Universität des Saarlandes
Naturwissenschaftlich-Technische Fakultät I
Fachrichtung Mathematik

# Bachelorarbeit
# Untersuchungen zu Kettenbrüchen

vorgelegt von
Karl Bringmann
am 11.09.2009

Angefertigt unter der Leitung
und begutachtet von
Prof. Dr. Ernst-Ulrich Gekeler

Betreut von
Dipl.-Math. Johannes Lengler

# Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Saarbrücken, den 11.09.2009

(Unterschrift)

# Inhaltsverzeichnis

# 1 Einführung

## 1.1. Kettenbrüche und ein Gauß'sches Problem

Ein *Kettenbruch* ist ein (endlicher oder unendlicher) Bruch von der Form

$$x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \dots}}}$$

mit natürlichen Zahlen $b_k$. Jede reelle Zahl lässt sich (nahezu) eindeutig als Kettenbruch darstellen. Diese Form der Darstellung einer Zahl hat weniger praktische Anwendungen, ist aber von großer theoretischer Bedeutung, da sich viele Eigenschaften einer Zahl in dieser Darstellung leichter analysieren lassen. Sie spielt vor allem in der Zahlentheorie eine große Rolle.

Gauß stellte sich (und Laplace) 1812 die folgende Frage: Wählt man eine zufällige gleichverteilte reelle Zahl $T$ (im Einheitsintervall $[0, 1]$), dann verhalten sich auch die Kettenbruchkoeffizienten $b_k(T)$ zufällig. *Wie sieht die Verteilung dieser Zufallsvariablen* $b_k(T)$ *aus?*

Gauß konnte zeigen, dass die Wahrscheinlichkeit, dass der $k$-te Koeffizient größer gleich einer natürlichen Zahl $m$ ist, also $\Pr[b_k(T) \geq m]$, beim Grenzübergang $k \to \infty$ gegen $\log\left(1 + \frac{1}{m}\right)$ strebt. Diese Grenzverteilung erhielt später den Namen Gauß-Kuzmin-Verteilung. Gleichzeitig stellte er die weiterführende Frage, wie sich der Fehlerterm $r_k = \Pr[b_k(T) \geq m] - \log\left(1 + \frac{1}{m}\right)$ verhalte.

Dieser Term konnte erst 1928 von Kuzmin analysiert werden, nachzulesen in [Khi63]: Er zeigte, dass $r_k = O(\lambda^{\sqrt{k}})$ für $k \to \infty$ und eine Konstante $0 < \lambda < 1$. 1929 bewies Lévy [Lev29] die bessere Schranke $r_k = O(\lambda^k)$ für $\lambda = 0.7$. Schließlich gelang es Wirsing [Wir74] zu zeigen, dass

$$\lim_{k\to\infty} \frac{\Pr[b_k(T) \geq m] - \log\left(1 + \frac{1}{m}\right)}{(-\lambda)^k} = \Psi(1/m)$$

mit einer Konstanten $\lambda$ bekannt als die Gauß-Kuzmin-Wirsing-Konstante und einer analytischen Funktion $\Psi(x)$. Mehr zur historischen Entwicklung der Gauß-Kuzmin-

Verteilung kann auf [Wei] nachgelesen werden.

Man kann also sagen, dass die Verteilung von $b_k(T)$ sehr genau bekannt ist.

## 1.2. Unsere Variante

In der vorliegenden Arbeit werden wir uns mit einem leicht abgeänderten Problem beschäftigen: Wir wählen eine obere Schranke $N$ und ziehen eine zufällige gleichverteilte natürliche Zahl $D$ zwischen 1 und $N$. Nun betrachten wir $\sqrt{D}$ und dessen Kettenbruchentwicklung: *Was ist die Verteilung von* $b_k(\sqrt{D})$*?* Da der ganzzahlige Anteil einer solchen Wurzel keine Rolle spielt für die $k$-ten Kettenbruchkoeffizienten, $k > 0$, können wir die Menge dieser Wurzeln als endliche Teilmenge der überabzählbar unendlichen Menge $[0, 1]$ ansehen, in der wir $T$ zufällig gewählt hatten. Dies bedeutet aber, dass uns die Antwort auf Gauß' Frage nicht weiterhilft, zumindest nicht direkt. Besonders interessiert sind wir an der Grenzverteilung für $N \to \infty$, da wir auf diese Weise die Willkür bei der Wahl von $N$ beseitigen, und an dem Fehler zu dieser Grenzverteilung für endliche $N$. Genauso interessant bleibt die Frage, wenn wir $D$ nicht nur als natürliche Zahl, sondern sogar als quadratfreie Zahl wählen.

Wie sich herausstellen wird, sind die Verteilungen von $b_k(\sqrt{D})$ und $b_k(T)$ sehr ähnlich, was nicht von vorneherein klar ist, und wir können den Fehler zwischen beiden Verteilungen gut abschätzen. Dazu aber später.

So dargelegt wirkt unsere Variante des Gauß'schen Problems ein wenig aus der Luft gegriffen. Sie motiviert sich allerdings aus der Zahlentheorie:

## 1.3. Der Regulator eines quadratischen Zahlkörpers

Der *Regulator* $R$ eines Zahlkörpers ist eine wichtige Invariante. Wenn nicht von eigenem Interesse, so suchen wir Abschätzungen des Regulators, um diese mithilfe der analytischen Klassenzahlformel zu Abschätzungen der *Klassenzahl* eines Zahlkörpers zu transformieren, welche für den Zahlentheoretiker eine noch interessantere Invariante darstellt ([Zag81]).

Wir beschränken uns auf den Fall eines reell-quadratischen Zahlkörpers $K = \mathbb{Q}(\sqrt{D})$ mit einer quadratfreien natürlichen Zahl $D$ (der Einfachheit halber sei $D \equiv 2$ oder $3 \pmod 4$). Für diesen berechnen wir den Regulator, indem wir die Kettenbruchentwicklung von $\sqrt{D}$ betrachten: Diese ist immer periodisch, d.h. die Folge der Kettenbruchkoeffizienten ist periodisch. Sei $\ell$ die Periodenlänge. Nun betrachten wir statt des unendlichen Kettenbruchs mit Koeffizienten $[b_0; b_1, b_2, \ldots, b_\ell, \ldots]$ den Kettenbruch, der entsteht, wenn wir bei $b_{\ell-1}$ aufhören, also $[b_0; b_1, \ldots, b_{\ell-1}]$. Dies ist ein endlicher Kettenbruch, also eine rationale Zahl $\frac{x}{y}$, in der Sprache von Kapitel 2 ist dies der $(\ell - 1)$-te Konvergent von $\sqrt{D}$. Dann ist der Regulator gerade $\left|\log|x + y\sqrt{D}|\right|$.

Eine von Herrn Lengler aufgeworfene Fragestellung ist nun die folgende: *Was ist ein "typischer" Regulator eines quadratischen Zahlkörpers?* Sie zielt ab auf Antworten der

Form: Wählt man $D$ zufällig in $\{1, \ldots, N\}$, so ist die erwartete Größe des Regulators $X$, oder: so liegen 90% der Regulatoren im Bereich $[X, Y]$. Da der Beweis solcher Sätze außer Reichweite scheint, wären auch heuristische Argumente interessant, welche ähnliche Aussagen erlauben.

Wir haben gesehen, wie sich der Regulator berechnet. Da $x$ und $y$ dabei Zähler und Nenner eines Konvergenten der Kettenbruchentwicklung von $\sqrt{D}$ sind, ergeben sich zwei "Zutaten", die zur Beantwortung der obigen Fragestellung nötig sind: "Typische" Periodenlängen $\ell$ und "typische" Kettenbruchkoeffizienten $b_1, \ldots, b_{\ell-1}$.

Die erste Zutat scheint unerreichbar: Bisher gibt es nur sehr weit auseinander liegende obere und untere Schranken für die Periodenlänge (siehe [Coh77]), aber keinerlei Aussagen über mittlere Periodenlängen.

Die zweite Zutat gehen wir in der vorliegenden Arbeit an: Wir beweisen Aussagen über die Verteilung von $b_k(\sqrt{D})$, falls $D$ als zufällige Zahl zwischen 1 und $N$ gezogen wird. Und kennen wir die Verteilung des Koeffizienten, so kennen wir auch "typische" Koeffizienten, wie auch immer wir "typisch" interpretieren.

Anhand dieser zahlentheoretischen Motivation wird auch klar, warum die Frage besonders interessant wird, wenn wir $D$ zufällig aus den *quadratfreien* Zahlen zwischen 1 und $N$ ziehen: Es ist $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D \cdot k^2})$ für jedes $k \in \mathbb{N}$, es kommt also bei der Bildung des quadratischen Zahlkörpers nicht auf quadratische Teiler von $D$ an.

## 1.4. Das Resultat

Wir nehmen also eine zufällige natürliche Zahl $D$ zwischen 1 und $N$ und betrachten $\sqrt{D}$, wobei wir den ganzzahligen Anteil weglassen. Wie sich herausstellt, ist diese Zufallsvariable intuitiv recht gleichverteilt im Einheitsintervall $[0, 1]$. Wie dieser Begriff formal zu definieren ist, um unseren Ansprüchen gerecht zu werden, findet sich in Kapitel 2. Diese Gleichverteilung ist die einzige Eigenschaft, die wir benutzen werden, um unser Resultat zu zeigen:

Wir beweisen, dass für obiges $D$ die Differenz der Wahrscheinlichkeiten $\Pr[b_k(\sqrt{D}) \leq m]$ und $\Pr[b_k(T) \leq m]$ beschränkt ist durch $O\big(N^{-\frac{1}{4}} \log^{k-1}(N)\big)$, wenn wir $N$ gegen $\infty$ gehen lassen und $k$ konstant ist. Die durch die $O$-Notation versteckte Konstante ist dabei nur von $k$ abhängig. Dies sagt uns, dass die beiden Verteilungen von $b_k(\sqrt{D})$ und $b_k(T)$ im Grenzwert, für $N \to \infty$, gleich sind.

Wir können sogar für ein mit $N$ wachsendes $k$ eine Aussage treffen: Falls $k = o(\log(N)/\log\log(N))$, also nicht zu schnell wächst, so ist die Differenz der beiden Wahrscheinlichkeiten beschränkt durch $O(N^{\varepsilon - \frac{1}{4}})$ für jedes $\varepsilon > 0$. Dies sagt uns in etwa folgendes: Wählen wir eine zufällige Zahl in der Größenordnung von $N$ und ziehen die Wurzel, so verhalten sich zumindest die ersten $o(\log(N)/\log\log(N))$ Kettenbruchkoeffizienten so, wie wir es durch die Verteilung von $b_k(T)$ erwarten würden. Hier offenbart sich auch ein Ansatzpunkt, um die vorliegende Arbeit im Hinblick auf die im vorherigen Abschnitt vorgestellte Fragestellung zu typischen Regulatoren zu verbessern: Diese Schranke für $k$ sollte vergrößert werden, um von mehr oder sogar allen Kettenbruchkoeffizienten einer zufälligen Wurzel die Verteilung zu kennen.

Schränken wir $D$ auf die quadratfreien Zahlen zwischen 1 und $N$ ein, so erhalten wir auch leicht, dass die Differenz der Wahrscheinlichkeiten $\Pr[b_k(\sqrt{D}) \leq m]$ und $\Pr[b_k(T) \leq m]$ gegen 0 geht für $N \to \infty$. Benutzen wir eine bessere Abschätzung für die Anzahl $\sigma(x)$ quadratfreier Zahlen kleiner gleich $x$, welche allerdings nur unter der Riemann-Hypothese gilt, so bekommen wir auch eine effektive Abschätzung der Differenz durch $O(N^{\varepsilon - \frac{5}{27}})$ für alle $\varepsilon > 0$.

Für die betrachtete Differenz der beiden Wahrscheinlichkeiten zeigen wir zudem eine untere Schranke, welche zwar fern unserer oberen Schranke liegt, aber von eigenständigem Interesse ist.

Die genauen Formulierungen der Resultate finden sich in den Korollaren 4.3 und 4.4.

## 1.5. Vergleich zu Existierendem

Während der Arbeit an meiner Bachelorarbeit veröffentlichte Lerner [Ler08] eine Abhandlung über Kettenbrüche von Wurzeln rationaler Zahlen. Sein Theorem 1 zeigt unter anderem, dass $\left|\Pr[b_k(\sqrt{D}) = m] - \Pr[b_k(T) = m]\right| \to 0$ für $m \in \mathbb{N}$ und $N \to \infty$, also dass beide Verteilungen im Grenzwert übereinstimmen. Sein Beweis beruht auf der gleichen Idee, die auch wir benutzen: Die betrachteten Zahlen sind gleichverteilt im Einheitsintervall, was uns ermöglicht, die Riemann-Integrierbarkeit einer bestimmten Indikatorfunktion auszunutzen, um die gewünschte Wahrscheinlichkeit als Grenzwert endlicher Summen darzustellen. Zum Zeitpunkt da meine Lösungsidee ausgearbeitet war, hatte ich allerdings noch keine Kenntnis von Lerners Arbeit.

Die Darstellung des Beweises in [Ler08] ist viel knapper, als dies in der vorliegenden Arbeit der Fall ist. Das liegt daran, dass wir über Lerners Resultat hinaus eine effektive Fehlerabschätzung hinzufügen (welche allerdings technisch aufwendiger ist): Wir sind in der Lage, eine Fehlerschranke von $O(N^{\varepsilon - \frac{1}{4}})$ (und genauer) zwischen beiden Verteilungen anzugeben. Dies ermöglicht uns zudem, für mit $N$ wachsendes $k$ eine Konvergenz der Verteilung zu zeigen, nicht nur für konstantes $k$, also Aussagen zu treffen über die ersten $o(\log(N)/\log\log(N))$ Kettenbruchkoeffizienten der Wurzel einer zufälligen Zahl der Größenordnung $N$, was weit über Lerners Resultat hinaus geht.

## 1.6. Überblick über die Kapitel

Im nächsten Kapitel werden wir Notation zu Kettenbrüchen einführen, sowie einige fundamentale Aussagen sammeln, welche wir in den nachfolgenden Kapiteln benutzen werden. In Kapitel 3 definieren wir uns interessierende Mengen und führen den Begriff der Gleichverteilung ein, von dem wir zeigen, dass die definierten Mengen ihn erfüllen. Die Formulierung und der Beweis des Hauptresultats finden sich in Kapitel 4. Kapitel 5 beschäftigt sich mit einer unteren Schranke für den betrachteten Fehler. In Kapitel 6 schlussendlich finden sich die Beweise einiger Lemmata, welche wir in Kapitel 4 unterdrückt haben.

