Eigenschaften von Näherungsbrüchen

Lemma Eigenschaften von Näherungsbrüchen

Es gilt

1. $q_{n+1} > q_n \geq n$ für $n \in \mathbb{N}$.
2. $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$ für $n \in \mathbb{N}_0$.
3. $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ für $n \in \mathbb{N}_0$.
4. $\mathrm{ggT}(p_n, q_n) = 1$.

Beweis:

(1) **IA** für $n = 1$: Es gilt $q_0 = 1$, $q_1 = a_1 \geq 1$ und damit

$$q_2 = a_2 q_1 + q_0 \geq q_1 + q_0 > q_1 \geq 1.$$

- **IS** $n \to n+1$: Es gilt

$$q_{n+1} = a_n q_n + q_{n-1} \geq q_n + q_{n-1} > q_n.$$

- Aus $q_n > \ldots > q_1 > 1$ folgt $q_n \geq n$.

(2) Wir schreiben $p_n q_{n-1} - p_{n-1} q_n$ als

$$\det \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \det \prod_{i=0}^{n} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \prod_{i=0}^{n} \det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = (-1)^{n+1}.$$

Eigenschaften von Näherungsbrüchen

Beweis: (Fortsetzung)

(3) Aus (2) folgt

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = a_n (-1)^n. \end{aligned}$$

(4) Sei $d = \mathrm{ggT}(p_n, q_n)$. Damit gilt $d \mid p_n q_{n-1} - p_{n-1} q_n$.

- Aus (2) folgt $d \mid (-1)^{n+1}$ und damit $d = \pm 1$.

Konvergenz von Kettenbrüchen

Satz Konvergenz von Kettenbrüchen

Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$. Dann gilt:

1. Die Brüche $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ bilden eine konvergente Folge.
2. Die Teilfolge $\frac{p_{2n}}{q_{2n}}$ wächst streng monoton, die Teilfolge $\frac{p_{2n+1}}{q_{2n+1}}$ fällt streng monoton.

Beweis:

(1) Aus $p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$ folgt

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^{i+1}}{q_{i-1} q_i} \text{ für alle } i \in \mathbb{N}_0.$$

- Wir entwickeln in einer Teleskopsumme

$$\frac{p_n}{q_n} = \sum_{i=1}^{n} \left(\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}}\right) + \frac{p_0}{q_0} = a_0 + \sum_{i=1}^{n} \frac{(-1)^{i+1}}{q_{i-1} q_i}.$$

- Die $\frac{1}{q_{i-1} q_i}$ bilden eine streng monotone Nullfolge.
- D.h. ihre alternierende Reihe ist konvergent und damit auch die $\frac{p_n}{q_n}$.

Konvergenz von Kettenbrüchen

Beweis: (Fortsetzung)

(2) Aus $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ folgt

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_{n-2} q_n} \text{ für alle } n \in \mathbb{N}_0.$$

- Für $n \geq 2$ sind a_n, q_n, q_{n-2} positiv und daher ist der Term

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} \begin{cases} \text{positiv} & \text{für } n \text{ gerade.} \\ \text{negativ} & \text{für } n \text{ ungerade.} \end{cases}$$

- D.h. die Teilfolge $\frac{p_{2n}}{q_{2n}}$ wächst streng monoton und die Teilfolge $\frac{p_{2n+1}}{q_{2n+1}}$ fällt streng monoton.

Konvergenz der Kettenbruchentwicklung

Satz Konvergenz der Kettenbruchentwicklung

Sei $x \in \mathbb{R} \setminus \mathbb{Q}$ mit Kettenbruch $x = [a_0, a_1, \ldots]$. Dann konvergieren die Näherungsbrüche $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ gegen x. Es gilt für $n \in \mathbb{N}$

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{n(n+1)}.$$

Beweis:

- Sei $x = [a_0, a_1, \ldots, a_n, r_n] = \frac{r_n p_n + p_{n-1}}{r_n q_n + q_{n-1}}$ für ein $r_n \in \mathbb{R}_{>0} \setminus \mathbb{N}$.
- Damit folgt

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{(r_n p_n + p_{n-1}) q_n - p_n (r_n q_n + q_{n-1})}{q_n (r_n q_n + q_{n-1})} \\ &= \frac{p_{n-1} q_n - p_n q_{n-1}}{q_n (r_n q_n + q_{n-1})} = \frac{(-1)^n}{q_n (r_n q_n + q_{n-1})}. \end{aligned}$$

- Wegen $a_{n+1} := \lfloor r_n \rfloor$ und $r_n \notin \mathbb{N}$ folgt $r_n > a_{n+1}$ bzw. $\frac{1}{r_n} < \frac{1}{a_{n+1}}$. D.h.

