2 \cdot K_m(2, a_2, \ldots, a_{m-1}, 2)^2 = 2 \cdot (2^{\frac{l-1}{2}})^2 = 2^l \end{aligned}$$

  was den Induktionsschritt für ungerade $l$ abschließt.

- Sei nun $l \geq 12$ gerade.
  Dann ist $\frac{l}{2} \geq 6$, also kann man wieder nach Induktionsvoraussetzung $2^{\frac{l}{2}}$ darstellen als
  $$2^{\frac{l}{2}} = K_m(2, a_2, \ldots, a_{m-1}, 2)$$
  wobei wieder $a_i \leq 3$ für $2 \leq i \leq m-1$.

Anwendung des Faltungslemmas mit $b = 0$ ergibt:

$$K_{2m}(2, a_2, \ldots, a_{m-1}, 3, 1, a_{m-1}, \ldots a_2, 2) \\ = K_m(2, a_2, \ldots, a_{m-1}, 2)^2 = (2^{\frac{l}{2}})^2 = 2^l$$

Somit ist der Induktionsschritt auch für gerade $l$ gezeigt, und der Satz bewiesen.

□

*Bemerkung* 22. Die meisten Darstellungen als Kontinuanten am Induktionsanfang ($6 \leq l \leq 11$) im letzten Beweis müssen nicht mühsam berechnet werden, sondern können mit dem Faltungslemma und passender Wahl eines kleineren Startwerts und passendem $b$ ermittelt werden.

- Für $l = 6$ nimmt man den Startwert $K_3(2, 1, 2) = 8$ und $b = 0$, um

  $$K_8(2, 1, 2, 0, 1, 1, 1, 2) = K_6(2, 1, 3, 1, 1, 2) = 64$$

  zu erhalten.

- Für $l = 7$ wählt man $K_3(2, 1, 2) = 8$ als Startwert, sowie $b = 1$. Dann erhält man:

  $$K_8(2, 1, 2, 1, 1, 1, 1, 2) = 2 \cdot 8^2 = 128$$

- Für $l = 8$ wähle den Startwert $K_3(2, 3, 2) = 16$ und $b = 0$. Das ergibt:

  $$K_8(2, 3, 2, 0, 1, 1, 3, 2) = K_6(2, 3, 3, 1, 3, 2) = 16^2 = 256$$

- Für $l = 9$ nehme $K_3(2, 3, 2) = 16$ und $b = 1$:

  $$K_8(2, 3, 2, 1, 1, 1, 3, 2) = 2 \cdot 16^2 = 512$$

- Für $l = 10$ wähle wieder den Startwert $K_3 = (2, 3, 2) = 16$ und $b = 3$ im Faltungslemma. Das ergibt:

  $$K_8(2, 3, 2, 3, 1, 1, 3, 2) = 4 \cdot 16^2 = 1024$$

- Die Darstellung für $l = 11$,

  $$K_{10}(2, 1, 1, 2, 3, 3, 1, 1, 2, 2)$$

konnte offensichtlich (da $a_2 \neq a_9$) nicht durch Anwendung des Faltungslemmas gewonnen werden.
Dieser Fall muss gesondert berechnet werden, zum Beispiel kann man die Kettenbruchdarstellungen von $\frac{a}{2048}$ überprüfen, wobei $a$ ungerade ist und

$$\underbrace{683}_{>\lfloor\frac{2048}{3}\rfloor} \leq a < \underbrace{1024}_{=\frac{2048}{2}}.$$

So findet man

$$\frac{791}{2048} = [0; 2, 1, 1, 2, 3, 3, 1, 1, 2, 2],$$

woraus man die Kontinuante ablesen kann.

*Bemerkung* 23. Die Menge $\{2^l : \quad l \geq 0\} \not\subseteq S_2$, also ist $b = 3$ die kleinste Zahl, für die Zarembas Vermutung für alle Potenzen von 2 gilt. Die kleinste solche Potenz, die nicht in $S_2$ liegt, ist $16 = 2^4$. Denn man kann sich davon überzeugen, dass die folgende Liste der Darstellungen von 16 als Kontinuanten vollständig ist, wenn man von Spiegelungen ($K_n(a_1, \ldots, a_n) = K_n(a_n, \ldots, a_1)$ nach (1.26)) absieht:

$$\begin{aligned} 16 = K_1(16) = K_2(1, 15) = K_3(1, 14, 1) = K_5(1, 1, 3, 1, 1) = K_4(1, 1, 3, 2) \\ = K_3(2, 3, 2) = K_2(3, 5) = K_3(1, 2, 5) = K_4(1, 2, 4, 1) = K_3(3, 4, 1) \end{aligned}$$

**Satz 11.** *Für alle Potenzen der Zahl* 3 *gilt Vermutung 1 mit* $b = 3$. *Anders formuliert:*

$$\{3^l : \quad l \geq 0\} \subseteq S_3$$

*Beweis.* Für $0 \leq l \leq 3$ ist die Behauptung erfüllt, was man durch leichtes Nachrechnen bestätigt:

$$\begin{aligned} 1 &= K_1(1) \\ 3 &= K_2(1, 2) \\ 9 &= K_3(1, 3, 2) \\ 27 &= K_4(2, 1, 2, 3) \end{aligned}$$

Für $l \geq 4$ gilt sogar mehr, nämlich: Für jedes $l \geq 4$ gibt es ein $n \in \mathbb{N}$, sodass $3^l$ eine Darstellung als Kontinuante der Form

$$3^l = K_n(2, a_2, a_3, \ldots, a_{n-1}, 2)$$

hat, wobei $a_i \leq 3$ für $2 \leq i \leq n-1$.
Zeige das mit Induktion.
Für $4 \leq l \leq 7$ kann man folgende Darstellungen finden:

$$\begin{aligned} 81 &= K_7(2,1,1,1,1,2,2) \\ 243 &= K_8(2,1,1,1,3,1,2,2) \\ 729 &= K_9(2,1,1,2,1,3,1,3,2) \\ 2187 &= K_{10}(2,1,2,2,1,2,3,2,1,2) \end{aligned}$$

Sei nun $l \geq 8$ und das Gewünschte für alle $4 \leq k \leq l-1$ schon gezeigt.