# 2 Fundamentales zu Kettenbrüchen

Ein *Kettenbruch* ist ein (endlicher oder unendlicher) Bruch von der Form

$$x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \dots}}}$$

mit $b_0 \in \mathbb{Z}$ und natürlichen Zahlen $b_i > 0$ für $i > 0$.

Die Theorie der Kettenbrüche liefert eine Vielzahl interessanter Ergebnisse. Der Leser sei zu einer umfangreichen Lektüre an das Standardwerk [Per13] verwiesen, tieferliegende Ergebnisse finden sich in [Khi63]. Im Folgenden werden wir einige Notation klären sowie von uns benötigte grundlegende Aussagen zu Kettenbrüchen formulieren, deren Beweise der geneigte Leser ebenso in [Per13] nachlesen kann. Aufgrund der hohen Vielfalt an konkurrierenden Notationen auf diesem Gebiet empfiehlt sich eine Lektüre dieses Kapitels auch für den fortgeschrittenen Leser.

Der Übersichtlichkeit halber schreiben wir einen Kettenbruch auch als

$$x = [b_0; b_1, b_2, b_3, \dots],$$

wobei die Folge der $b_i$ endlich oder unendlich sein darf. Dabei nennen wir $b_i = b_i(x)$ den $i$-ten *Kettenbruchkoeffizienten* von $x$ für $i \in \mathbb{N}$.

Wie man leicht einsieht, ist jeder endliche Kettenbruch eine rationale Zahl. Zudem lässt sich jede rationale Zahl als endlicher Kettenbruch darstellen. Diese Darstellung wird eindeutig, falls man die Konvention beachtet, dass der letzte Kettenbruchkoeffizient niemals 1 sein darf. Ein unendlicher Kettenbruch entspricht also einer irrationalen Zahl. Auch hier gilt, dass sich jede irrationale Zahl eindeutig als unendlicher Kettenbruch darstellen lässt.

Es ist weiterhin bekannt, welche Zahlen eine periodische Kettenbruchentwicklung haben, d.h. bei denen die Folge der Koeffizienten $b_i$ ab einem $k \in \mathbb{N}$ periodisch wird. Diese Zahlen sind genau die $x \in \mathbb{R}$ der Form

$$x = \frac{a + \sqrt{b}}{c}$$

mit $a \in \mathbb{Z},\ b \in \mathbb{N},\ b$ kein Quadrat, $0 \neq c \in \mathbb{Z}$. Insbesondere haben also Wurzeln natürlicher Zahlen eine periodische Kettenbruchentwicklung. Wir schreiben solche periodischen Kettenbrüche in der Form

$$x = [b_0; b_1, \ldots, b_k, \overline{b_{k+1}, \ldots, b_{k+\ell}}]$$

wenn sich $b_{k+1}, \ldots, b_{k+\ell}$ periodisch wiederholen.

Für endliche Kettenbrüche $x$ ist der $i$-te Koeffizient $b_i(x)$ nicht notwendigerweise definiert, zumindest nicht, falls die Kettenbruchentwicklung von $x$ weniger als $i$ Terme enthält. Allerdings rechtfertigt sich die Schreibweise $b_i(x)$ für alle $x \in \mathbb{R} \setminus \mathbb{Q}$, da diese Zahlen ja gerade den unendlichen Kettenbrüchen entsprechen und eine eindeutige Kettenbruchentwicklung besitzen. Daher müssen wir Aussagen über den $i$-ten Kettenbruchkoeffizienten auf die Menge $\mathbb{R} \setminus \mathbb{Q}$ einschränken.

Ein wichtiger Begriff bei der Untersuchung von Kettenbrüchen sind die *Konvergenten* $\frac{A_i}{B_i} = \frac{A_i(x)}{B_i(x)}$ von $x$ für $i \in \mathbb{N}_0$. Dies sind endliche Näherungsbrüche von $x$, nämlich

$$\frac{A_i}{B_i} := [b_0; b_1, \ldots, b_i],$$

wobei wir den Bruch in gekürzter Form wollen, also $(A_i, B_i) = 1$. Es ist klar, dass auch die Konvergenten nicht notwendig für einen endlichen Kettenbruch definiert sind, zumindest aber für alle $x \in \mathbb{R} \setminus \mathbb{Q}$. Wir haben beispielsweise

$$\frac{A_0}{B_0} = \frac{b_0}{1}, \quad \frac{A_1}{B_1} = b_0 + \frac{1}{b_1} = \frac{b_0 b_1 + 1}{b_1}, \quad \ldots$$

Dabei ist nicht von vorneherein klar, ob die auftretenden Brüche bereits in gekürzter Form sind. Es zeigt sich aber, dass sich die (gekürzten) $A_i$ und $B_i$ über einfache Rekursionen berechnen lassen, denn es gilt für $i \geq 2$

$$\begin{aligned} A_i &= b_i A_{i-1} + A_{i-2} \\ B_i &= b_i B_{i-1} + B_{i-2} \end{aligned} \tag{2.1}$$

Diese Rekursionen können wir auf $i \geq 1$ erweitern, indem wir

$$A_{-1} := 1,\ B_{-1} := 0 \tag{2.2}$$

setzen. Es ergeben sich sofort die Abschätzungen

$$0 \leq B_k \leq B_{k+1} \tag{2.3}$$

für $k \in \mathbb{N}_0$.

Die für die vorliegende Arbeit wichtigste Eigenschaft der Konvergenten ist die Formel

$$x = \frac{A_{i-1}\xi_i + A_{i-2}}{B_{i-1}\xi_i + B_{i-2}}, \tag{2.4}$$

wobei

$$\xi_i := [b_i; b_{i+1}, b_{i+2}, \ldots].$$

Durch sie gewinnen wir leicht obere und untere Abschätzungen für $x$ vermittels seiner Konvergenten.

Eine letzte hilfreiche Eigenschaft, die wir benötigen werden, ist die folgende Identität, welche für alle $i \geq 1$ gilt:

$$A_i B_{i-1} - A_{i-1} B_i = (-1)^{i-1}. \tag{2.5}$$

# 3 Gleichverteilung im Einheitsintervall

Wir sind an der Verteilung der Kettenbruchkoeffizienten von Wurzeln natürlicher Zahlen interessiert. Das von mir gewählte Modell zieht hierfür gleichverteilt eine zufällige natürliche Zahl D aus der Menge $\{1, \dots, n\}$ für eine feste obere Schranke $n \in \mathbb{N}$ und betrachtet die Verteilung von $b_k(\sqrt{D})$ für $k \in \mathbb{N}$. Die Verteilung des nullten Kettenbruchkoeffizienten ist trivial, da $b_0(\sqrt{D}) = \lfloor \sqrt{D} \rfloor$, also der ganzzahlige Anteil von $\sqrt{D}$ ist. Wir betrachten also nur $k \geq 1$. Dafür gilt aber, dass $b_k(\sqrt{D}) = b_k(\mathrm{frac}(\sqrt{D}))$, wobei $\mathrm{frac}(r)$ den fraktionalen Anteil $r - \lfloor r \rfloor$ von $r$ für $r \in \mathbb{R}$ bezeichnet.

Dabei müssen wir aufpassen, dass $b_k$ definiert ist, was nach Kapitel 2 zumindest dann erfüllt ist, wenn $\sqrt{D} \in \mathbb{R} \setminus \mathbb{Q}$, also $D$ kein Quadrat ist. Zudem wird es technisch einfacher sein, diejenigen Zahlen zu betrachten, welche zwischen zwei Quadratzahlen liegen. Wir untersuchen also die folgenden Mengen:

**Definition 3.1.** *Seien für $n \in \mathbb{N}$*

$$M_n := \{\mathrm{frac}(\sqrt{k}) \mid n^2 < k < (n+1)^2\}$$
$$M_n^U := \{\mathrm{frac}(\sqrt{k}) \mid 1 < k \leq n,\ k \text{ kein Quadrat}\}$$

Dann gilt $\bigcup_{i=1}^{n-1} M_i \subseteq M_N^U \subseteq \bigcup_{i=1}^{n} M_i$ für $n^2 \leq N \leq (n+1)^2$ und es sind $M_n, M_n^U \subset [0,1] \setminus \mathbb{Q}$.

Auf der anderen Seite sind oft auch nur die Wurzeln aus quadratfreien natürlichen Zahlen interessant. So macht es beispielsweise keinen Unterschied, ob wir den Körper $\mathbb{Q}(\sqrt{D})$ oder $\mathbb{Q}(\sqrt{k^2 D})$ betrachten für $k, D \in \mathbb{N}$, beide Körper sind isomorph. Wir schränken obige Mengen wie folgt ein, um auch den Fall quadratfreier Zahlen betrachten zu können:

**Definition 3.2.** *Seien für $n \in \mathbb{N}$*

$$Q_n := \{\mathrm{frac}(\sqrt{k}) \mid n^2 < k < (n+1)^2,\ k \text{ quadratfrei}\}$$
$$Q_n^U := \{\mathrm{frac}(\sqrt{k}) \mid 1 < k \leq n,\ k \text{ quadratfrei}\}$$

Die einzige Eigenschaft dieser Mengen, die wir benutzen werden, um die Verteilung des k-ten Koeffizienten abzuschätzen, ist ihre Gleichverteilung im Interval $[0, 1)$ im Sinne von folgender Definition:

**Definition 3.3.** *Eine Familie endlicher Mengen $(S_n)_{n=1}^{\infty}$, $S_n \subset [0,1)$, heiße* gleichverteilt*, wenn für jedes Intervall $I = (a,b) \subseteq [0,1)$ der Länge $|I| := b - a$ gilt:*

$$|\#(S_n \cap I)/\#S_n - |I|| \to 0$$

*für $n \to \infty$. Sie heiße* gleichverteilt mit Fehler $F(n)$*, wenn sogar*

$$|\#(S_n \cap I) - |I| \cdot \#S_n| \leq F(n)$$

*für alle $n \in \mathbb{N}$ gilt und $F(n) = o(\#S_n)$.*

Für eine gleichverteilte Familie $(S_n)$ gilt klar, dass $\#S_n \to \infty$. Gleichverteilung impliziert immer eine Gleichverteilung mit Fehler $o(\#S_n)$.

**Bemerkung 3.4.** *Beim Nachweis von Definition 3.3 spielt es keine Rolle, ob wir offene, geschlossene oder halb-offene Intervalle $I$ zulassen. Betrachten wir statt Intervallen der Form $(a,b)$ Intervalle der Form $[a,b], (a,b]$ oder $[a,b)$ (deren Länge wir ebenso als $b-a$ definieren), so verändert sich der Fehler um höchstens 2. Asymptotisch ändert sich der Fehler somit nicht für die von uns betrachteten Familien.*

Es stellt sich heraus, dass alle in den Definitionen 3.1 und 3.2 angegebenen Mengen gleichverteilt sind. Wir finden scharfe Fehlerschranken für die Gleichverteilung von $M_n$ und $M_n^U$ und nach Annahme der Riemann-Hypothese auch gute Fehlerschranken für $Q_n$ und $Q_n^U$. Dabei benutzen wir die (in der Informatik übliche) Schreibweise $f(n) = \Theta(g(n))$, falls ein $n_0 \in \mathbb{N}$ und Konstanten $c_1, c_2 > 0$ existieren, sodass $c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$. Also impliziert $f(n) = \Theta(g(n))$, dass $f(n) = O(g(n))$ und nicht $f(n) = o(g(n))$ gilt:

**Lemma 3.5.** *Es gelten:*

*(i) Die Familie $(M_n)_{n=1}^{\infty}$ ist gleichverteilt mit Fehler $O(1)$.*

*(ii) Die Familie $(M_n^U)_{n=1}^{\infty}$ ist gleichverteilt mit Fehler $\Theta(\sqrt{\#M_n^U})$.*

*(iii) Die Familie $(Q_n)_{n=1}^{\infty}$ ist gleichverteilt. Unter der Riemann-Hypothese ist diese Familie sogar gleichverteilt mit Fehler $O((\#Q_n)^{17/27+\varepsilon})$ für alle $\varepsilon > 0$.*

*(iv) Die Familie $(Q_n^U)_{n=1}^{\infty}$ ist gleichverteilt. Unter der Riemann-Hypothese ist diese Familie sogar gleichverteilt mit Fehler $O((\#Q_n^U)^{44/54+\varepsilon})$ für alle $\varepsilon > 0$.*

Der Rest des Kapitels besteht aus dem Beweis von Lemma 3.5.

*Beweis von Lemma 3.5.(i).* (i) Wir betrachten zuerst die Familie $(X_n)_{n=1}^{\infty}$ mit $X_n = \{\frac{i}{2n} \mid 0 \leq i < 2n\}$.

(ii) Die Familie $(X_n)$ ist gleichverteilt mit Fehler $O(1)$, denn:

Sei $I \subseteq [0,1)$ ein Intervall. Wir können $I$ schreiben als $I = I_1 \cup I_2 \cup I_3$ mit $I_2 = [\frac{i}{2n}, \frac{j}{2n})$, $i, j \in \{0, \ldots, 2n-1\}$, $I_1 = I \cap [0, \frac{i}{2n}), I_3 = I \cap [\frac{j}{2n}, 1]$ und $|I_1|, |I_3| \leq \frac{1}{2n}$. Dann ist

$$|\#(X_n \cap I) - |I| \cdot \#X_n| \leq \sum_{i=1}^{3} |\#(X_n \cap I_i) - |I_i| \cdot \#X_n| \leq 2 = O(1),$$

da der Summand für $i = 2$ gleich 0 ist und $|I_i| \leq \frac{1}{2n}$, also $0 \leq \#(X_n \cap I_i) \leq 1, 0 \leq |I_i| \cdot \#X_n \leq 1$ für $i = 1, 3$, weswegen die beiden weiteren Summanden jeweils durch 1 beschränkt sind.