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n (a_{n+1} q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}} \leq \frac{1}{n(n+1)}.$$

- Damit konvergieren die Näherungsbrüche $\frac{p_n}{q_n}$ gegen x.

Kettenbruch der Euler-Zahl

Bsp: : Kettenbruchentwicklung der Euler-Zahl

- Euler zeigte 1744 , dass

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, \ldots].$$

- Dies liefert die folgenden Approximationen für e.

$[a_0, a_1, \ldots, a_n]$	$\frac{p_n}{q_n}$	$e - \frac{p_n}{q_n}$
$[2]$	2	$7 \cdot 10^{-1}$
$[2, 1]$	3	$-3 \cdot 10^{-1}$
$[2, 1, 2]$	$\frac{8}{3}$	$5 \cdot 10^{-2}$
$[2, 1, 2, 1]$	$\frac{11}{4}$	$-3 \cdot 10^{-2}$
$[2, 1, 2, 1, 1]$	$\frac{19}{7}$	$4 \cdot 10^{-3}$
$[2, 1, 2, 1, 1, 4]$	$\frac{87}{32}$	$-5 \cdot 10^{-4}$

Übung:

Zeigen Sie, dass Kettenbrüche eine *Bestapproximation* liefern. D.h.

$$|x - \tfrac{p_n}{q_n}| \leq |x - \tfrac{p}{q}| \text{ für alle Brüche } \tfrac{p}{q} \in \mathbb{Q} \text{ mit } q \leq q_n.$$

Auftreten von Näherungsbrüchen

Ziel: Jeder Bruch, der x sehr gut approximiert, ist ein Näherungsbruch.

Satz Auftauchen von Näherungsbrüchen

Sei $x \in \mathbb{R}$. Sei $\frac{p}{q} \in \mathbb{Q}$ mit $\mathrm{ggT}(p,q) = 1$, $q > 0$ und $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$.
Dann ist $\frac{p}{q}$ ein Näherungsbruch in der Kettenbruchentwicklung von x.

Beweis:

- Sei $\frac{p}{q} = [a_0, a_1, \ldots, a_n]$. Falls $x = \frac{p}{q}$, sind wir fertig.
- Ansonsten existiert ein $r_n \in \mathbb{R}_{>0}$ mit $x = [a_0, a_1, \ldots, a_n, r_n]$.
- Wir definieren $r_i := [a_{i+1}, \ldots, a_n, r_n]$ für $i = 0, \ldots, n-1$. Damit gilt

$$\begin{aligned} & [a_0, a_1, \ldots, a_i, r_i] = [a_0, a_1, \ldots, a_i, [a_{i+1}, \ldots, a_n, r_n]] \\ = \quad & [a_0, a_1, \ldots a_n, r_n] = x \quad \text{für } 0 \leq i \leq n. \end{aligned}$$

- Ferner ist $r_i = [a_{i+1}, r_{i+1}] = a_{i+1} + \frac{1}{r_{i+1}}$ für $0 \leq i < n$.
- Z.z.: $[a_0, \ldots, a_i, r_i]$ ist für $0 \leq i \leq n$ Kettenbruchentwicklung von x.