- Wenn $l$ ungerade ist, dann ist $\frac{l-1}{2} \geq 4$. Laut Induktionsvoraussetzung hat also $3^{\frac{l-1}{2}}$ eine Darstellung als Kontinuante der Form

  $$3^{\frac{l-1}{2}} = K_m(2, a_2, \ldots, a_{m-1}, 2)$$

  mit $a_i \leq 3$ für $2 \leq i \leq m-1$ und $m \in \mathbb{N}$.
  Anwendung des Faltungslemma mit $b = 2$ ergibt

  $$\begin{aligned} &K_{2m+2}(2, a_2, \ldots, a_{m-1}, 2, 2, 1, 1, a_{m-1}, \ldots, a_2, 2) \\ &\qquad = 3 \cdot K_m(2, a_2, \ldots a_{m-1}, 2)^2 = 3 \cdot 3^{l-1} = 3 \end{aligned}$$

  Somit ist der Induktionsschritt für ungerades $l > 8$ gezeigt.

- Für den Fall, dass $l \geq 8$ gerade ist, gilt $\frac{l}{2} \geq 4$ und daher hat nach Induktionsvoraussetzung $3^{\frac{l}{2}}$ eine Kontinuantendarstellung der Form:

  $$3^{\frac{l}{2}} = K_m(2, a_2, \ldots, a_{m-1}, 2)$$

  wobei $a_i \leq 3$ für $2 \leq i \leq m-1$ und $m \in \mathbb{N}$.
  Wenn man darauf das Faltungslemma mit $b = 0$ anwendet, so erhält man:

  $$\begin{aligned} &K_{2m+2}(2, a_2, \ldots, a_{m-1}, 2, 0, 1, 1, a_{m-1}, \ldots, a_2, 2) \\ &\quad = K_{2m}(2, a_2, \ldots, a_{m-1}, 3, 1, a_{m-1}, \ldots, a_2, 2) = K_m(2, a_2, \ldots, a_{m-1}, 2)^2 = 3^l \end{aligned}$$

Somit ist der Induktionsschritt auch für die geraden $l > 8$ gezeigt. □

*Bemerkung* 24. Wie auch für die Potenzen von 2, gilt hier wieder $\{3^l : \quad l \geq 0\} \not\subseteq S_2$.

Hier ist $3^2 = 9$ die kleinste Zahl, die nicht in $S_3$ ist. Denn eine Auflistung aller Möglichkeiten, 9 als Kontinuante darzustellen, ergibt, wieder ohne Spiegelungen:

$$\begin{aligned} 9 = K_1(9) = K_2(1,8), = K_3(1,7,1) = K_2(2,4) \\ = K_3(1,1,4) = K_4(1,1,3,1) = K_3(2,3,1) \end{aligned}$$

**Satz 12.** *Für alle Potenzen der Zahl* 5 *gilt Vermutung 1 mit* $b = 4$*. Anders formuliert:*

$$\{5^l : \quad l \geq 0\} \subseteq S_4$$

*Beweis.* Es wird die folgende stärkere Behauptung bewiesen: Für jedes $l \in \mathbb{N}$ gibt es eine natürliche Zahl $m$, sodass $5^l$ eine Kontinuantendarstellung der Form

$$5^l = K_m(2, a_2, \ldots, a_{m-1}, 2)$$

hat, mit $a_i \leq 4$ für $2 \leq i \leq m-1$. Der Beweis erfolgt durch Induktion:
Für $l = 1$ hat man $5 = K_2(2,2)$.
Sei nun $l > 1$ und die Behauptung für alle natürlichen $k < l$ schon gezeigt.

- Wenn $l$ ungerade ist, dann ist $\frac{l-1}{2} \geq 1$. Laut Induktionsannahme kann man daher $5^{\frac{l-1}{2}}$ als
$$5^{\frac{l-1}{2}} = K_m(2, a_2, \ldots, a_{m-1}, 2)$$
mit $a_i \leq 4$ für $2 \leq i \leq m-1$ darstellen.
Es folgt Anwendung des Faltungslemma mit $b = 4$:
$$\begin{aligned} K_{2m+2}(2, a_2, \ldots, a_{m-1}, 2, 4, 1, 1, a_{m-1}, \ldots, a_2, 2) \\ = 5 \cdot K_m(2, a_2, \ldots, a_{m-1}, 2)^2 = 5 \cdot 5^{l-1} = 5^l \end{aligned}$$
Also ist die gewünschte Darstellung für $5^l$ gefunden.

- Wenn $l > 1$ gerade ist, dann ist $\frac{l}{2} \geq 1$. Nach Induktionsvoraussetzung hat daher $5^{\frac{l}{2}}$ eine Darstellung als Kontinuante der Form
$$5^{\frac{l}{2}} = K_m(2, a_2, \ldots, a_{m-1}, 2)$$
wobei $a_i \leq 4$ für $2 \leq i \leq m-1$ gilt.