(iii) Es ist nach Taylor-Formel:

$$\sqrt{n^2 + x} = n + \frac{x}{2n} - \int_0^x \frac{x - t}{4(n^2 + t)^{3/2}} dt$$

Für $0 \leq x \leq 2n$ können wir den Integranden nach unten durch 0 und nach oben durch $\frac{x}{4n^3}$, also das Integral betragsmäßig durch $\frac{x^2}{4n^3} \leq \frac{1}{n}$ abschätzen. Es ist dann

$$\sqrt{n^2 + x} = n + \frac{x}{2n} + O\Big(\frac{1}{n}\Big).$$

Also existiert eine Konstante $c \in \mathbb{N}$, sodass für alle $n \in \mathbb{N}, 1 \leq i \leq 2n$ gilt:

$$\frac{i - c}{2n} \leq \sqrt{n^2 + i} - n \leq \frac{i + c}{2n}$$

Oder, für $M_n = \{m_i \mid 1 \leq i \leq 2n\}, m_i = \mathrm{frac}(\sqrt{n^2 + i})$ und $x_i = \frac{i}{2n}$:

$$x_{i-c} \leq m_i \leq x_{i+c}$$

(wobei $x_{-j} := 0$ und $x_{2n-1+j} := 1$ sein soll für $j \in \mathbb{N}$).

(iv) Nun ist für jedes Intervall $I \subseteq [0, 1)$ nach Dreiecksungleichung:

$$\begin{aligned}
&|\#(M_n \cap I) - |I| \cdot \#M_n| \\
&\leq |\#(X_n \cap I) - |I| \cdot \underbrace{\#M_n}_{=\#X_n}| + |\#(X_n \cap I) - \#(M_n \cap I)| \\
&\overset{(ii)}{\leq} O(1) + |\#(X_n \cap I) - \#(M_n \cap I)|.
\end{aligned}$$

(v) Für ein Intervall $I = (a, b]$ (nach Bemerkung 3.4 spielt es keine Rolle, welche Art: offenes, geschlossenes oder halb-offenes Intervall wir betrachten) lässt sich obiger Term aber gerade schreiben als

$$
\begin{aligned}
&|\#(X_n \cap I) - \#(M_n \cap I)| \\
&= \big|\#\{x \in X_n \mid x \le b\} - \#\{x \in X_n \mid x \le a\} \\
&\quad - (\#\{x \in M_n \mid x \le b\} - \#\{x \in M_n \mid x \le a\})\big| \\
&\le \big|\#\{x \in X_n \mid x \le b\} - \#\{x \in M_n \mid x \le b\}\big| \\
&\quad + \big|\#\{x \in X_n \mid x \le a\} - \#\{x \in M_n \mid x \le a\}\big|.
\end{aligned}
$$

Sei nun

$$
\begin{aligned}
s &:= \max\{i \mid 1 \le i \le 2n,\ m_i \le b\} \\
r &:= \max\{i \mid 0 \le i < 2n,\ x_i \le b\}.
\end{aligned}
$$

Nun ist $m_s$ das größte Element in $\{x \in M_n \mid x \le b\}$. Dann ist wegen (iii) $x_r$ eines der $x_{s-c}, x_{s-c+1}, \ldots, x_{s+c}$, denn

$$
x_{s-c} \le m_s \le b < m_{s+1} \le x_{s+c+1}.
$$

Damit können wir aber die Differenz der Anzahlen an Elementen durch $c$ nach oben abschätzen. Wir erhalten also insgesamt:

$$
\begin{aligned}
&|\#(X_n \cap I) - \#(M_n \cap I)| \\
&\le c + c = O(1).
\end{aligned}
$$

Mit (iv) ergibt sich die Behauptung.

□

Als einfache Folgerung daraus ergibt sich die Aussage über $M_n^U$:

*Beweis von Lemma 3.5.(ii).* Es ist $M_N^U = S \cup \bigcup_{i=1}^{n-1} M_i$ für $N \in \mathbb{N}, n := \lfloor \sqrt{N} \rfloor$ und eine Menge $S$ mit $\#S \le 2\sqrt{N}$. Für ein Intervall $I \subseteq [0,1)$ gilt dann

$$
\begin{aligned}
&|\#(M_N^U \cap I) - |I| \cdot \#M_N^U| \\
&\le |\#(S \cap I) - |I| \cdot \#S| + \sum_{i=1}^{n-1} |\#(M_i \cap I) - |I| \cdot \#M_i| \\
&= O(\sqrt{N}) + O(\sqrt{N}) = O(\sqrt{\#M_N^U}).
\end{aligned}
$$

Zudem zeigt man wie im Beweis zu 3.5.(i), dass für $k \in \mathbb{N}$

$$\begin{aligned}\sqrt{k^2+1}-k &= \frac{1}{2k} - \int_0^1 \frac{1-t}{4(k^2+t)^{3/2}}dt \\ &\geq \frac{1}{2k} - \frac{1}{4k^2} \\ &= \frac{1}{2k}(1-\frac{1}{2k}) \\ &\geq \frac{1}{4k}.\end{aligned}$$

Daher liegt kein Element von $M_N^U$ im Intervall $(0, \frac{1}{4n})$ für $n = \lfloor\sqrt{N}\rfloor$. Der Fehler $F(N)$ ist also mindestens

$$\frac{1}{4n} \cdot \#M_N^U \geq \frac{1}{4\sqrt{N}} \cdot \#M_N^U \geq \frac{1}{8\sqrt{\#M_N^U}} \cdot \#M_N^U = \frac{1}{8}\sqrt{\#M_N^U}$$

für $N \geq 1$, da $\#M_N^U = N - n \geq \frac{N}{4}$. □

Eine ähnliche Fehlerabschätzung wie für die Mengen $M_n$ können wir auch für $Q_n$ durchführen. Dazu betrachten wir die Funktion $\sigma(x) := \#\{n \leq x \mid n \text{ quadratfrei}\}$. Es ist bekannt, dass

$$\sigma(x) = \frac{6}{\pi^2}x + r(x) \text{ mit } r(x) = O(\sqrt{x}). \tag{3.6}$$

Die beste Abschätzung für $r(x)$, die ohne zusätzliche Annahme auskommt, stammt von Walfisz [Wal63] und impliziert

$$r(x) = o(\sqrt{x}). \tag{3.7}$$

Unter der Riemann-Hypothese sind bessere Abschätzungen möglich, siehe [Pap05] für einen Überblick über alle bekannten Ergebnisse. Die beste mir bekannte Abschätzung ist von Jia [Jia93] und liefert

$$r(x) = O(x^{17/54+\varepsilon}) \tag{3.8}$$

für alle $\varepsilon > 0$.

Diese Ergebnisse nutzend, können wir die Aussage über $Q_n$ beweisen:

*Beweis von Lemma 3.5.(iii).* Sei $I \subseteq [0,1)$ ein Intervall, I = (a,b] (nach Bemerkung 3.4 spielt es keine Rolle, welche Art offenes, geschlossenes oder halb-offenes Intervall wir betrachten). Es ist

$$\#(I \cap Q_n) = \sigma((n+b)^2) - \sigma((n+a)^2),$$

denn die rechte Seite zählt gerade die quadratfreien natürlichen Zahlen zwischen $n^2$ und $(n+1)^2$, deren Wurzel einen fraktionalen Anteil zwischen $a$ und $b$ hat.

Nach Aussage (3.6) ist dies aber

$$\begin{aligned}\#(I \cap Q_n) &= \frac{6}{\pi^2}((n+b)^2 - (n+a)^2) + r((n+b)^2) - r((n+a)^2) \\ &= \frac{6}{\pi^2}(2(b-a)n + b^2 - a^2) + r((n+b)^2) - r((n+a)^2) \\ &= (b-a)\frac{12}{\pi^2}n + O(1) + r((n+b)^2) - r((n+a)^2),\end{aligned}$$

da $0 \leq a, b \leq 1$.

Zudem ist

$$\begin{aligned}\#Q_n &= \sigma((n+1)^2) - \sigma(n^2) \\ &= \frac{6}{\pi^2}((n+1)^2 - n^2) + r((n+1)^2) - r(n^2) \\ &= \frac{6}{\pi^2}(2n+1) + r((n+1)^2) - r(n^2) \\ &= \frac{12}{\pi^2}n + O(1) + r((n+1)^2) - r(n^2).\end{aligned}$$

Zusammenfassend ist also

$$\begin{aligned}&|\#(I \cap Q_n) - |I| \cdot \#Q_n| \\ &= \Big|(b-a)\frac{12}{\pi^2}n + O(1) + r((n+b)^2) - r((n+a)^2) \\ &\quad - (b-a)\big(\frac{12}{\pi^2}n + O(1) + r((n+1)^2) - r(n^2)\big)\Big| \\ &\leq O(1) + |r((n+1)^2)| + |r((n+b)^2)| + |r((n+a)^2)| + |r(n^2)|.\end{aligned}$$

Nach (3.7) ist nun $r(x) = o(\sqrt{x})$, also

$$|\#(I \cap Q_n) - |I| \cdot \#Q_n| = o(n) = o(\#Q_n),$$

denn $\#Q_n = \frac{6}{\pi^2}(2n+1) + o(n)$.

Unter der Riemann-Hypothese bekommen wir mit (3.8)

$$\begin{aligned}|\#(I \cap Q_n) - |I| \cdot \#Q_n| &= O((n^2)^{17/54+\varepsilon/2}) \\ &= O(n^{17/27+\varepsilon}) \\ &= O(\#Q_n^{17/27+\varepsilon})\end{aligned}$$

für alle $\varepsilon > 0$. □

Die Ausweitung auf $Q_n^U$ ist wiederum einfach:

*Beweis von Lemma 3.5.(iv).* Es ist $Q_N^U = S \cup \bigcup_{i=1}^{n-1} Q_i$ für $N \in \mathbb{N}, n := \lfloor \sqrt{N} \rfloor$ und eine Menge $S$ mit $\#S \leq 2\sqrt{N}$. Für ein Intervall $I \subseteq [0,1)$ ist

$$\begin{aligned}
&|\#(Q_n^U \cap I) - |I| \cdot \#Q_n^U| \\
&\leq |\#(S \cap I) - |I| \cdot \#S| + \sum_{i=1}^{n-1} |\#(Q_i \cap I) - |I| \cdot \#Q_i| \\
&= O(n) + o(n^2) = o(Q_n^U),
\end{aligned}$$

da $\#Q_n^U = \frac{6}{\pi^2} n^2 + o(n)$. Unter der Riemann-Hypothese gilt sogar

$$\begin{aligned}
&|\#(Q_n^U \cap I) - |I| \cdot \#Q_n^U| \\
&\leq |\#(S \cap I) - |I| \cdot \#S| + \sum_{i=1}^{n-1} |\#(Q_i \cap I) - |I| \cdot \#Q_i| \\
&= O(n) + O(n \cdot n^{17/27+\varepsilon}) \\
&= O(n^{44/27+\varepsilon}) \\
&= O((\#Q_n^U)^{44/54+\varepsilon})
\end{aligned}$$

für alle $\varepsilon > 0$. □

# 4 Satz über die Konvergenz der Verteilung

In diesem Kapitel formulieren und beweisen wir unser Hauptresultat, welches Aussagen über die Kettenbruchkoeffizienten der Elemente gleichverteilter Familien ermöglicht. Als Korollar erhalten wir Aussagen über die Kettenbruchkoeffizienten von Wurzeln natürlicher Zahlen und Wurzeln quadratfreier Zahlen.

## 4.1. Formulierung und Folgerungen

Wir definieren zwei Zufallsvariablen $T$ und $D_n = D(S_n)$:

**Definition 4.1.** *$T$ sei eine zufällige gleichverteilte reelle Zahl aus dem Einheitsintervall $[0,1)$, und für eine Familie endlicher Mengen $(S_n)_{n=1}^{\infty}$ sei $D(S_n)$ eine zufällige gleichverteilte Zahl aus $S_n$ für $n \in \mathbb{N}$. Dabei schreiben wir $D_n = D(S_n)$ wann immer die Familie $(S_n)_n$ aus dem Kontext klar ist.*

Im Rest des Kapitels werden wir folgenden Satz beweisen:

**Satz 4.2.** *Sei $(S_n)_{n=1}^{\infty}$ eine Familie endlicher Mengen, $S_n \subset [0,1) \setminus \mathbb{Q}$, $(S_n)_n$ gleichverteilt mit Fehler $F(n)$. Dann gilt gleichmäßig in $m \in \mathbb{N}$ und für $k = k(n) \in \mathbb{N}$:*
*Falls $k = o\Big(\log\big(\frac{\#S_n}{F(n)}\big) / \log\log\big(\frac{\#S_n}{F(n)}\big)\Big)$ ist*

$$\big|\Pr[b_k(D_n) \le m] - \Pr[b_k(T) \le m]\big| = O\bigg(\Big(\frac{\#S_n}{F(n)}\Big)^{\varepsilon - \frac{1}{2}}\bigg)$$

*für $n \to \infty$ und jedes $\varepsilon > 0$.*
*Für konstantes $k$ gilt sogar*

$$\big|\Pr[b_k(D_n) \le m] - \Pr[b_k(T) \le m]\big| = O\bigg(\Big(\frac{\#S_n}{F(n)}\Big)^{-\frac{1}{2}} \log^{k-1}\Big(\frac{\#S_n}{F(n)}\Big)\bigg)$$

*für $n \to \infty$.*

Der obige Satz zeigt, dass die Verteilungen von $b_k(D_n)$ und $b_k(T)$ asymptotisch gleich sind für jede gleichverteilte Familie $(S_n)_n$ und gibt sogar explizite Fehlerschranken. Dabei mussten wir $S_n \subset [0,1) \setminus \mathbb{Q}$ fordern, damit $b_k(D_n)$ für alle $n$ definiert ist.

Die von der $O$-Notation versteckten Konstanten sind in beiden Fällen von $k$ abhängig. Dies bedeutet für den ersten Fall aber nicht, dass diese Konstante mit $k$ wächst, sondern, sobald wir eine Funktion $k(n)$ gewählt haben, die die Bedingung erfüllt, existiert eine absolute Konstante $C$, welche statt der $O$-Notation eingesetzt werden kann.