Auftreten von Näherungsbrüchen

Beweis: (Fortsetzung)

- Zeigen $r_i > 1$ für $i \leq n$, dann ist $a_{i+1} = \lfloor r_i \rfloor$ in KETTENBRUCH.
- Sei $r_n > 1$. Dann gilt $r_{n-1} = a_n + \frac{1}{r_n} > 1$.
- Es folgt induktiv, dass $r_{n-2}, \ldots, r_0 > 1$. Bleibt z.z.: $r_n > 1$.
- Nach dem Lemma für Näherungsbrüche (Folie 146) gilt
$$\frac{p}{q} = \frac{p_n}{q_n} \text{ und } x = \frac{p_n r_n + p_{n-1}}{q_n r_n + q_{n-1}}.$$
- $\frac{p}{q}, \frac{p_n}{q_n}$ sind gekürzte Brüche mit $q, q_n > 0$, d.h. $p = p_n$ und $q = q_n$.
- Aus unserer Voraussetzung folgt
$$\begin{aligned} \frac{1}{2q_n^2} &> \left| x - \frac{p}{q} \right| = \left| \frac{p_n r_n + p_{n-1}}{q_n r_n + q_{n-1}} - \frac{p_n}{q_n} \right| = \left| \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n (q_n r_n + q_{n-1})} \right| \\ &= \left| \frac{(-1)^n}{q_n (q_n r_n + q_{n-1})} \right| = \frac{1}{q_n (q_n r_n + q_{n-1})}. \end{aligned}$$
- Es folgt $q_n + q_{n-1} < 2q_n < q_n r_n + q_{n-1}$ und damit $r_n > 1$.

Brechen von RSA mit kleinem geheimen Schlüssel

Satz von Wiener (1990)

Sei (N, e) ein öffentlicher RSA Schlüssel mit $2 < e < \varphi(N)$ und $N = pq$, p, q gleicher Bitgröße. Sei $ed = 1 \bmod \varphi(N)$ mit $d < \frac{1}{3}N^{\frac{1}{4}}$. Dann liefert die Kettenbruchentwicklung von $\frac{e}{N}$ das geheime d.

Beweis:

- Aus $ed = 1 \bmod \varphi(N)$ folgt für ein $k \in \mathbb{N}$
$$ed = 1 + k\varphi(N) = 1 + k(p-1)(q-1) = 1 + kN - k(p+q-1).$$
- Jeder gemeinsame Teiler von k und d teilt 1. D.h. $\mathrm{ggT}(k, d) = 1$.
- Teilen durch dN liefert $\frac{e}{N} - \frac{k}{d} = \frac{1-k(p+q-1)}{dN}$.
- Falls $\left|\frac{1-k(p+q-1)}{dN}\right| = \frac{k(p+q-1)-1}{dN} < \frac{1}{2d^2}$, dann taucht der gekürzte Bruch $\frac{k}{d}$ in der Kettenbruchentwicklung von $\frac{e}{N}$ auf.
- Diese Bedingung ist äquivalent zu $2d(k(p+q-1)-1) < N$.

Brechen von RSA mit kleinem geheimen Schlüssel

- Wir beweisen die stärkere Bedingung $2dk(p+q) < N$.
- Dazu benötigen wir obere Schranken für k und $p+q$.
- Es gilt $k = \frac{ed-1}{\varphi(N)} < \frac{e}{\phi(N)} \cdot d < d$.
- OBdA gelte $p \leq q$. Da p, q gleiche Bitgröße besitzen, folgt
$$p \leq \sqrt{N} \leq q < 2p \leq 2\sqrt{N}.$$
- D.h. wir erhalten $p+q < 3\sqrt{N}$. Dies erfüllt unsere Bedingung:
$$2dk(p+q) < 2d^2(p+q) < \tfrac{2}{9}\sqrt{N} \cdot 3\sqrt{N} < N.$$
- Damit erhalten wir das geheime d aus dem Kettenbruch von $\frac{e}{N}$.

Übung: Seien $a \in \mathbb{Z}$, $n \in \mathbb{N}$ mit $\mathrm{ggT}(a,n) = 1$. Konstruieren Sie mit Hilfe eines Kettenbruchs ein Inverses x von a in U_n, d.h. $ax \equiv 1 \bmod n$.

Definition Pellsche Gleichung

Sei $d \in \mathbb{N}$ kein Quadrat. Dann heißt $x^2 - dy^2 = 1$ *Pellsche Gleichung*.