Anwendung des Faltungslemma mit $b = 0$ ergibt:

$$K_{2m+2}(2, a_2, \ldots, a_{m-1}, 2, 0, 1, 1, a_{m-1}, \ldots, a_2, 2)$$
$$= K_{2m}(2, a_2, \ldots, a_{m-1}, 3, 1, a_{m-1}, \ldots, a_2, 2) = K_m(2, a_2, \ldots, a_{m-1}, 2)^2 = 5^l$$

Damit ist der Induktionsschritt auch für gerade $l \in \mathbb{N}$ bewiesen.

□

Der folgende Satz wurde von M. Yodphotong und V. Laohakosol gezeigt [13].

**Satz 13.** *Für alle Potenzen der Zahl* 6 *gilt Vermutung 1 mit* $b = 5$. *Anders formuliert:*

$$\{6^l : \quad l \geq 0\} \subseteq S_5$$

*Beweis.* Für $l = 0$ ist die Aussage trivial, für $l = 1$ hat man $6 = K_2(1, 5)$.
Für $l \geq 2$ wird folgende stärkere Aussage bewiesen:
Für jedes $l \geq 2$ hat $6^l$ eine Kontinuantendarstellung der Form

$$6^l = K_m(a_1, \ldots, a_m)$$

sodass $2 \leq a_1, a_m \leq 4$ und $a_i \leq 5$ für $2 \leq i \leq m-1$. Zeige das mit vollständiger Induktion. Für den Induktionsanfang erhält man für $l = 2$ und $l = 3$:

$$36 = K_4(3, 3, 1, 2)$$
$$216 = K_5(4, 2, 2, 4, 2)$$

Sei nun $l \geq 4$.

- Wenn $l$ gerade ist, dann ist $\frac{l}{2} \geq 2$. Nach Induktionsannahme kann man dann $6^{\frac{l}{2}}$ als
$$6^{\frac{l}{2}} = K_m(a_1, \ldots, a_m)$$
schreiben, wobei $2 \leq a_1, a_m \leq 4$ und $a_i \leq 5$ für $2 \leq i \leq m-1$.
Verwende nun das Faltungslemma mit $b = 0$:

$$K_{2m+2}(a_1, \ldots, a_m, 0, 1, a_m - 1, a_{m-1}, \ldots, a_1)$$
$$= K_{2m}(a_1, \ldots, a_m + 1, a_m - 1, a_{m-1}, \ldots, a_1) = K_m(a_1, \ldots, a_m)^2 = 6^l$$

Weil $2 \leq a_1 \leq 4$, $a_m + 1 \leq 5$ und $a_m - 1 \geq 1$, ist der Induktionsschritt für alle geraden $l$ gezeigt.

- Wenn $l$ ungerade ist, dann gilt $\frac{l-1}{2} \geq 2$.
  Deshalb gibt es nach Induktionsvoraussetzung eine Kontinuante $K_m(a_1, \ldots, a_m)$ mit $2 \leq a_1, a_m \leq 4$ und $a_i \leq 5$ für $2 \leq i \leq m-1$, sodass

$$6^{\frac{l-1}{2}} = K_m(a_1, \ldots, a_m)$$

  Anwendung des Faltungslemma mit $b = 5$ ergibt

$$\begin{aligned} &K_{2m+2}(a_1, \ldots, a_m, 5, 1, a_m - 1, a_{m-1}, \ldots, a_1) \\ &= 6 \cdot K_m(a_1, \ldots, a_m)^2 = 6 \cdot 6^{l-1} = 6^l \end{aligned}$$

  Da $a_m - 1 \geq 1$ und $2 \leq a_1 \leq 4$ ist der Induktionsschritt auch für ungerade $l$ bewiesen und somit der Satz gezeigt.

□

*Bemerkung* 25. Für Potenzen von Zahlen $x \geq 7$ funktioniert die in den letzten Sätzen verwendete Beweismethode nicht mehr, da im Falle eines ungeraden $l$ immer das Faltungslemma mit $b = x - 1$ angewendet wurde. Damit wäre für das Ergebnis die Vermutung 1 nicht mehr mit der Schranke $b = 5$ erfüllt. Für höhere Basen kann man aber immerhin noch Aussagen für einige gerade Exponenten zeigen. So gilt etwa, bewiesen von T. Komatsu [7]:

**Satz 14.** *Für $c \in \{1, 3, 5, 7, 9, 11\}$ gilt:*

$$\{7^{c \cdot 2^l} : \quad l \geq 0\} \subseteq S_3$$

*Beweis.* Für den Beweis benützt man folgende Beweisidee: Wenn

$$n = K_m(2, a_2, \ldots, a_{m-1}, 2) \tag{3.2}$$

dann erhält man mit dem Faltungslemma (und $b = 0$)

$$n^2 = K_{2m}(2, a_2, \ldots a_{m-1}, 3, 1, a_{m-1}, \ldots, a_2, 2) \tag{3.3}$$

Wenn also in (3.2) $a_i \leq 3$ für $2 \leq i \leq m-1$ gilt, insbesondere also $n \in S_3$ gilt, dann gilt das auch für die Darstellung von $n^2$ in (3.3), mehr noch: Das gleiche Argument ist auf $n^2$ anwendbar, sodass dann auch $n^{2^l} \in S_3$, für jedes $l \in \mathbb{N}$.

Man muss zum Beweis des Satzes also nur mehr geeignete Anfangswerte finden. Die Aussage des Satzes folgt dann durch fortgesetztes Quadrieren im Sinne der Beweisidee.

- Für $c = 1$ hat man $7 = K_3(1, 2, 2)$ und

$$7^2 = K_6(2, 1, 1, 2, 1, 2).$$

  Fortgesetztes Quadrieren liefert die Aussage.