Insbesondere existiert nach Wahl von Konstanten $\varepsilon, \varepsilon', C' > 0$ für jedes

$$k = k(n) \leq C' \log\Big(\frac{\#S_n}{F(n)}\Big) / \Big(\log\log\Big(\frac{\#S_n}{F(n)}\Big)\Big)^{1+\varepsilon'} \tag{$*$}$$

eine Konstante $C = C_{\varepsilon,\varepsilon',C'}$, sodass die Differenz der Wahrscheinlichkeiten durch $C\big(\frac{\#S_n}{F(n)}\big)^{\varepsilon-\frac{1}{2}}$ absolut beschränkt ist. Wir erhalten also das folgende Resultat: Wählen wir uns ein $n \in \mathbb{N}$ und ein zufälliges Element von $S_n$, so kennen wir Abschätzungen über die Verteilung der ersten $k(n)$ Kettenbruchkoeffizienten mit $k(n)$ wie in $(*)$. Damit kennen wir die Verteilung der ersten $\log(n)/(\log\log(n))^{1+\varepsilon'}$ Kettenbruchkoeffizienten der Wurzel einer zufälligen Zahl $D \in M_n^U$.

In obiger Formulierung und im Rest dieser Arbeit benutzen wir $\Pr[A(T)]$ als Kurzschreibweise für $\Pr[A(T) \mid T \notin \mathbb{Q}]$ für ein von $T$ abhängiges Ereignis $A(T)$, da, wie in Kapitel 2 erläutert, $b_k(T)$ nur für $T \in \mathbb{R} \setminus \mathbb{Q}$ notwendig definiert ist. Dies ist möglich, da die Wahrscheinlichkeit bei Herausnehmen der Nullmenge $\mathbb{Q}$ nicht verändert wird, und es ist auch üblich.

Angewendet auf $M_n$, $M_n^U$, $Q_n$ und $Q_n^U$ erhalten wir mit Lemma 3.5 folgende Korollare:

**Korollar 4.3.** *Es gelten gleichmäßig in $m \in \mathbb{N}$ und für $k = k(n) \in \mathbb{N}$:*

*(i) Falls $k = o\big(\log(n)/\log\log(n)\big)$, ist*

$$\big|\Pr[b_k(D(M_n)) \leq m] - \Pr[b_k(T) \leq m]\big| = O(n^{\varepsilon-\frac{1}{2}})$$

*für $n \to \infty$ und jedes $\varepsilon > 0$.*

*Für konstantes $k$ gilt sogar*

$$\big|\Pr[b_k(D(M_n)) \leq m] - \Pr[b_k(T) \leq m]\big| = O(n^{-\frac{1}{2}} \log^{k-1}(n))$$

*für $n \to \infty$.*

*(ii) Falls $k = o\big(\log(n)/\log\log(n)\big)$, ist*

$$\big|\Pr[b_k(D(M_n^U)) \leq m] - \Pr[b_k(T) \leq m]\big| = O(n^{\varepsilon-\frac{1}{4}})$$

*für $n \to \infty$ und jedes $\varepsilon > 0$.*

*Für konstantes $k$ gilt sogar*

$$\big|\Pr[b_k(D(M_n)) \le m] - \Pr[b_k(T) \le m]\big| = O(n^{-\frac{1}{4}} \log^{k-1}(n))$$

*für $n \to \infty$.*

**Korollar 4.4.** *Es gelten gleichmäßig in $m \in \mathbb{N}$ und für $k = k(n) \in \mathbb{N}$:*

*(i) Für konstantes $k$ und $n \to \infty$ gelten*

$$\big|\Pr[b_k(D(Q_n)) \le m] - \Pr[b_k(T) \le m]\big| \to 0,$$
$$\big|\Pr[b_k(D(Q_n^U)) \le m] - \Pr[b_k(T) \le m]\big| \to 0.$$

*(ii) Unter der Riemann-Hypothese gilt für $k = o\big(\log(n)/\log\log(n)\big)$*

$$\big|\Pr[b_k(D(Q_n)) \le m] - \Pr[b_k(T) \le m]\big| = O(n^{\varepsilon - \frac{10}{27}})$$

*für $n \to \infty$ und jedes $\varepsilon > 0$.*

*(iii) Unter der Riemann-Hypothese gilt für $k = o\big(\log(n)/\log\log(n)\big)$*

$$\big|\Pr[b_k(D(Q_n^U)) \le m] - \Pr[b_k(T) \le m]\big| = O(n^{\varepsilon - \frac{5}{27}})$$

*für $n \to \infty$ und jedes $\varepsilon > 0$.*

Für $Q_n$ und $Q_n^U$ erhalten wir für konstantes $k$ keine bessere Schranke als für langsam wachsendes, da schon durch den Gleichverteilungsfehler dieser Mengen ein $\varepsilon$ im Exponenten hinzukommt.

## 4.2. Beweis für $k = 1$

Wir zeigen obigen Satz zuerst für $k = 1$, da dieser Spezialfall schnell bewiesen ist und der Fall $k \ge 2$ andere Hilfsmittel benötigt:

*Beweis von Satz 4.2 für $k = 1$.* Es ist für $T \in [0,1) \setminus \mathbb{Q}$: $b_1(T) = \lfloor T^{-1} \rfloor$ und dies ist genau dann kleiner gleich $m$, wenn $T > \frac{1}{m+1}$, also ist $\Pr[b_1(T) \le m] = 1 - \frac{1}{m+1}$. Zudem

ist

$$\begin{aligned}\Pr[b_1(D_n) \leq m] &= \frac{\#(S_n \cap (\frac{1}{m+1}, 1))}{\#S_n} \\ &= |(\frac{1}{m+1}, 1)| + O\Big(\frac{F(n)}{\#S_n}\Big) \\ &= \Pr[b_1(T) \leq m] + O\Big(\Big(\frac{F(n)}{\#S_n}\Big)^{\frac{1}{2}-\varepsilon}\Big),\end{aligned}$$

dito für $O\Big(\sqrt{\frac{F(n)}{\#S_n}} \log^{k-1}\big(\frac{\#S_n}{F(n)}\big)\Big)$. Dabei ist der Übergang zu einem kleineren Exponenten erlaubt, da $F(n) = o(\#S_n)$, also die Basis kleiner als 1 ist für $n$ groß genug. □

## 4.3. Beweis für $k > 1$

Um den Satz für $k > 1$ zu beweisen, benutzen wir folgende geometrische Intuition: Wir betrachten die Menge aller Zahlen im Einheitsintervall, die als $k$-ten Kettenbruchkoeffizienten eine Zahl kleiner gleich $m$ haben. Diese Menge ist als abzählbar unendliche Vereinigung von Intervallen darstellbar. Die Wahrscheinlichkeit, dass $b_k(T) \leq m$ gilt, ist gerade die Summe der Längen dieser Intervalle, da dies genau dann gilt, wenn $T$ in eines dieser Intervalle fällt. Die Wahrscheinlichkeit, dass $b_k(D_n) \leq m$ gilt, ist die Anzahl an Elementen von $S_n$, die in diese Intervalle fallen, geteilt durch $\#S_n$. Wir wollen zeigen, dass beide Wahrscheinlichkeiten ungefähr gleich sind.

Nach der Definition von Gleichverteilung wissen wir, dass in jedes einzelne Intervall genau so viele Elemente fallen, wie auch sollen, modulo einen Fehler von $F(n)$. Dies sagt allerdings nichts aus über eine Vereinigung abzählbar unendlich vieler Intervalle. Daher nehmen wir uns nun die größten dieser Intervalle heraus, also alle Intervalle, die länger als ein festes $\alpha \in (0, 1)$ sind. Dies sind nur endlich viele, sagen wir $M(\alpha)$ Intervalle. Der Fehler, den wir in diesen großen Intervallen machen, lässt sich durch $M(\alpha) \cdot F(n)$ abschätzen. Nun fehlt es noch, den Fehler auf den Intervallen der Länge $< \alpha$ abzuschätzen. Wie sich herausstellt, ist dies aber damit getan, die Wahrscheinlichkeit abzuschätzen, mit der $T$ in einem dieser kurzen Intervalle landet. Zusammen mit einer Abschätzung von $M(\alpha)$ und über $\alpha$ optimierend erhalten wir die Aussage des Satzes.

Um diesen Beweis zu formalisieren, benötigen wir zuerst einige Schreibweisen und Begriffe. Für $1 < k \in \mathbb{N}$ und ein $\underline{b} \in \mathbb{N}^{k-1}$ schreiben wir $\underline{b} = (b_1, \ldots, b_{k-1})$, sodass wir die Einträge von $\underline{b}$ als Kettenbruchkoeffizienten einer Zahl $x = [0; b_1, \ldots, b_{k-1}, \ldots]$ interpretieren können. Für ein $\underline{b} \in \mathbb{N}^{k-1}$ und $0 \leq i < k$ definieren wir $A_i(\underline{b})/B_i(\underline{b})$ als den $i$-ten Konvergenten einer Zahl der Form $[0; b_1, \ldots, b_{k-1}, \ldots]$, also $A_i(\underline{b})/B_i(\underline{b}) = [0; b_1, \ldots, b_i]$, $(A_i(\underline{b}), B_i(\underline{b})) = 1$. Ist $\underline{b} \in \mathbb{N}^{k-1}$ fest und aus dem Kontext klar, so schreiben wir auch $A_i = A_i(\underline{b})$ und $B_i = B_i(\underline{b})$.

Wir schreiben abkürzend $\underline{b}_{k-1}(x)$ für $(b_1(x), \ldots, b_{k-1}(x))$ und $x \in [0, 1) \setminus \mathbb{Q}$.

Nun definieren wir die folgenden Intervalle:

**Definition 4.5.** *Für $\underline{b} \in \mathbb{N}^{k-1}$ und $m \in \mathbb{N}$ definieren wir*

$$I_{\underline{b}} := \left\{ \frac{A_{k-1}t + A_{k-2}}{B_{k-1}t + B_{k-2}} \;\middle|\; t \in (1, \infty) \right\},$$
$$I_{\underline{b},m} := \left\{ \frac{A_{k-1}t + A_{k-2}}{B_{k-1}t + B_{k-2}} \;\middle|\; t \in (1, m+1) \right\}.$$

Dabei ist $A_{k-i}$ als $A_{k-i}(\underline{b})$ zu lesen, analog für $B_{k-i}$, $i = 1, 2$.

Aus Aussage (2.4) wird ersichtlich, dass das Intervall $I_{\underline{b}}$ die Menge aller Zahlen ist, deren Kettenbruchentwicklung die Form $[0; b_1, \ldots, b_{k-1}, \ldots]$ hat, mit beliebigen $\ell$-ten Koeffizienten für $\ell \geq k$. Es enthält auch endliche Kettenbrüche, aber jeder solche endliche Kettenbruch muss wenigstens $k$ Koeffizienten haben und falls er genau $k$ Koeffizienten hat, muss der $k$-te Koeffizient ungleich 1 sein, da sonst die in Kapitel 2 erwähnte Konvention verletzt ist.

Das Intervall $I_{\underline{b},m}$ hingegen ist die Menge aller Zahlen, deren Kettenbruchentwicklung die Form $[0; b_1, \ldots, b_{k-1}, b_k, \ldots]$ hat, mit beliebigen $\ell$-ten Koeffizienten für $\ell > k$ und einen $k$-ten Koeffizienten $b_k \leq m$. Es gilt wortwörtlich die gleiche Anmerkung zu endlichen Kettenbrüchen wie für $I_{\underline{b}}$.

Da jede reelle Zahl eine eindeutige Darstellung als Kettenbruch besitzt, sind die Intervalle $I_{\underline{b}}$, $\underline{b} \in \mathbb{N}^{k-1}$ paarweise überschneidungsfrei. Dasselbe gilt für die Intervalle $I_{\underline{b},m}$, $\underline{b} \in \mathbb{N}^{k-1}$, da $I_{\underline{b},m} \subsetneq I_{\underline{b}}$.

Zudem überdecken die Intervalle $I_{\underline{b}}$, $\underline{b} \in \mathbb{N}^{k-1}$ das Einheitsintervall, oder zumindest fast: Einige endliche Kettenbrüche werden nicht eingefangen. Um diese Aussage korrekt zu formulieren, führen wir eine Äquivalenzrelation $\cong$ auf Teilmengen von $[0, 1)$ ein: Für $A, B \subseteq [0, 1)$ sei $A \cong B :\Leftrightarrow A \cup \mathbb{Q} = B \cup \mathbb{Q}$, wenn also beide Mengen bis auf die endlichen Kettenbrüche übereinstimmen. Dann gilt, dass die Intervalle $I_{\underline{b}}$ das Einheitsintervall überdecken im Sinne von

$$\bigcup_{\underline{b} \in \mathbb{N}^{k-1}} I_{\underline{b}} \cong [0, 1). \tag{4.6}$$

Die Länge dieser Intervalle lässt sich leicht bestimmen:

**Lemma 4.7.** *Für $1 < k \in \mathbb{N}, \underline{b} \in \mathbb{N}^{k-1}$ und $m \in \mathbb{N}$ gelten*

$$|I_{\underline{b}}| = \frac{1}{B_{k-1}(B_{k-1} + B_{k-2})},$$
$$|I_{\underline{b},m}| = \frac{m}{(B_{k-1} + B_{k-2})((m+1)B_{k-1} + B_{k-2})}.$$

*Beweis.* Wir rechnen nach:

$$
\begin{aligned}
|I_{\underline{b}}| &= \Big|\frac{A_{k-1}+A_{k-2}}{B_{k-1}+B_{k-2}} - \frac{A_{k-1}}{B_{k-1}}\Big| \\
&= \Big|\frac{A_{k-2}B_{k-1} - A_{k-1}B_{k-2}}{B_{k-1}(B_{k-1}+B_{k-2})}\Big|
\end{aligned}
$$

Mit Aussage (2.5) erhalten wir also die erste Behauptung. Weiterhin gilt

$$
\begin{aligned}
|I_{\underline{b},m}| &= \Big|\frac{A_{k-1}+A_{k-2}}{B_{k-1}+B_{k-2}} - \frac{(m+1)A_{k-1}+A_{k-2}}{(m+1)B_{k-1}+B_{k-2}}\Big| \\
&= \Big|\frac{m(A_{k-2}B_{k-1} - A_{k-1}B_{k-2})}{(B_{k-1}+B_{k-2})((m+1)B_{k-1}+B_{k-2})}\Big|,
\end{aligned}
$$

also wiederum mit Aussage (2.5) die zweite Behauptung. □

Wie weiter oben skizziert wollen wir uns diejenigen Intervalle $I_{\underline{b},m}$ hernehmen, deren Länge größer als ein festes $\alpha \in [0,1]$ ist. Zu diesen definieren wir einige Begriffe:

**Definition 4.8.** *Wir setzen für* $1 < k \in \mathbb{N}$, $m \in \mathbb{N}$ *und* $\alpha \in [0,1]$

$$
\begin{aligned}
L(\alpha) &:= \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|\geq\alpha}} |I_{\underline{b},m}|, \\
M(\alpha) &:= \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|\geq\alpha}} 1, \\
R(\alpha) &:= \Pr[|I_{\underline{b}_{k-1}(T),m}| < \alpha] = \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|<\alpha}} |I_{\underline{b}}|.
\end{aligned}
$$

Dabei ist $L(\alpha)$ die Gesamtlänge der langen Intervalle, also der Intervalle $I_{\underline{b},m}$, $\underline{b} \in \mathbb{N}^{k-1}$ der Länge $\geq \alpha$. $M(\alpha)$ ist die Anzahl an langen Intervallen, also die Anzahl an Intervallen, über die wir in der Summe $L(\alpha)$ aufsummieren. Schließlich ist $R(\alpha)$ die Wahrscheinlichkeit, dass $T$ in der Obermenge $I_{\underline{b}}$ eines kurzen Intervalles landet, dass also $|I_{\underline{b}_{k-1}(T),m}| < \alpha$ gilt.

Da alle in $L(\alpha)$ aufsummierten Intervalle eine Länge $\geq \alpha$ haben und überschneidungsfrei sind, folgt sofort

$$
M(\alpha) \leq 1/\alpha. \tag{4.9}
$$

Später werden wir eine stärkere Ungleichung für $M(\alpha)$ beweisen.

Mit diesen Definitionen lässt sich nun $\Pr[b_k(T) \leq m]$ wie folgt abschätzen:

**Lemma 4.10.** *Für $1 < k \in \mathbb{N},\ m \in \mathbb{N}$ und $\alpha \in [0,1]$ gilt*

$$L(\alpha) \leq \Pr[b_k(T) \leq m] \leq L(\alpha) + R(\alpha).$$

*Beweis.* Es gilt genau dann $b_k(T) \leq m$, wenn $T$ in eines der Intervalle $I_{\underline{b},m},\ \underline{b} \in \mathbb{N}^{k-1}$ fällt. Also ist

$$\begin{aligned}\Pr[b_k(T) \leq m] &= \sum_{\underline{b} \in \mathbb{N}^{k-1}} |I_{\underline{b},m}| \\ &= \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ |I_{\underline{b},m}| \geq \alpha}} |I_{\underline{b},m}| + \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ |I_{\underline{b},m}| < \alpha}} |I_{\underline{b},m}|.\end{aligned}$$

Die erste Summe ist gerade $L(\alpha)$. Wegen $0 \leq |I_{\underline{b},m}| \leq |I_{\underline{b}}|$ ist die zweite Summe von unten durch 0 und von oben durch $R(\alpha)$ beschränkt. Es folgt die Behauptung. □

Für die Wahrscheinlichkeit $\Pr[b_k(D_n) \leq m]$ gelten ähnliche Ungleichungen wie für $\Pr[b_k(T) \leq m]$:

**Lemma 4.11.** *Für $n, k, m \in \mathbb{N},\ k > 1$ und $\alpha \in [0,1]$ gilt*

$$L(\alpha) - \frac{F(n)M(\alpha)}{\#S_n} \leq \Pr[b_k(D_n) \leq m] \leq L(\alpha) + R(\alpha) + \frac{F(n)(2M(\alpha)+1)}{\#S_n}.$$

*Beweis.* Es ist

$$\begin{aligned}\Pr[b_k(D_n) \leq m] &= \frac{1}{\#S_n} \sum_{\underline{b} \in \mathbb{N}^{k-1}} \#(S_n \cap I_{\underline{b},m}) \\ &\geq \frac{1}{\#S_n} \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ |I_{\underline{b},m}| \geq \alpha}} \#(S_n \cap I_{\underline{b},m}) \\ &\geq \frac{1}{\#S_n} \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ |I_{\underline{b},m}| \geq \alpha}} (|I_{\underline{b},m}| \cdot \#S_n - F(n)) \\ &= L(\alpha) - \frac{F(n)M(\alpha)}{\#S_n}.\end{aligned}$$

Nach oben schätzen wir ähnlich ab:

$$\begin{aligned}\Pr[b_k(D_n) \le m] &= \frac{1}{\#S_n} \sum_{\underline{b}\in\mathbb{N}^{k-1}} \#(S_n \cap I_{\underline{b},m}) \\ &\le \frac{1}{\#S_n}\Big( \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|\ge\alpha}} \#(S_n \cap I_{\underline{b},m}) + \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|<\alpha}} \#(S_n \cap I_{\underline{b}})\Big)\end{aligned}$$

Wegen Aussage (4.6) gilt aber

$$\bigcup_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|<\alpha}} I_{\underline{b}} \cong [0,1) \setminus \bigcup_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|\ge\alpha}} I_{\underline{b}}.$$

Daher lässt sich ersteres als Vereinigung von höchstens $M(\alpha)+1$ überschneidungsfreien Intervallen $J_1, \ldots, J_s$ schreiben modulo $\cong$, d.h. es gilt

$$\bigcup_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|<\alpha}} I_{\underline{b}} \cong \bigcup_{i=1}^{s} J_s.$$

Es gilt dann $\sum_{i=1}^{s} |J_i| = R(\alpha)$ und wir können wie folgt ersetzen (wobei wir $S_n \cap \mathbb{Q} = \emptyset$ benutzen):

$$\begin{aligned}\Pr[b_k(D_n) \le m] &\le \frac{1}{\#S_n}\Big( \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|\ge\alpha}} \#(S_n \cap I_{\underline{b},m}) + \sum_{i=1}^{s} \#(S_n \cap J_i)\Big) \\ &\le \frac{1}{\#S_n}\Big( \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|\ge\alpha}} (|I_{\underline{b},m}| \cdot \#S_n + F(n)) + \sum_{i=1}^{s} (|J_i| \cdot \#S_n + F(n))\Big) \\ &= L(\alpha) + R(\alpha) + \frac{F(n)(M(\alpha)+s)}{\#S_n} \\ &\le L(\alpha) + R(\alpha) + \frac{F(n)(2M(\alpha)+1)}{\#S_n}\end{aligned}$$

□

Aus den beiden vorangehenden Lemmata folgt direkt:

**Korollar 4.12.** *Für $n, k, m \in \mathbb{N},\ k > 1$ und $\alpha \in [0,1]$ gilt*

$$\big|\Pr[b_k(D_n) \le m] - \Pr[b_k(T) \le m]\big| \le R(\alpha) + \frac{F(n)(2M(\alpha)+1)}{\#S_n}.$$

An dieser Stelle wissen wir bereits, dass der Fehler $\big|\Pr[b_k(D) \le m] - \Pr[b_k(T) \le m]\big|$ gegen 0 geht für $n \to \infty$: Wählen wir $\alpha = \alpha(n) \to 0$ so, dass $M(\alpha) = o\big(\frac{\#S_n}{F(n)}\big)$ gilt, so geht der rechte Summand gegen 0, aber auch $R(\alpha)$, da $\alpha \to 0$.

Der Rest dieses Kapitels (sowie Kapitel 6) befasst sich also damit, effektive Abschätzungen des Fehlerterms herzuleiten. Dazu benötigen wir Schranken für $R(\alpha)$ und $M(\alpha)$. Der Übersicht halber skizzieren wir diesen letzten Teil des Beweises von Satz 4.2 im Folgenden nur und sparen dabei die Beweise der Lemmata aus, da diese recht lang und technisch werden. Zu finden sind diese Beweise in Kapitel 6.

Wegen Lemma 4.7 ist klar, dass die Länge eines Intervalls $I_{\underline{b}}$ eng zusammenhängt mit der Größe der Konvergenten $B_{k-1}$. Daher benötigen wir zuerst eine Abschätzung für letzteres, und zwar in der Art, dass nur sehr wenige Zahlen einen zu großen oder zu kleinen $k$-ten Konvergenten $B_k$ haben.

Der Hauptsatz der Metrischen Approximationstheorie besagt, dass es eine Konstante $B > 0$ gibt, sodass $B_k < e^{Bk}$ fast überall gilt, wenn $k$ gegen unendlich strebt. Dieser hilft uns nicht direkt weiter, da wir auch kleine $k$ zulassen wollen. Allerdings lässt sich aus dem Beweis dieses Satzes im Buch von Khintchine [Khi63, S. 75ff] leicht eine Schranke extrahieren, die genau aussagt, was wir wollen. Wir zitieren sie hier erweitert um eine analoge untere Schranke. In Kapitel 6 geben wir den Beweis dieser Schranke wieder:

**Lemma 4.13.** *Für alle $k \in \mathbb{N}$ und $\Delta \in \mathbb{R}$ mit $\Delta \ge (2e)^k$ gilt:*

$$\frac{2^{-2k-1}}{(k-1)!}\log^{k-1}(\Delta)\Delta^{-1} < \Pr[B_k(T) \ge \Delta] < \frac{k2^{2k}}{(k-1)!}\log^{k-1}(\Delta)\Delta^{-1}.$$

Mithilfe dieser Schranken können wir nun den Restterm $R(\alpha)$ relativ scharf nach unten und oben abschätzen. Wir erinnern daran, dass

$$R(\alpha) = \sum_{\substack{\underline{b}\in\mathbb{N}^{k-1} \\ |I_{\underline{b},m}|<\alpha}} |I_{\underline{b}}|.$$

Nun nutzen wir aus, dass ein Intervall $I_{\underline{b},m}$ nur kurz ist, wenn der Konvergent $B_{k-1}(\underline{b})$ groß ist. Die Wahrscheinlichkeit für letzteres, also das Maß aller Zahlen mit großem Konvergenten, können wir aber mit dem vorangegangenen Lemma abschätzen:

**Lemma 4.14.** *Für alle $2 \le k \in \mathbb{N}$ und $0 < \alpha \le \frac{1}{6}(2e)^{-2k}$ gilt*

$$\frac{2^{-3k}}{(k-1)!}\log^{k-1}(\alpha^{-1})\sqrt{\alpha} < R(\alpha) < \frac{\sqrt{6}\,k\,2^{k+1}}{(k-1)!}\log^{k-1}(\alpha^{-1})\sqrt{\alpha}.$$

Wir hatten in Aussage (4.9) schon eine triviale obere Schranke für $M(\alpha)$, nämlich durch $1/\alpha$. Diese ist aber recht schwach, wie folgendes Lemma zeigt, welches sich der beiden vorangegangenen bedient:

**Lemma 4.15.** *Für $2 \leq k \in \mathbb{N}$ und alle $\alpha \leq e^{-15(k-1)}$ gilt*

$$M(\alpha) \leq \lambda^k R(\alpha)^{-1} \log^{2k-2}(R(\alpha)^{-1}) + e^{15(k-1)},$$

*für ein $0 < \lambda \leq e^{9.1760}$.*

Diese Aussagen in der Hand können wir nun den Beweis des Satzes abschließen:

*Beweis von Satz 4.2 für $k \geq 2$.* Es ist nach Korollar 4.12 und Lemma 4.15 für $0 < \alpha \leq e^{-15(k-1)}$:

$$\begin{aligned}
&\big|\Pr[b_k(D_n) \leq m] - \Pr[b_k(T) \leq m]\big| \\
&\leq R(\alpha) + \frac{F(n)(2M(\alpha)+1)}{\#S_n} \\
&\leq R(\alpha) + 3\frac{F(n)}{\#S_n}(\lambda^k R(\alpha)^{-1} \log^{2k-2}(R(\alpha)^{-1}) + e^{15(k-1)})
\end{aligned}$$

Wir wollen nun $R(\alpha)$ durch $\sqrt{\frac{F(n)}{\#S_n}} \log^{k-1}\left(\frac{\#S_n}{F(n)}\right)$ ersetzen, um die rechte Seite asymptotisch zu minimieren. Es ist aber $R(\alpha)$ keine stetige Funktion, daher wird dieser Wert nicht notwendigerweise angenommen. Lemma 4.14 liefert aber Abschätzungen von $R(\alpha)$ nach unten und oben durch stetige, monoton wachsende Funktionen. Daher gilt, dass für jedes $0 \leq X \leq R(e^{-15(k-1)})$ ein $0 \leq \alpha \leq e^{-15(k-1)}$ existiert mit

$$X \leq R(\alpha) \leq \sqrt{6}k2^{4k+1}X.$$

Dabei ist $\sqrt{6}k2^{4k+1}$ der Quotient der Vorfaktoren der oberen und unteren Abschätzung von $R(\alpha)$. Setzen wir $X := \sqrt{\frac{F(n)}{\#S_n}} \log^{k-1}\left(\frac{\#S_n}{F(n)}\right)$, so erhalten wir also

$$\begin{aligned}
&\big|\Pr[b_k(D_n) \leq m] - \Pr[b_k(T) \leq m]\big| \\
&\leq \left(\sqrt{6}k2^{4k+1} + 3\lambda^k \frac{\log^{2k-2}\left(\sqrt{\frac{F(n)}{\#S_n}} \log^{k-1}\left(\frac{\#S_n}{F(n)}\right)\right)}{\log^{2k-2}\left(\frac{\#S_n}{F(n)}\right)}\right) \\
&\qquad \cdot \sqrt{\frac{F(n)}{\#S_n}} \log^{k-1}\left(\frac{\#S_n}{F(n)}\right) + 3e^{15(k-1)}\frac{F(n)}{\#S_n},
\end{aligned}$$

falls $X \leq R(e^{-15(k-1)})$. Dann ist allerdings auch $X \leq 1$, also können wir den auftretenden Quotienten durch $(1/2)^{2k-2}$ nach oben abschätzen. Es entsteht

$$\begin{aligned}&\big|\Pr[b_k(D_n) \le m] - \Pr[b_k(T) \le m]\big| \\ &\le (\sqrt{6}k2^{4k+1} + 3\lambda^k 2^{2-2k})\sqrt{\frac{F(n)}{\#S_n}}\log^{k-1}\Big(\frac{\#S_n}{F(n)}\Big) + 3e^{15(k-1)}\frac{F(n)}{\#S_n},\end{aligned}$$

Wir können $R(e^{-15(k-1)})$ wie folgt nach unten abschätzen, wiederum Lemma 4.14 benutzend:

$$\begin{aligned}R(e^{-15(k-1)}) &\ge \frac{2^{-3k}}{(k-1)!}\log^{k-1}(e^{15(k-1)})\sqrt{e^{-15(k-1)}} \\ &\ge 2^{-3k}15^{k-1}e^{-15(k-1)/2}.\end{aligned}$$

Die Bedingung $X \le R(e^{-15(k-1)})$ ist also erfüllt, falls

$$\sqrt{\frac{F(n)}{\#S_n}}\log^{k-1}\big(\frac{\#S_n}{F(n)}\big) \le 2^{-3k}15^{k-1}e^{-15(k-1)/2},$$

oder, äquivalent,

$$k-1 \le \frac{\frac{1}{2}\log\big(\frac{\#S_n}{F(n)}\big) - 3\log(2)}{\log\log\big(\frac{\#S_n}{F(n)}\big) + \log(2^3e^{15/2}/15)}.$$

Für $k = o\Big(\log\big(\frac{\#S_n}{F(n)}\big)/\log\log\big(\frac{\#S_n}{F(n)}\big)\Big)$ ist also

$$\big|\Pr[b_k(D_n) \le m] - \Pr[b_k(T) \le m]\big| = O\bigg(\Big(\frac{F(n)}{\#S_n}\Big)^{\frac{1}{2}-\varepsilon}\bigg)$$

für $n \to \infty$ und jedes $\varepsilon > 0$.
Für konstantes $k$ gilt sogar

$$\big|\Pr[b_k(D_n) \le m] - \Pr[b_k(T) \le m]\big| = O\bigg(\sqrt{\frac{F(n)}{\#S_n}}\log^{k-1}\Big(\frac{\#S_n}{F(n)}\Big)\bigg)$$

für $n \to \infty$. □

# 5 Untere Schranken

In diesem Kapitel werden wir untere Abschätzungen für den Fehler in Korollar 4.3 zeigen, also für die Fehler

$$\big|\Pr[b_k(D(M_n)) \le m] - \Pr[b_k(T) \le m]\big| \text{ sowie}$$
$$\big|\Pr[b_k(D(M_n^U)) \le m] - \Pr[b_k(T) \le m]\big|.$$

Diese Schranken werden weit davon entfernt sein, unseren oberen Schranken zu entsprechen, sind aber von eigenständigem Interesse.