- Für $c = 3$ verwende den folgenden Startwert, um $7^{3 \cdot 2^l} \in S_3$ für alle $l \in \mathbb{N}_0$ zu erhalten:

$$7^3 = K_{10}(2, 2, 1, 1, 1, 1, 1, 1, 1, 2)$$

- Für $c = 5$ verwende

$$7^5 = K_{15}(2, 2, 2, 1, 1, 1, 1, 2, 1, 2, 1, 2, 1, 1, 2)$$

  und fortgesetztes Quadrieren ergibt $\{7^{5 \cdot 2^l} : \quad l \in \mathbb{N}_0\} \subseteq S_3$.

- Für $c = 7$ nehme

$$7^7 = K_{21}(2, 2, 1, 2, 1, 1, 1, 1, 1, 3, 2, 1, 1, 1, 2, 1, 2, 1, 2, 1, 2)$$

  sodass wieder $\{7^{7 \cdot 2^l} : \quad l \in \mathbb{N}_0\} \subseteq S_3$ folgt.

- Wenn $c = 9$ ist, erreicht man $\{7^{9 \cdot 2^l} : \quad l \in \mathbb{N}_0\} \subseteq S_3$ durch fortgesetztes Quadrieren im Sinne der Beweisidee, ausgehend von:

$$7^9 = K_{28}(2, 2, 2, 1, 1, 2, 1, 2, 2, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 2, 1, 2, 1, 1, 2, 1, 1, 2)$$

- Für $c = 11$ verwendet man den Startwert

$$7^{11} = K_{33}(2, 2, 1, 2, 1, 2, 1, 2, 1, 1, 2, 2, 2, 2, 2, 1, 1, 1, 2, 1, 1, 1, 2, 1, 2, 1, 1, 1, 1, 1, 2, 1, 2)$$

  um mit der gleichen Methode wie zuvor $\{7^{11 \cdot 2^l} : \quad l \in \mathbb{N}_0\} \subseteq S_3$ zu erhalten.

□

*Bemerkung* 26. Die Methode aus dem Beweis zum letzten Satz läßt sich noch etwas verallgemeinern:

Wenn $n = K_m(a_1, \ldots, a_m)$ mit $a_i \leq k$ für $1 \leq i \leq m$ und $a_1, a_m \notin \{1, k\}$, dann ist $n^2 = K_{2m}(a_1, \ldots a_{m-1}, a_m + 1, a_m - 1, a_{m-1}, \ldots, a_2, a_1)$, das heißt auch $n^2$ hat eine Kontinuante mit allen Eintragungen $\leq k$ und man kann die Methode mit $n^2$ fortsetzen, da $a_1 \notin \{1, k\}$.
Da die Vermutung 1 mit $b = 5$ formuliert wurde, spielt hier nur $3 \leq k \leq 5$ eine Rolle.

*Beispiel* 3. Für $10 = K_2(3, 3)$ läßt sich die in Bemerkung 26 vorgestellte Methode anwenden. Es gilt $100 = K_4(3, 2, 4, 3)$ und allgemein $\{10^{2^l} : \quad l \in \mathbb{N}_0\} \subseteq S_4$.

Weiters gilt $10^3 = K_6(3, 4, 4, 3, 2, 2)$ und daraus folgt $\{10^{3 \cdot 2^l} : \quad l \in \mathbb{N}_0\} \subseteq S_4$.

## 3.2 Eine untere Schranke für $N_b(x)$

In diesem Abschnitt folgen wir im Wesentlichen [12].

**Definition 15.** Für $x \in \mathbb{R}$, $x \geq 1$ und $b \in \mathbb{N}$ sei

$$\mathcal{N}_b(x) := \{m \in \mathbb{N} : \ m \leq x, \ m \in S_b\}.$$

Weiters sei $N_b(x) := |\mathcal{N}_b(x)|$.

*Bemerkung* 27. Die Größe $N_b(x)$ gibt also die Anzahl der natürlichen Zahlen $\leq x$ an, für die die Vermutung von Zaremba mit Schranke $b$ gilt.
Demnach besagt die Vermutung in ihrer Präzisierung $b = 5$, dass $N_5(x) = \lfloor x \rfloor$.

In diesem Kapitel soll eine untere Schranke für $N_b(x)$ gefunden werden. Zuerst müssen einige Hilfsresultate gezeigt werden:

**Lemma 9.** *Es sei $k \leq n$, $a_i \in \mathbb{N}$ für $1 \leq i \leq n$, $b_i \in \mathbb{N}$ für $1 \leq i \leq k$ und $a_1 > 1$. Wenn $K_n(a_1, \ldots, a_n) = K_k(b_1, \ldots, b_k)$ und $K_{n-1}(a_1, \ldots, a_{n-1}) = K_{k-1}(b_1, \ldots, b_{k-1})$, dann ist $n = k$ und $a_i = b_i$ für $1 \leq i \leq n$.*

*Beweis.* Es gilt

$$[0; a_n, \ldots, a_1] \overset{(1.31)}{=} \frac{K_{n-1}(a_1, \ldots, a_{n-1})}{K_n(a_1, \ldots, a_n)} = \frac{K_{k-1}(b_1, \ldots, b_{k-1})}{K_k(b_1, \ldots, b_k)} \overset{(1.31)}{=} [0; b_k, \ldots, b_1]$$

Die Aussage folgt nun aus der Eindeutigkeit der Kettenbruchdarstellung (Satz 3), da $k \leq n$ und $a_1 \neq 1$. □

**Korollar 1.** *Für $x \in \mathbb{R}$, $x \geq 1$, $b \in \mathbb{N}$, $b \geq 2$ sei $\mathcal{M}_b(x)$ definiert als:*

$$\mathcal{M}_b(x) := \{(r,s) \in \mathbb{N}^2 : r \leq x, \exists n \in \mathbb{N} \quad \textit{und} \quad \exists c_i \ (1 \leq i \leq n) \textit{ mit } 1 \leq c_i \leq b, \\ c_1 \neq 1, \textit{ sodass} \quad r = K_n(c_1, \ldots, c_n) \quad \textit{und} \quad s = K_{n-1}(c_1, \ldots, c_{n-1})\}$$

*Dann gilt: Für $(r,s) \in \mathcal{M}_b(x)$ sind die $c_1, \ldots, c_n$ eindeutig bestimmt.*

*Beweis.* Das folgt direkt aus dem letzten Lemma. □

**Lemma 10.** *Sei $n \in \mathbb{N}_0$, $a_1, \ldots, a_n, b \in \mathbb{N}$ mit $a_1, \ldots, a_n \leq b$. Dann gilt:*

$$K_n(a_1, \ldots, a_n) \leq \left(\frac{b + \sqrt{b^2+4}}{2}\right)^n \tag{3.4}$$

*Beweis.* Der Beweis erfolgt mit Induktion nach $n$.
Für $n = 0$ ist die Aussage trivial.
Der Fall $n = 1$ ergibt sich aus

$$K_1(a_1) = a_1 \leq b < \frac{b + \sqrt{b^2+4}}{2}.$$

Sei nun $n > 1$.

$$\begin{aligned}
K_n(a_1, \ldots, a_n) &\overset{(1.28)}{=} \underbrace{K_{n-1}(a_1, \ldots, a_{n-1})}_{\substack{\text{Induktionsvoraussetzung} \\ \leq}} a_n + \underbrace{K_{n-2}(a_1, \ldots, a_{n-2})}_{\substack{\text{Induktionsvoraussetzung} \\ \leq}} \\
&\leq \left(\frac{b + \sqrt{b^2+4}}{2}\right)^{n-1} \cdot b + \left(\frac{b + \sqrt{b^2+4}}{2}\right)^{n-2} \\
&= \left(\frac{b + \sqrt{b^2+4}}{2}\right)^{n-2} \cdot \left(\frac{b + \sqrt{b^2+4}}{2} \cdot b + 1\right) \\
&= \left(\frac{b + \sqrt{b^2+4}}{2}\right)^{n-2} \cdot \frac{b^2 + \sqrt{b^2+4} \cdot b + 2}{2} \\
&= \left(\frac{b + \sqrt{b^2+4}}{2}\right)^{n-2} \cdot \frac{b^2 + 2b\sqrt{b^2+4} + (b^2+4)}{4} \\
&= \left(\frac{b + \sqrt{b^2+4}}{2}\right)^{n-2} \cdot \left(\frac{b + \sqrt{b^2+4}}{2}\right)^2 = \left(\frac{b + \sqrt{b^2+4}}{2}\right)^n
\end{aligned}$$

□

Nun sind wir in der Lage, den zentralen Satz dieses Kapitels zu beweisen:

**Satz 15.** *Für $x \in \mathbb{R}$, $x \geq 1$ und $b \in \mathbb{N}$, $b \geq 2$ gilt*

$$N_b(x) > \frac{1}{\sqrt{2b}}\, x^{\frac{C(b)}{2}},$$

*wobei*

$$C(b) := \frac{\log b}{\log \frac{b+\sqrt{b^2+4}}{2}}.$$

*Beweis.* Offensichtlich ist $\mathcal{M}_b(x) \subseteq \mathcal{N}_b(x) \times \mathcal{N}_b(x)$. Daher ist

$$M_b(x) \leq N_b(x)^2 \tag{3.5}$$

wobei $M_b(x) := |\mathcal{M}_b(x)|$.
Aus der Definition von $\mathcal{M}_b(x)$ ergibt sich nun die Abschätzung

$$M_b(x) \geq \sum_{n=1}^{\infty} \underbrace{\left( \sum_{c_1=2}^{b} \sum_{c_2=1}^{b} \sum_{c_3=1}^{b} \cdots \sum_{c_n=1}^{b} 1 \right)}_{K_n(c_1,\ldots,c_n) \leq x}.$$

Aus (3.4) erhält man nun, dass für $x \geq 1$ aus

$$n \leq \frac{\log x}{\log \frac{b+\sqrt{b^2+4}}{2}}$$

folgt, dass $K_n(c_1, \ldots, c_n) \leq x$. Setze nun

$$C(b, x) := \frac{\log x}{\log \frac{b+\sqrt{b^2+4}}{2}}.$$

Es folgt

$$\begin{aligned} M_b(x) &\geq \sum_{n \leq C(b,x)} \left( \sum_{c_1=2}^{b} \sum_{c_2=1}^{b} \cdots \sum_{c_n=1}^{b} 1 \right) = \sum_{n \leq C(b,x)} (b-1) b^{n-1} \\ &\geq \frac{1}{2} \sum_{n \leq C(b,x)} b^n > \frac{1}{2} b^{C(b,x)-1} = \frac{1}{2b}\, b^{C(b,x)} \\ &= \frac{1}{2b}\, b^{\frac{\log x}{\log\left(\left(b+\sqrt{b^2+4}\right)/2\right)}} = \frac{1}{2b}\, x^{\frac{\log b}{\log\left(\left(b+\sqrt{b^2+4}\right)/2\right)}} \end{aligned}$$

Aus (3.5) folgt nun

$$N_b(x) > \frac{1}{\sqrt{2b}}\, x^{\frac{\log b}{2\log\left(\left(b+\sqrt{b^2+4}\right)/2\right)}}.$$ □

## 3.3 Eine obere Schranke für die Teilnenner

In diesem Abschnitt folgen wir im Wesentlichen [2], wenn nicht anders angegeben.