Dazu betrachten wir Kettenbrüche der Form

$$x = [n; \overline{\frac{2n}{k}, 2n}]$$

mit $n, k \in \mathbb{N},\ k|2n$. Nach Kapitel 2 handelt es sich um quadratische Irrationalzahlen, also um Zahlen der Form $\frac{a+\sqrt{b}}{c},\ a, b, c \in \mathbb{Z}, b > 0, c \neq 0$. Genauer gilt für $y := [\overline{\frac{2n}{k}, 2n}]$

$$y = \frac{2n}{k} + \frac{1}{2n + \frac{1}{y}},$$

nach kurzem Rechnen erhalten wir also

$$y = \frac{n + \sqrt{n^2 + k}}{k}.$$

Wegen $x = n + \frac{1}{y}$ rechnen wir sofort nach, dass

$$x = \sqrt{n^2 + k}.$$

Wurzeln von dieser Form haben also Periodenlänge 2 wann immer $k|2n$. Insbesondere haben diese Wurzeln sehr große $k$-te Kettenbruchkoeffizienten für gerade $k \in \mathbb{N}$, denn diese Koeffizienten sind alle $2n$.

Bezeichne $\sigma_0(n)$ die Anzahl an Teilern einer natürlichen Zahl $n$. Dann gibt es $\sigma_0(2n)$ viele $k \in \mathbb{N}$, für die $\sqrt{n^2 + k}$ einen großen $k$-ten Koeffizienten hat.

Es gilt also für gerades $k \in \mathbb{N}$

$$\Pr[b_k(D(M_n)) = 2n] \geq \frac{\sigma_0(2n)}{2n} \geq \frac{1}{2} \cdot \frac{\sigma_0(n)}{n}. \tag{5.1}$$

Die Funktion $\log(\sigma_0(n))$ hat aber als Maximalordnung $\log 2 \frac{\log n}{\log \log n}$ (für einen Beweis, siehe [HW58, Satz 317]), daher existiert für jedes $\varepsilon > 0$ und $N \in \mathbb{N}$ ein $n \geq N$ mit

$$\begin{aligned} \log(\sigma_0(n)) &\geq (1-\varepsilon) \log 2 \frac{\log n}{\log \log n}, \text{ also} \\ \sigma_0(n) &\geq n^{\frac{(1-\varepsilon)\log 2}{\log \log n}}. \end{aligned}$$

Es existieren also unendlich viele $n \in \mathbb{N}$ mit

$$\Pr[b_k(D(M_n)) = 2n] \geq \frac{1}{2} \cdot \frac{n^{\frac{(1-\varepsilon)\log 2}{\log \log n}}}{n}. \tag{5.2}$$

Durch aufsummieren von (5.1) leiten wir sofort eine untere Schranke für $M_N^U$ her, für $N = (n+1)^2,\ n \in \mathbb{N}$:

$$\Pr[b_k(D(M^U_{(n+1)^2})) \geq n] \geq \frac{1}{(n+1)^2} \sum_{i=\lceil n/2 \rceil}^{n} \sigma_0(2i) \geq \frac{1}{(n+1)^2} \sum_{i=\lceil n/2 \rceil}^{n} \sigma_0(i). \tag{5.3}$$

Es ist aber bekanntermaßen $\sum_{i=1}^{n} \sigma_0(i) = n \log n + O(n)$, (eine noch stärkere Aussage findet sich in [HW58, Satz 320]) also ist

$$\begin{aligned} \Pr[b_k(D(M^U_{(n+1)^2})) \geq n] &\geq \frac{1}{(n+1)^2} \Big( n \log(n) - \left\lceil \frac{n}{2} \right\rceil \log \left( \left\lceil \frac{n}{2} \right\rceil \right) + O(n) \Big) \\ &\geq \frac{1}{(n+1)^2} \Big( \frac{n}{2} \log(n) + O(n) \Big) \\ &= \frac{\log(n)}{2n} + O\Big(\frac{1}{n}\Big). \end{aligned}$$

Es existieren also für jedes gerade $k \in \mathbb{N}$ unendlich viele $N \in \mathbb{N}$ mit

$$\Pr[b_k(D(M_N^U)) \geq \sqrt{N}] \geq \frac{\log(N)}{4\sqrt{N}} + O\Big(\frac{1}{\sqrt{N}}\Big). \tag{5.4}$$

Auf der anderen Seite ist

$$\begin{aligned}\Pr[b_k(T) \le m] &= \sum_{\underline{b}\in\mathbb{N}^{k-1}} |I_{\underline{b},m}| \\ &= \sum_{\underline{b}\in\mathbb{N}^{k-1}} |I_{\underline{b}}| \frac{mB_{k-1}(B_{k-1}+B_{k-2})}{(B_{k-1}+B_{k-2})((m+1)B_{k-1}+B_{k-2})} \\ &= \sum_{\underline{b}\in\mathbb{N}^{k-1}} |I_{\underline{b}}| \frac{mB_{k-1}}{(m+1)B_{k-1}+B_{k-2}}.\end{aligned}$$

Dabei haben wir Lemma 4.7 benutzt, um die Länge von $|I_{\underline{b},m}|$ mit der von $|I_{\underline{b}}|$ zu vergleichen. In obigen Summen steht $B_{k-i}$ für den von $\underline{b}$ induzierten $(k-i)$-ten Konvergenten. Da $0 \le B_{k-2} \le B_{k-1}$ ist, liegt der Quotient auf der rechten Seite zwischen $\frac{m}{m+2}$ und $\frac{m}{m+1}$. Die Intervalle $I_{\underline{b}}$ überdecken aber das Einheitsintervall, also gilt

$$\sum_{\underline{b}\in\mathbb{N}^{k-1}} |I_{\underline{b}}| = 1.$$

Daher bekommen wir eine Abschätzung von $\Pr[b_k(T) \le m]$ durch

$$\frac{m}{m+2} \le \Pr[b_k(T) \le m] \le \frac{m}{m+1},$$

oder, äquivalent,

$$\frac{2}{m+1} \ge \Pr[b_k(T) \ge m] \ge \frac{1}{m}. \tag{5.5}$$

Kombination von (5.2), (5.4) und (5.5) liefert nun den folgenden Satz:

**Satz 5.6.** *Für gerade $k \in \mathbb{N}$ und unendliche viele $n \in \mathbb{N}$ gelten*

$$\begin{aligned}\big|\Pr[b_k(D(M_n)) \ge 2n] - \Pr[b_k(T) \ge 2n]\big| &\ge \frac{1}{2}\cdot\frac{n^{\frac{(1-\varepsilon)\log 2}{\log\log n}}}{n} + O\Big(\frac{1}{n}\Big) \quad \textit{und} \\ \big|\Pr[b_k(D(M_n^U)) \ge \sqrt{n}] - \Pr[b_k(T) \ge \sqrt{n}]\big| &\ge \frac{\log(n)}{4\sqrt{n}} + O\Big(\frac{1}{\sqrt{n}}\Big).\end{aligned}$$

Dies bedeutet, dass man in Korollar 4.3 die Fehler nicht durch $O\Big(\frac{n^{\frac{(1-\varepsilon)\log 2}{\log\log n}}}{n}\Big)$ bzw. $o\big(\frac{\log(n)}{\sqrt{n}}\big)$ ersetzen kann (für alle $\varepsilon > 0$).

# 6 Beweise der Lemmata

Es folgen die in Kapitel 4 ausgelassenen Beweise einiger Lemmata.

## 6.1. Lemma 4.13

*Beweis von Lemma 4.13.* (i) Für $k = 1$ gilt die Abschätzung trivialerweise, denn es ist für $T \in [0,1) \setminus \mathbb{Q}:\ B_k(T) = b_1(T) = \lfloor T^{-1} \rfloor$, also

$$\Pr[B_k(T) \geq \Delta] = \Pr[\lfloor T^{-1} \rfloor \geq \lceil \Delta \rceil] = \Pr[T < 1/(\lceil \Delta \rceil - 1)] = 1/(\lceil \Delta \rceil - 1)$$

und dies liegt für alle $\Delta \geq 2e$ in den angegebenen Schranken.

(ii) Für $k \geq 2$ ergibt sich aus der Berechnungsvorschrift (2.1) für die $B_i$

$$b_i B_{i-1} \leq B_i \leq 2 b_i B_{i-1}.$$

also induktiv

$$\prod_{i=1}^{k} b_i \leq B_k \leq 2^k \prod_{i=1}^{k} b_i.$$

Zudem ist $B_1 = b_1 B_0 + B_{-1} = b_1 \cdot 1 + 0 < 2b_1$ und $B_2 = b_2 B_1 + B_0 = b_2 B_1 + 1 > b_2 B_1$, also gilt in beide Richtungen an mindestens einer Stelle die Ungleichheit. Es folgt

$$\prod_{i=1}^{k} b_i < B_k < 2^k \prod_{i=1}^{k} b_i.$$

(iii) Ein Interval $I_{\underline{b}}$, für $\underline{b} \in \mathbb{N}^k$, in dem $B_k \geq \Delta$ gilt, hat eine Länge von

$$|I_{\underline{b}}| = \frac{1}{B_k(B_k + B_{k-1})}$$

nach Lemma (4.7). Mit $0 \leq B_{k-1} \leq B_k$ erhalten wir

$$\frac{1}{2^{k+1}(b_1 b_2 \cdots b_k)^2} < \frac{1}{2B_k^2} \leq |I_{\underline{b}}| \leq \frac{1}{B_k^2} < \frac{1}{(b_1 b_2 \cdots b_k)^2}.$$

Dies erlaubt uns schon, die Wahrscheinlichkeit $\Pr[B_k(T) \geq \Delta]$ abzuschätzen durch

$$\Pr[B_k(T) \geq \Delta] = \sum_{\substack{\underline{b} \in \mathbb{N}^k \\ B_k(\underline{b}) \geq \Delta}} |I_{\underline{b}}| < \sum_{\substack{\underline{b} \in \mathbb{N}^k \\ 2^k b_1 b_2 \cdots b_k \geq \Delta}} \frac{1}{(b_1 b_2 \cdots b_k)^2}$$

und analog

$$\Pr[B_k(T) \geq \Delta] > \sum_{\substack{\underline{b} \in \mathbb{N}^k \\ b_1 b_2 \cdots b_k \geq \Delta}} \frac{1}{2^{k+1}(b_1 b_2 \cdots b_k)^2}.$$

(iv) Um diese Summen abzuschätzen bemerken wir, dass

$$\begin{aligned}
\prod_{i=1}^{k} \frac{1}{b_i^2} &= \prod_{i=1}^{k} \Big(1 + \frac{1}{b_i}\Big) \frac{1}{b_i(b_i+1)} \\
&\leq 2^k \prod_{i=1}^{k} \frac{1}{b_i(b_i+1)} \\
&= 2^k \prod_{i=1}^{k} \int_{b_i}^{b_i+1} \frac{dx_i}{x_i^2} \\
&= 2^k \int_{a_1}^{a_1+1} \int_{a_2}^{a_2+1} \cdots \int_{a_k}^{a_k+1} \frac{dx_1 dx_2 \cdots dx_k}{x_1^2 x_2^2 \cdots x_k^2}.
\end{aligned}$$

Andererseits gilt nach analogen Schlüssen klar

$$\prod_{i=1}^{k} \frac{1}{b_i^2} \geq \int_{a_1}^{a_1+1} \int_{a_2}^{a_2+1} \cdots \int_{a_k}^{a_k+1} \frac{dx_1 dx_2 \cdots dx_k}{x_1^2 x_2^2 \cdots x_k^2}.$$

Demnach ist

$$\sum_{\substack{\underline{b} \in \mathbb{N}^k \\ b_1 b_2 \cdots b_k \geq 2^{-k}\Delta}} \frac{1}{(b_1 b_2 \cdots b_k)^2} \leq 2^k J_k(2^{-k}\Delta),$$

wobei $J_k(g)$ für $g \in \mathbb{R}$ das $k$-fache Integral

$$\int \int \cdots \int \frac{dx_1 dx_2 \cdots dx_k}{x_1^2 x_2^2 \cdots x_k^2}$$

über die Region

$$\begin{aligned} &x_i \geq 1 \ (i = 1, \ldots, k) \\ &x_1 x_2 \cdots x_k \geq g \end{aligned}$$

steht. Andererseits ist

$$\sum_{\substack{\underline{b} \in \mathbb{N}^k \\ b_1 b_2 \cdots b_k \geq \Delta}} \frac{1}{2^{k+1}(b_1 b_2 \cdots b_k)^2} \geq 2^{-k-1} J'_k(\Delta),$$

wobei $J'_k(g)$ für $g \in \mathbb{R}$ das $k$-fache Integral

$$\int \int \cdots \int \frac{dx_1 dx_2 \cdots dx_k}{x_1^2 x_2^2 \cdots x_k^2}$$

über die Region

$$\begin{aligned} &x_i \geq 1 (i = 1, \ldots, k) \\ &(x_1 - 1)(x_2 - 1) \cdots (x_k - 1) \geq g \end{aligned}$$

ist. Wir schränken diese Region weiter ein, indem wir fordern:

$$\begin{aligned} &x_i \geq 2 \ (i = 1, \ldots, k) \\ &x_1 x_2 \cdots x_k \geq 2^k g \end{aligned}$$

Eine Variablensubstitution $x'_i = x_i/2$ $(i = 1, \ldots, k)$ liefert uns nun das Integral $J_k(g)$ (auch über die gleiche Region!) versehen mit einem Faktor $2^{-k}$, also

$$\sum_{\substack{\underline{b} \in \mathbb{N}^k \\ b_1 b_2 \cdots b_k \geq \Delta}} \frac{1}{2^{k+1}(b_1 b_2 \cdots b_k)^2} \geq 2^{-2k-1} J_k(\Delta),$$

(v) Für $g \leq 1$ wird die Region von $J_k(g)$ zur Region $1 \leq x_i < \infty$ $(i = 1, \ldots, k)$ und wir erhalten

$$J_k(g) = \Big[\int_1^\infty \frac{dx}{x^2}\Big]^k = 1.$$

(vi) Wir zeigen nun induktiv, dass für $g > 1$ gilt:

$$J_k(g) = \frac{1}{g}\sum_{i=0}^{k-1}\frac{\log^i(g)}{i!}.$$

Tatsächlich gilt für $k = 1$:

$$\int_g^\infty \frac{dx}{x^2} = \frac{1}{g}.$$

Nehmen wir nun an, die Gleichung gelte für ein $k \in \mathbb{N}$. Dann gilt auch

$$\begin{aligned} J_{k+1}(g) &= \int_1^\infty \frac{dx_{k+1}}{x_{k+1}^2} J_k\Big(\frac{g}{x_{k+1}}\Big) \\ &= \frac{1}{g}\int_0^g J_k(u)du \\ &= \frac{1}{g}\Big[\int_0^1 J_k(u)du + \int_1^g J_k(u)du\Big]. \end{aligned}$$

Ersetzen wir nun das erste Integral mittels der Gleichung aus (v) und das zweite mittels der Induktionsvoraussetzung, so erhalten wir

$$\begin{aligned} J_{k+1}(g) &= \frac{1}{g}\Big[1 + \sum_{i=0}^{k-1}\frac{\log^{i+1}(g)}{(i+1)!}\Big] \\ &= \frac{1}{g}\sum_{i=0}^{k}\frac{\log^i(g)}{i!}. \end{aligned}$$

(vii) Einsetzen von (vi) in die obere Abschätzung aus (iv) liefert nun

$$\Pr[B_k(T) \geq \Delta] < 2^k J_k(2^{-k}\Delta) = \frac{4^k}{\Delta}\sum_{i=0}^{k-1}\frac{\log^i(2^{-k}\Delta)}{i!}.$$

Wegen $\Delta \geq (2e)^k$, also $\log(2^{-k}\Delta) \geq k$ sieht man leicht, dass jeder Term in obiger Summe kleiner oder gleich $\frac{\log^{k-1}(2^{-k}\Delta)}{(k-1)!}$ ist, denn für $a \geq 1$ ist $\frac{(ak)^{k-1}}{(k-1)!}$ maximal unter $\frac{(ak)^0}{0!}, \frac{(ak)^1}{1!}, \ldots, \frac{(ak)^{k-1}}{(k-1)!}$. Damit bekommen wir

$$\Pr[B_k(T) \geq \Delta] < \frac{4^k}{\Delta} k \frac{\log^{k-1}(2^{-k}\Delta)}{(k-1)!} \leq \frac{k4^k}{(k-1)!} \log^{k-1}(\Delta)\Delta^{-1}.$$

Andererseits erhalten wir für die untere Schranke

$$\begin{aligned}\Pr[B_k(T) \geq \Delta] &> 2^{-2k-1} J_k(\Delta) \\ &= \frac{2^{-2k-1}}{\Delta} \sum_{i=0}^{k-1} \frac{\log^i(\Delta)}{i!} \\ &\geq \frac{2^{-2k-1}}{\Delta} \frac{\log^{k-1}(\Delta)}{(k-1)!}.\end{aligned}$$

□

## 6.2. Lemma 4.14

*Beweis von Lemma 4.14.* Es ist nach Definition

$$R(\alpha) = \Pr[|I_{\underline{b}_{k-1}(T),m}| < \alpha].$$

Mit Lemma 4.7 erhalten wir

$$R(\alpha) = \Pr\Big[\Big|\frac{m}{(B_{k-1}(T) + B_{k-2}(T))((m+1)B_{k-1}(T) + B_{k-2}(T))}\Big| < \alpha\Big]. \qquad (*)$$

Nun liefert $B_{k-2}(T) \leq B_{k-1}(T)$:

$$\begin{aligned}R(\alpha) &\leq \Pr[\frac{m}{2(m+2)} \frac{1}{B_{k-1}(T)^2} < \alpha] \\ &\leq \Pr[\frac{1}{6} \frac{1}{B_{k-1}(T)^2} < \alpha] \\ &= \Pr[B_{k-1}(T) > (6\alpha)^{-1/2}] \\ &< \frac{k2^{2k}}{(k-1)!} \log^{k-1}((6\alpha)^{-1/2})\sqrt{6\alpha} \\ &\leq \frac{\sqrt{6}\, k\, 2^{k+1}}{(k-1)!} \log^{k-1}(\alpha^{-1})\sqrt{\alpha}\end{aligned}$$

wobei wir Lemma 4.13 genutzt haben. Dabei muss $(6\alpha)^{-1/2} \geq (2e)^k$ gelten, damit wir dieses Lemma verwenden können.

Andersherum bekommen wir aus $(*)$

$$\begin{aligned} R(\alpha) &\geq \Pr[\frac{1}{B_{k-1}(T)^2} < \alpha] \\ &= \Pr[B_{k-1}(T) > \alpha^{-1/2}] \\ &> \frac{2^{-2k-1}}{(k-1)!} \log^{k-1}(\alpha^{-1/2})\sqrt{\alpha} \\ &= \frac{2^{-3k}}{(k-1)!} \log^{k-1}(\alpha^{-1})\sqrt{\alpha} \end{aligned}$$

unter der Bedingung $\alpha^{-1/2} \geq (2e)^k$. Beide Bedingungen sind erfüllt, falls $\alpha \leq \frac{1}{6}(2e)^{-2k}$. □

## 6.3. Lemma 4.15

*Beweis von Lemma 4.15.* (i) Es ist für $0 < \alpha_a \leq \alpha_e \leq 1$

$$M(\alpha_a) - M(\alpha_e) = \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ \alpha_e > |I_{\underline{b},m}| \geq \alpha_a}} 1,$$

weswegen wir eine obere Abschätzung bekommen:

$$\begin{aligned} M(\alpha_a) - M(\alpha_e) \leq \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ \alpha_e > |I_{\underline{b},m}| \geq \alpha_a}} \frac{|I_{\underline{b},m}|}{\alpha_a} &\leq \sum_{\substack{\underline{b} \in \mathbb{N}^{k-1} \\ \alpha_e > |I_{\underline{b},m}| \geq \alpha_a}} \frac{|I_{\underline{b}}|}{\alpha_a} \\ &= \frac{1}{\alpha_a}(R(\alpha_e) - R(\alpha_a)), \end{aligned}$$

da $I_{\underline{b},m} \subseteq I_{\underline{b}}$.
Dann gilt aber auch für $\alpha_a = \alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n = \alpha_e$:

$$\begin{aligned} M(\alpha_a) - M(\alpha_e) &= \sum_{i=1}^{n-1} (M(\alpha_i) - M(\alpha_{i+1})) \\ &\leq \sum_{i=1}^{n-1} \frac{1}{\alpha_i} (R(\alpha_{i+1}) - R(\alpha_i)) \\ &= \sum_{i=1}^{n-1} \frac{1}{\alpha_i} (y_{i+1} - y_i) \end{aligned}$$

mit $y_i := R(\alpha_i), i = 1, \ldots, n$.

(ii) Nun ist aber nach Lemma 4.14 für $0 < \alpha \leq \frac{1}{6}(2e)^{-2k}$

$$R(\alpha) < \gamma \log^{k-1}(\alpha^{-1})\sqrt{\alpha} =: f(\alpha) \text{ mit } \gamma := \frac{\sqrt{6}\, k\, 2^{k+1}}{(k-1)!}.$$

Dabei ist $f(\alpha)$ für $0 < \alpha < e^{2-2k}$ eine streng monoton wachsende Funktion, denn wir rechnen nach, dass

$$\frac{d}{d\alpha}[\log^{k-1}(\alpha^{-1})\sqrt{\alpha}] = \log^{k-2}(\alpha^{-1})(2 - 2k - \log(\alpha))/(2\sqrt{\alpha}),$$

und dies ist positiv, falls $\alpha < e^{2-2k}$. Also existiert eine eindeutige Umkehrfunktion

$$f^{-1} : (0, f(e^{2-2k})] \to (0, e^{2-2k}]$$

von $f$ und es gilt dann für $\alpha \leq \frac{1}{6}(2e)^{-2k},\ y = R(\alpha)$

$$f^{-1}(y) \leq \alpha.$$

Also folgern wir mit (i) für $\alpha_e \leq \frac{1}{6}(2e)^{-2k}$

$$M(\alpha_a) - M(\alpha_e) \leq \sum_{i=1}^{n-1} \frac{1}{f^{-1}(y_i)} (y_{i+1} - y_i).$$

(iii) Wir schreiben abkürzend $f^*(y) := (f^{-1}(y))^{-1}$ für $y \in (0, f(e^{2-2k}))$. Dann gilt nach Definition von $f$:

$$\begin{aligned} y &= \gamma \log^{k-1}((f^{-1}(y))^{-1})\sqrt{(f^{-1}(y))} \\ &= \gamma \log^{k-1}(f^*(y))/\sqrt{(f^*(y))} \end{aligned}$$

Nach Umformen erhalten wir also die Gleichung

$$f^*(y) = \gamma^2 \log^{2k-2}(f^*(y))/y^2. \tag{6.1}$$

(iv) Um dies weiter abzuschätzen benutzen wir nun folgendes: Für $m \in \mathbb{N}, x > 0$ und $1 < c < e$ gilt

$$\frac{e^x}{x^m} \geq e^{m(1-\log c)}\Big(\frac{\log c}{m}\Big)^m e^{x/c}, \tag{6.2}$$

denn es ist:

$$\frac{d}{di}\frac{c^i}{(i+m)^m} = \frac{c^i}{(i+m)^{m+1}}((i+m)\log(c) - m),$$

also offenbart sich ein Tiefpunkt an $i = m(\frac{1}{\log c} - 1)$. Demnach ist

$$\frac{c^i i!}{(i+m)!} \geq \frac{c^i}{(i+m)^m} \geq \frac{c^{m(\frac{1}{\log c}-1)}}{(m(\frac{1}{\log c}-1)+m)^m} = e^{m(1-\log c)}\Big(\frac{\log c}{m}\Big)^m.$$

Es ist aber

$$\begin{aligned} \frac{e^x}{x^m} &\geq \sum_{i=0}^{\infty} \frac{x^i}{(i+m)!} \\ &\geq \sum_{i=0}^{\infty} e^{m(1-\log c)}\Big(\frac{\log c}{m}\Big)^m \frac{x^i}{c^i i!} \\ &= e^{m(1-\log c)}\Big(\frac{\log c}{m}\Big)^m e^{x/c}. \end{aligned}$$

(v) Setzen wir in (6.2) $x = \log f^*(y)$, $m = 2k-2$, so ist wegen $f^*(y) \geq e^{2k-2}$ und $k \geq 2$ tatsächlich $x = \log f^*(y) > 0$. Wir erhalten für $1 < c < e$

$$\frac{f^*(y)}{\log^{2k-2} f^*(y)} \geq e^{(2k-2)(1-\log c)}\Big(\frac{\log c}{2k-2}\Big)^{2k-2}(f^*(y))^{1/c}.$$

Wegen Gleichung (6.1) ist die linke Seite aber gerade $\gamma^2/y^2$. Umformen führt zu

$$f^*(y) \leq \left( e^{(2k-2)(\log(c)-1)} \left( \frac{2k-2}{\log c} \right)^{2k-2} \frac{\gamma^2}{y^2} \right)^c.$$

(vi) Es gilt nun also mit (3) und (6):

$$M(\alpha_a) - M(\alpha_e) \leq \sum_{i=1}^{n-1} \left( e^{(2k-2)(\log(c)-1)} \left( \frac{2k-2}{\log c} \right)^{2k-2} \frac{\gamma^2}{y_i^2} \right)^c (y_{i+1} - y_i),$$

also gilt nach dem Grenzübergang $n \to \infty$, da die rechte Seite Riemann-integrierbar ist:

$$\begin{aligned} M(\alpha_a) - M(\alpha_e) &\leq \int_{R(\alpha_a)}^{R(\alpha_e)} \left( e^{(2k-2)(\log(c)-1)} \left( \frac{2k-2}{\log c} \right)^{2k-2} \frac{\gamma^2}{y^2} \right)^c dy \\ &= \left[ \left( e^{(2k-2)(\log(c)-1)} \left( \frac{2k-2}{\log c} \right)^{2k-2} \gamma^2 \right)^c \frac{y^{1-2c}}{1-2c} \right]_{R(\alpha_a)}^{R(\alpha_e)} \\ &\leq \left( e^{(2k-2)(\log(c)-1)} \left( \frac{2k-2}{\log c} \right)^{2k-2} \gamma^2 \right)^c \frac{R(\alpha_a)^{1-2c}}{2c-1} \end{aligned}$$