In Vermutung 1 hatten wir angenommen, dass es für alle $m \in \mathbb{N}$ ein zu $m$ teilerfremdes $a$ gibt, sodass die Teilnenner der Kettenbruchdarstellung von $\frac{a}{m}$ durch einen Konstante beschränkt sind.
In diesem Kapitel wird ein schwächeres Resultat gezeigt, nämlich dass die Teilnenner durch gewisse Funktionen beschränkt sind, genauer:

**Satz 16.** *Für jedes $m \in \mathbb{N}$, $m > 1$ gibt es ein zu $m$ teilerfremdes $a \in \mathbb{N}$, sodass für die Kettenbruchdarstellung $[c_0; c_1, \ldots, c_r]$ von $\frac{a}{m}$ gilt:*

$$c_i \leq B \log m (\log \log m)^2 \quad \textit{für } 1 \leq i \leq r$$

*wobei $B$ eine von $m$ unabhängige Konstante ist.*
*Wenn $m$ eine Primzahl ist, so gilt das Resultat ohne den Faktor $(\log \log m)^2$.*

Der Beweis beruht im Wesentlichen auf folgendem Satz:

**Satz 17.** *Für jedes natürliche $d > 8$ gibt es ein Paar $a_1, a_2 \in \mathbb{N}$ mit $a_i$ jeweils relativ prim zu $d$, sodass*

$$\prod_{i=1}^{2} \left\| k \frac{a_i}{d} \right\| > \left( \frac{\varphi(d)}{d} \right)^2 (4d \log d)^{-1} \quad \textit{für } 1 \leq k < d. \tag{3.6}$$

*Hier ist $\| \cdot \|$ der Abstand zur nächsten ganzen Zahl und $\varphi$ die Eulersche $\varphi$-Funktion.*

*Beweis.* Der Beweis verwendet eine kombinatorische Methode:
Es wird gezeigt, dass die Anzahl der Paare $a_1, a_2 \leq \frac{d}{2}$ mit $a_i$ jeweils relativ prim zu $d$ größer ist als die Anzahl solcher Paare, für die (3.6) nicht gilt. Dadurch wird also die Existenz eines Paares, das (3.6) erfüllt, gezeigt, ohne so ein Paar konkret anzugeben, oder zu erklären, wie man es erhält.
Wir gehen folgendermaßen vor: Für $d \in \mathbb{N}$ und $a_1, a_2 \in \mathbb{N}$ sei $L$ eine positive reelle Zahl, die später gewählt wird. Wir nennen das Paar $a_1, a_2$ *exzeptionell* (bezüglich $d$ und $L$), wenn

$$\prod_{i=1}^{2} \left\| k \frac{a_i}{d} \right\| > \frac{1}{L} \quad \text{für alle } k,\ 1 \leq k < d. \tag{3.7}$$

Offensichtlich ist für ein exzeptionelles Paar $a_1, a_2$ notwendig jedes $a_i$ relativ prim zu $d$.

Wenn für ein $k$ ($1 \leq k < d$) die Ungleichung in (3.7) nicht erfüllt ist, so sagen wir, $k$ *schließt* das Paar $a_1, a_2$ *aus*.
Es sei die Größe $J(k, d, L)$ definiert als die Anzahl der Paare $a_1, a_2$, für die jedes $a_i$ teilerfremd mit $d$ ist, sowie $1 \leq a_1 < a_2 \leq \frac{d}{2}$ gilt und die von $k$ ausgeschlossen sind.
Es sei nun $d > 8$. Es soll eine obere Schranke für $J(k, d, L)$ gefunden werden.

- Wir betrachten zuerst den Fall $\mathrm{ggT}(k, d) = 1$. In diesem Fall gilt

$$\left\{ \left\| k\frac{a}{d} \right\| : 1 \leq a \leq \frac{d}{2},\ \mathrm{ggT}(a, d) = 1 \right\} = \left\{ \frac{b}{d} : 1 \leq b \leq \frac{d}{2},\ \mathrm{ggT}(b, d) = 1 \right\}$$

  und daher $J(k, d, L) = J(1, d, L)$. Ein Paar $a_1, a_2 \leq \frac{d}{2}$ ist von $k = 1$ ausgeschlossen, wenn

$$a_1 \leq \frac{d^2}{La_2} \tag{3.8}$$

  Die Anzahl der Paare $a_1, a_2 \leq \frac{d}{2}$, für die (3.8) gilt, ist kleiner als

$$\sum_{a=1}^{\lfloor \frac{d}{2} \rfloor} \frac{d^2}{La} < \frac{d^2}{L}\left(\log\frac{d}{2} + 0.68\right) < \frac{d^2}{L}\log d. \tag{3.9}$$

  Da in $J(k, d, L)$ nur Paare mit $a_1 < a_2$ gezählt werden, kann das Ergebnis durch 2 dividiert werden, sodass man

$$J(k, d, L) = J(1, d, L) < \frac{d^2}{2L}\log d$$

  erhält. Die Einschränkung, dass die $a_i$ jeweils teilerfremd zu $d$ sind, wurde hier nicht verwendet.