Wir setzen nun $c := 1 + \delta \frac{\log(R(\alpha_e)^{-1})}{\log(R(\alpha_a)^{-1})}$. Dann ist $1 < c \leq 1 + \delta$, also

$$\delta \geq c - 1 \geq \log(c) \geq \log(1+\delta)(c-1)/\delta = \log(1+\delta) \frac{\log(R(\alpha_e)^{-1})}{\log(R(\alpha_a)^{-1})}.$$

Wir können also abschätzen

$$\begin{aligned} &M(\alpha_a) - M(\alpha_e) \\ &\leq \left( e^{(2k-2)(\delta-1)} \left( \frac{(2k-2)\log(R(\alpha_a)^{-1})}{\log(1+\delta)\log(R(\alpha_e)^{-1})} \right)^{2k-2} \gamma^2 \right)^c \cdot \\ &\quad R(\alpha_a)^{-1} R(\alpha_e)^{-2\delta} \\ &\leq \left( e^{(2k-2)(\delta-1)} \left( \frac{(2k-2)}{\log(1+\delta)\log(R(\alpha_e)^{-1})} \right)^{2k-2} \gamma^2 \right)^{1+\delta} \cdot \\ &\quad R(\alpha_a)^{-1} R(\alpha_e)^{-2\delta} \log(R(\alpha_a)^{-1})^{(2k-2)(1+\delta\frac{\log(R(\alpha_e)^{-1})}{\log(R(\alpha_a)^{-1})})}, \end{aligned}$$

und wegen $\log(\log(x))/\log(x) \leq e^{-1}$, also $\log(x)^{1/\log(x)} \leq e^{1/e}$ für $x > 1$ gilt

$$
\begin{aligned}
&M(\alpha_a) - M(\alpha_e) \\
&\leq \left( e^{(2k-2)(\delta-1)} \Big( \frac{(2k-2)}{\log(1+\delta)\log(R(\alpha_e)^{-1})} \Big)^{2k-2} \gamma^2 \right)^{1+\delta} \cdot \\
&\qquad R(\alpha_a)^{-1} R(\alpha_e)^{-2\delta} \log^{2k-2}(R(\alpha_a)^{-1}) R(\alpha_e)^{-\delta/e}.
\end{aligned}
$$

An dieser Stelle wissen wir schon, dass für alle $\alpha_e \leq \frac{1}{6}(2e)^{-2k}$ gilt

$$
M(\alpha_a) \leq r_k R(\alpha_a)^{-1} \log^{2k-2}(R(\alpha_a)^{-1}) + s_k,
$$

wobei $r_k, s_k > 0$ von $k$ abhängige, aber von $\alpha_a$ unabhängige Konstanten sind.

(vii) Im Rest des Beweises schätzen wir den Vorfaktor $r_k$ genauer ab: Dazu brauchen wir obere und untere Schranken für $R(\alpha_e)$. Um zu solchen gelangen zu können, setzen wir

$$
\alpha_e := e^{-15(k-1)}.
$$

Dann ist die Bedingung $\alpha_e \leq \frac{1}{6}(2e)^{-2k}$ klar erfüllt. Zudem ist nun

$$
\begin{aligned}
e \cdot R(\alpha_e) &\leq e \frac{\sqrt{6} k 2^{k+1}}{(k-1)!} \log^{k-1}(\alpha_e^{-1}) \sqrt{\alpha_e} \\
&\leq \frac{\sqrt{6} e 2^{(k-1)+(k+1)}}{(k-1)!} 15^{k-1} (k-1)^{k-1} e^{-15(k-1)/2}.
\end{aligned}
$$

Für $N \in \mathbb{N}$ gelten aber

$$
\begin{aligned}
N! &= \exp\left( \sum_{i=1}^{N} \log(i) \right) \leq \exp\left( \int_1^{N+1} \log(x) dx \right) \\
&= \exp\big( (N+1)(\log(N+1) - 1) + 1 \big) = e \Big( \frac{N+1}{e} \Big)^{N+1} \text{ und} \\
N! &= \exp\left( \sum_{i=2}^{N} \log(i) \right) \geq \exp\left( \int_1^{N} \log(x) dx \right) \\
&= \exp\big( N(\log(N) - 1) + 1 \big) = e \Big( \frac{N}{e} \Big)^{N},
\end{aligned}
$$

also können wir weiter abschätzen zu

$$
\begin{aligned}
&eR(\alpha_e)\\
&\leq \sqrt{6}e2^{(k-1)+(k+1)}15^{k-1}e^{k-2}e^{-15(k-1)/2}\\
&= \exp\Big(1+\log(\sqrt{6})+2\log(2)-1+(k-1)\big(\log(15)+1+2\log(2)-\frac{15}{2}\big)\Big)\\
&\leq \exp\Big((k-1)\big(\frac{1}{2}\log(6)+4\log(2)+\log(15)+1-\frac{15}{2}\big)\Big)\\
&< 1,
\end{aligned}
$$

da der Term in der zweiten Klammer zu $-0.1235 < 0$ auswertet. Also ist $R(\alpha_e) < e^{-1}$, also $\log(R(\alpha_e)^{-1})) > 1$.

Auf der anderen Seite ist nach Lemma 4.14 auch

$$
\begin{aligned}
R(\alpha_e) &\geq \frac{2^{-3k}}{(k-1)!}\log^{k-1}(\alpha_e^{-1})\sqrt{\alpha_e}\\
&= \frac{2^{-3k}}{(k-1)!}(15(k-1))^{k-1}e^{-15(k-1)/2}\\
&\geq 2^{-3k}15^{k-1}\frac{e^{k-2}}{k-1}e^{-15(k-1)/2}.
\end{aligned}
$$

Setzen wir beides in (vi) ein, so erhalten wir

$$
\begin{aligned}
&M(\alpha_a)-M(\alpha_e)\\
&\leq \left(e^{(2k-2)(\delta-1)}\Big(\frac{(2k-2)}{\log(1+\delta)}\Big)^{2k-2}\gamma^2\right)^{1+\delta}\cdot\\
&\quad\Big(2^{3k}15^{-k+1}\frac{k-1}{e^{k-2}}e^{15(k-1)/2}\Big)^{\delta(2+1/e)}R(\alpha_a)^{-1}\log^{2k-2}(R(\alpha_a)^{-1})\\
&\leq \left(e^{(2k-2)(\delta-1)}\Big(\frac{2}{\log(1+\delta)}\Big)^{2k-2}6k^2 2^{2k+2}e^{k-2}\right)^{1+\delta}\cdot\\
&\quad\Big(2^{3k}15^{-k+1}\frac{k-1}{e^{k-2}}e^{15(k-1)/2}\Big)^{\delta(2+1/e)}R(\alpha_a)^{-1}\log^{2k-2}(R(\alpha_a)^{-1}),
\end{aligned}
$$

wobei wir nochmals eine einfache Schranke für die Fakultät benutzt haben beim Einsetzen von $\gamma = \frac{\sqrt{6}k2^{k+1}}{(k-1)!}$.

Somit existiert ein $\lambda > 0$, sodass

$$
M(\alpha_a) \leq \lambda^k R(\alpha_a)^{-1}\log^{2k-2}(R(\alpha_a)^{-1}) + e^{15(k-1)},
$$

für jedes $\alpha_a \leq e^{-15(k-1)}$, da nach Aussage (4.9): $M(\alpha_e) \leq 1/\alpha_e = e^{15(k-1)}$.

Genauer erhalten wir für $\delta = 0.0911$:

$$M(\alpha_a) \leq k^{2.3979} e^{8.7233k-4.1700} R(\alpha_a)^{-1} \log^{2k-2}(R(\alpha_a)^{-1}) + e^{15(k-1)}.$$

Wegen

$$\frac{k^{2.3979}}{e^{4.1700}} \leq \frac{k^3}{e^{4.1700}} = \frac{1}{3!}\Big(\frac{k}{\sqrt[3]{e^{4.1700}/6}}\Big)^3 \leq e^{\sqrt[3]{6/e^{4.1700}}k} \leq e^{0.4527k}$$

ist also $\lambda \leq e^{8.7233+0.4527} = e^{9.1760} \approx 9662.43$.

□

# Symbolverzeichnis

$\mathbb{N}$ ..... Die Menge der natürlichen Zahlen (ohne 0), $\mathbb{N} = \{1, 2, 3, \ldots\}$
$\mathbb{N}_0$ ..... Die Menge der natürlichen Zahlen mit 0, $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$
$\lfloor x \rfloor$ ..... Die größte ganze Zahl $n$ mit $n \leq x$
$\lceil x \rceil$ ..... Die kleinste ganze Zahl $n$ mit $n \geq x$
frac ..... Der fraktionale Anteil von $x$, also $\mathrm{frac}(x) = x - \lfloor x \rfloor$
$f(n) = O(g(n))$ ... $\exists c > 0,\ n_0 \in \mathbb{N}\colon \forall n \geq n_0\colon\ -c \cdot g(n) \leq f(n) \leq c \cdot g(n)$
$f(n) = o(g(n))$ ... $\forall c > 0\colon \exists n_0 \in \mathbb{N}\colon \forall n \geq n_0\colon\ -c \cdot g(n) \leq f(n) \leq c \cdot g(n)$
$f(n) = \Theta(g(n))$ ... $\exists c_1, c_2 > 0,\ n_0 \in \mathbb{N}\colon \forall n \geq n_0\colon c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$
$[b_0; b_1, b_2, b_3, \ldots]$ .. Darstellungsweise eines Kettenbruchs, S. 8
$b_i(x)$ ..... $i$-ter Kettenbruchkoeffizient von $x$, S. 8
$A_i(x)/B_i(x)$ ..... $i$-ter Konvergent von $x$, S. 9
$A_i(\underline{b})/B_i(\underline{b})$ ..... $i$-ter Konvergent einer Zahl mit Kettenbruchentwicklung $[0; b_1, \ldots, b_k, \ldots]$ für $\underline{b} = (b_1, \ldots, b_k)$, S. 21
$\underline{b}_{k-1}(x)$ ..... Kurzschreibweise für $(b_1(x), \ldots, b_{k-1}(x))$, S. 21
$I_{\underline{b}}$ ..... Intervall aller Kettenbrüche der Form $[0; b_1, \ldots, b_{k-1}, \ldots]$ für $\underline{b} = (b_1, \ldots, b_{k-1})$, S. 22
$I_{\underline{b},m}$ ..... Intervall aller Kettenbrüche der Form $[0; b_1, \ldots, b_{k-1}, b_k, \ldots]$ mit $b_k \leq m$ für $\underline{b} = (b_1, \ldots, b_{k-1})$, S. 22
$M_n$ ..... $M_n = \{\mathrm{frac}(\sqrt{k}) \mid n^2 < k < (n+1)^2\}$, S. 11
$M_n^U$ ..... $M_n^U = \{\mathrm{frac}(\sqrt{k}) \mid 1 < k \leq n,\ k \text{ kein Quadrat}\}$, S. 11
$Q_n$ ..... $Q_n = \{\mathrm{frac}(\sqrt{k}) \mid n^2 < k < (n+1)^2,\ k \text{ quadratfrei}\}$, S. 11
$Q_n^U$ ..... $Q_n^U = \{\mathrm{frac}(\sqrt{k}) \mid 1 < k \leq n,\ k \text{ quadratfrei}\}$, S. 11
$T$ ..... zufällige gleichverteilte reelle Zahl aus dem Einheitsintervall, S. 18
$D_n = D(S_n)$ ..... zufällige gleichverteilte Zahl aus $S_n$, S. 18
$(S_n)_{n=1}^{\infty}$ ..... gleichverteilte Familie von endlichen Mengen $S_n \subset [0, 1] \setminus \mathbb{Q}$, S. 18
$F(n)$ ..... Fehler der gleichverteilten Familie $(S_n)_n$, S. 18
$L(\alpha)$ ..... Gesamtlänge der langen Intervalle $I_{\underline{b}}$, S. 23
$M(\alpha)$ ..... Anzahl der langen Intervalle $I_{\underline{b}}$, S. 23
$R(\alpha)$ ..... Restterm; Wahrscheinlichkeit, dass $T$ in der Obermenge $I_{\underline{b}}$ eines kurzen Intervalles $I_{\underline{b},m}$ landet, S. 23
$\sigma(x)$ ..... Die Anzahl quadratfreier natürlicher Zahlen $n$ mit $n \leq x$, S. 15
$\sigma_0(n)$ ..... Die Anzahl an Teilern von $n$, S. 29

# Literaturverzeichnis


[Coh77] J. H. E. Cohn, *The length of the period of the simple continued fraction of $d^{1/2}$*, Pacific J. Math. **71** (1977), no. 1, 21–32.

[HW58] G. H. Hardy and E. M. Wright, *Einführung in die Zahlentheorie*, R. Oldenbourg, München, 1958.

[Jia93] Chao Hua Jia, *The distribution of square-free numbers*, Sci. China Ser. A **36** (1993), no. 2, 154–169.

[Khi63] A. Ya. Khintchine, *Continued fractions*, Übersetzt von Peter Wynn, P. Noordhoff Ltd., Groningen, 1963.

[Ler08] E. Yu Lerner, *Statistics of incomplete quotients of continued fractions of quadratic irrationalities*, http://arxiv.org/abs/0810.0718, 2008.

[Lev29] P. Levy, *Sur les lois de probabilité dont dependent les quotients complets et incomplets d'une fraction continue*, Bull. Soc. Math. France **57** (1929), 178–194.

[Pap05] Francesco Pappalardi, *A survey on k-freeness*, Number theory, Ramanujan Math. Soc. Lect. Notes Ser., vol. 1, Ramanujan Math. Soc., Mysore, 2005, pp. 71–88.

[Per13] Oskar Perron, *Die Lehre von den Kettenbrüchen*, B. G. Teubner Verlagsgesellschaft, Leipzig und Berlin, 1913.

[Wal63] Arnold Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Mathematische Forschungsberichte, XV, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

[Wei] Eric W. Weisstein, *Gauss-kuzmin distribution*, http://mathworld.wolfram.com/Gauss-KuzminDistribution.html, From MathWorld–A Wolfram Web Resource.

[Wir74] Eduard Wirsing, *On the theorem of Gauss-Kusmin-Lévy and a Frobenius-type theorem for function spaces*, Acta Arith. **24** (1973/74), 507–528, Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday, V.

[Zag81] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag, Berlin, 1981, Eine Einführung in die höhere Zahlentheorie, Hochschultext.