- Für den Fall $\mathrm{ggT}\,(k, d) = s > 1$ erhält man sogar eine um den Faktor $\frac{8}{9}$ bessere Abschätzung:
  Da $\mathrm{ggT}\left(\frac{k}{s}, \frac{d}{s}\right) = 1$ folgt aus dem bisher gezeigten, dass

$$J\left(\frac{k}{s}, \frac{d}{s}, L\right) < \frac{\left(\frac{d}{s}\right)^2}{2L}\log\left(\frac{d}{s}\right). \tag{3.10}$$

  Das ergibt eine obere Schranke für die Anzahl der Paare $a_1, a_2$ mit

$$1 \leq a_1 < a_2 \leq \frac{d}{2s} \quad \text{und } \mathrm{ggT}(a_i, d) = 1 \qquad \text{für } (i = 1, 2) \tag{3.11}$$

  die von $k$ ausgeschlossen sind.

Es müssen aber die Paare $1 \leq a_1 < a_2 \leq \frac{d}{2}$, die von $k$ ausgeschlossen sind, gezählt werden. Dazu teile die natürlichen Zahlen $t \leq \frac{d}{2}$ in Blöcke der Form

$$(j-1)\frac{d}{s} + 1 \leq t \leq \frac{jd}{s} \qquad j = 1, 2, \ldots \tag{3.12}$$

Für gerades $s$ gibt es $\frac{s}{2}$ solche Blöcke, für ungerades $s$ gibt es $\frac{s-1}{2}$ ganze Blöcke und einen Teilblock, also ist für allgemeines $s$ die Anzahl der Blöcke gleich $\left\lfloor \frac{s+1}{2} \right\rfloor$. Aus jedem Paar $a_1, a_2$ das (3.11) erfüllt und das von $k$ ausgeschlossen ist, können andere von $k$ ausgeschlossene Paare $a_1^{'}, a_2^{'}$ gewonnen werden, indem man

$$a_i^{'} \equiv \pm a_i \mod \frac{d}{s}$$

und $a_i^{'} \leq \frac{d}{2}$ für $i = 1, 2$ wählt. Jedes $a_1$ und jedes $a_2$ kann auf $f(s)$ verschiedene Arten gewählt werden, wobei

$$f(s) = 2\left\lfloor \frac{s+1}{2} \right\rfloor = 2 \text{ mal die Anzahl der Blöcke in (3.12).}$$

Auf diese Weise erhält man alle von $k$ ausgeschlossenen Paare $a_1^{'}, a_2^{'} \leq \frac{d}{2}$ mit $a_1^{'} \neq a_2^{'}$, für die gilt, dass kein $a_i^{'}$ ein ganzzahliges Vielfaches von $\frac{d}{s}$ ist. Wenn ein $a_i^{'}$ so ein Vielfaches von $\frac{d}{s}$ ist, soll das betreffende Paar aber ohnehin nicht gezählt werden, da wir nur an Paaren mit $\mathrm{ggT}(a_i^{'}, d) = 1$ für $i = 1, 2$ interessiert sind. Hier wird die Bedingung gebraucht, die im Fall $\mathrm{ggT}(k, d) = 1$ nicht verwendet wurde.
Wegen der Voraussetzung $a_1^{'} < a_2^{'}$ kann die berechnete Anzahl halbiert werden und so erhält man

$$J(k, d, L) < \frac{1}{2} f(s)^2 \frac{\left(\frac{d}{s}\right)^2}{2L} \log\left(\frac{d}{s}\right) \quad \text{wenn } \mathrm{ggT}(k, d) = s > 1.$$

Es läßt sich leicht überprüfen, dass $\frac{f(s)^2}{2s^2} \leq \frac{8}{9}$ ist, also folgt für $\mathrm{ggT}(k, d) > 1$:

$$J(k, d, L) < \frac{8}{9} \cdot \frac{d^2}{2L} \log d$$

Sei nun $N$ die Anzahl aller Paare $a_1, a_2$ mit $1 \leq a_1 < a_2 \leq \frac{d}{2}$ und $a_i$ jeweils relativ prim zu $d$.
Weil für $1 \leq k < d$ gilt, dass $\|k\frac{a_i}{d}\| = \|(d-k)\frac{a_i}{d}\|$, gilt (3.7) genau dann wenn die Ungleichung in (3.7) für alle $k \leq \frac{d}{2}$ gilt. Daher gibt es ein exzeptionelles Paar jedenfalls,

wenn

$$N = \binom{\frac{\varphi(d)}{2}}{2} > \frac{d}{2} \cdot \frac{d^2}{2L} \log d.$$

Da

$$\binom{\frac{\varphi(d)}{2}}{2} = \frac{\frac{\varphi(d)}{2}(\frac{\varphi(d)}{2} - 1)}{2} \geq \frac{\varphi(d)^2}{16}$$

reicht es, $L \geq 4d(\frac{d}{\varphi(d)})^2 \log d$ zu wählen, um die Existenz eines exzeptionellen Paares sicherzustellen.
Es gibt also ein Paar $a_1, a_2$ mit jeweils $a_i$ relativ prim zu $d$, sodass

$$\prod_{i=1}^{2} \left\| k\frac{a_i}{d} \right\| > \left( \frac{\varphi(d)}{d} \right)^2 (4d \log d)^{-1} \quad \text{für } 1 \leq k < d.$$

Das war gerade die Aussage des Satzes. □

*Bemerkung* 28. Es gilt die allgemeinere Aussage: Für alle natürlichen $n > 1$ und $d > 4n$ gibt es $a_1, \ldots, a_n \in \mathbb{N}$ jeweils relativ prim zu $d$, sodass

$$\prod_{i=1}^{n} \left\| k\frac{a_i}{d} \right\| > 4^{-n} \left( \frac{\varphi(d)}{d} \right)^n (d \log^{n-1} d)^{-1} \quad \text{für } 1 \leq k < d.$$

Der Beweis verläuft analog zum gezeigten, wobei die entsprechende Aussage zu (3.9) mit Induktion zu zeigen ist.

**Korollar 2.** *Für alle natürlichen $d \geq 2$ gibt es ein zu $d$ relativ primes $a \in \mathbb{N}$, sodass für die Kettenbruchentwicklung $[0; c_1, \ldots, c_r]$ von $\frac{a}{d}$ gilt:*

$$c_i \leq 4 \left( \frac{d}{\varphi(d)} \right)^2 \log d \qquad (1 \leq i \leq r)$$

*Beweis.* Man kann o.B.d.A. in (3.6) verlangen, dass $a_1 = 1$ und $a_2 = a$ gilt. Man kann nämlich in (3.6) die Zahlen $a_i$ durch $ba_i$ ersetzen, wobei $b$ zu $a_1$ reziprok $\mod d$ ist. Demnach besagt Satz 17, dass es für jedes natürliche $d > 8$ (für $d \leq 8$ kann die Aussage des Korollars leicht direkt nachgerechnet werden) ein zu $d$ teilerfremdes, natürliches $a < d$ gibt, sodass

$$k \left\| k\frac{a}{d} \right\| > \left( \frac{\varphi(d)}{d} \right)^2 (4 \log d)^{-1} \quad \text{für alle } k \text{ mit } 1 \leq k < d. \tag{3.13}$$

Für $0 \leq i \leq r$ seien $p_i, q_i$ die $i$-ten Näherungszähler beziehungsweise Näherungsnenner

von $\frac{a}{d}$. Es gilt dann wegen (1.21) und Satz 7

$$q_i \left\| q_i \frac{a}{d} \right\| \leq \frac{1}{c_{i+1}} \qquad (i = 0, \ldots, r-1).$$

Daraus folgt wegen (3.13)

$$c_i \leq 4 \left( \frac{d}{\varphi(d)} \right)^2 \log d.$$

□

Zum Beweis von Satz 16 muss jetzt nur noch gezeigt werden, dass $\frac{d}{\varphi(d)}$ asymptotisch durch $C \log\log d$ dominiert wird.
Dies folgt aus der wohlbekannten Tatsache, dass für hinreichend große $d \in \mathbb{N}$

$$\frac{d}{\varphi(d)} \leq e^{\gamma} \log\log d$$

gilt, was zum Beispiel in [8, S. 128] und [4] bewiesen wird. Hier ist $\gamma$ die Euler-Mascheroni-Konstante.

*Bemerkung* 29. T. W. Cusick [3] hat das folgende stärkere Resultat gezeigt:
Für jedes ganze $m$ gibt es ein ganzes, zu $m$ teilerfremdes $a$, sodass für die Kettenbruchdarstellung $[0; c_1, \ldots, c_r]$ von $\frac{a}{m}$ gilt:

$$c_i \leq 3 \log m \qquad \text{für } i = 1, \ldots, r$$

# Literaturverzeichnis


[1] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer, Berlin, 2008.

[2] T. W. Cusick, *Products of simultaneous approximations of rational numbers*, Arch. Math. **53** (1989), no. 2, 154–158.

[3] _____, *Zaremba's conjecture and sums of the divisor function*, Math. Comput. **61** (1993), no. 203, 171–176.

[4] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendon press Oxford, 1960.

[5] E. Hlawka, *Zur angenäherten Berechnung mehrfacher Integrale*, Monatsh. Math. **66** (1962), no. 2, 140–151.

[6] E. Hlawka und J. Schoissengeier, *Zahlentheorie: Eine Einführung*, Manz, Wien, 1979.

[7] T. Komatsu, *On a Zaremba's conjecture for powers*, Sarajevo J. Math **1** (2005), 9–13.

[8] E. Krätzel, *Zahlentheorie*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1981.

[9] H. Niederreiter, *Dyadic fractions with small partial quotients*, Monatsh. Math. **101** (1986), no. 4, 309–315.

[10] A. B. Owen, *Multidimensional variation for quasi-Monte Carlo, in: Contemporary multivariate analysis and design of experiments, Ser. Biostat.,2*, 2005, pp. 49–74.

[11] O. Perron, *Die Lehre von den Kettenbrüchen*, Band 1, BG Teubner, Stuttgart, 1954.

[12] J. W. Sander, *On a conjecture of Zaremba*, Monatsh. Math. **104** (1987), no. 2, 133–137.

[13] M. Yodphotong and V. Laohakosol, *Proofs of Zaremba's conjecture for powers of 6, in: Proceedings of the International Conference on Algebra and its Applications, Chulalongkorn Univ., Bangkok*, 2002, pp. 278–282.

[14] S. K. Zaremba, *Good lattice points, discrepancy, and numerical integration*, Ann. Mat. Pura Appl. **73** (1966), no. 1, 293–317.

[15] ———, *La Méthode des «Bons Treillis» pour le Calcul des Intégrales Multiples, in: Appl. of Number Theory to Numerical Analysis , ed. S. K. Zaremba*, 1972, pp. 39–119.

# Lebenslauf

## Persönliche Daten

| | |
|---|---|
| **Name** | Johannes Franz Puttinger |
| **Geburtsdatum** | 19. April 1982 |
| **Geburtsort** | Mödling, Niederösterreich |

## Schulbildung

| | |
|---|---|
| **1988–1992** | Volksschule Morzg, Salzburg |
| **1992–2000** | Akademisches Gymnasium, Salzburg |

## Hochschulbildung

| | |
|---|---|
| **2000–2001** | Diplomstudium Mathematik, Universität Wien |
| **2001–2002** | Beurlaubung vom Studium für Zivildienst |
| **2002–2010** | Diplomstudium Mathematik, Universität Wien |
| **2006–2007** | Teilnahme Erasmus-Mobilitätsprogramm, University College Cork |