§9. Diophantische Approximation

Wie jede reelle Zahl ist $\pi = 3,14159265\ldots$ – als Grenzwert einer Folge rationaler Zahlen durch rationale Zahlen approximierbar. Liu Hui (3. Jahrh.) hat einen Algorithmus angegeben, der π approximiert durch Vergleich der Kreise mit Polygonen. Mit einem 96-gon hat er π als ungefähr 3,1416 bestimmt. Zu Chongzhi (5. Jahrh.) hat $\frac{22}{7}$ und $\frac{355}{113} \approx 3,14159265$ bestimmt, durch ein $2^{13} \times 3$-gon. Das ist beeindruckend, aber ist es auch eine gute oder in irgendeinem Sinn eine beste Approximation? rationale

Die Dezimalentwicklung liefert immer bessere Approximation, je mehr Dezimalstellen man berücksichtigt. Eine gute Approximation sollte der reellen Zahl α nahekommen, aber relativ kleinen Nenner haben.

9.1 Definition: Sei $\alpha \in \mathbb{R}$. Eine rationale Zahl $\frac{a}{b}$ heißt eine beste Näherung für $\alpha :\Leftrightarrow \forall \frac{c}{d} \neq \frac{a}{b}$ mit $d, b \in \mathbb{N}$ und $d \leq b$ gilt $|d\alpha - c| > |b\alpha - a|$.

($d \leq b$ impliziert: $\underbrace{|d\alpha - c| \cdot \frac{1}{d}}_{|\alpha - \frac{c}{d}|} \geq |d\alpha - c| \frac{1}{b} > |b\alpha - a| \cdot \frac{1}{b} = |\alpha - \frac{a}{b}|$

$\Rightarrow \frac{a}{b}$ ist wirklich näher an α als $\frac{c}{d}$.

Die Bedingung in der Definition ist weniger anschaulich, aber stärker.)

Fragen: Existieren beste Näherungen?
Sind sie eindeutig?
Wie konstruiert man sie?

Wenn man den Nenner 1 zuläßt, scheitert die Eindeutigkeit: $\frac{3}{2}$ hat zwei beste Näherungen mit Nenner 1. nämlich?

Wir lassen $\alpha = \frac{p}{q} \in \mathbb{Q}$ zu. Dann wird nach Näherungen mit Nennern $< q$ gefragt.

Eine historische Motivation ist der folgende praktische Grund. Huygens wollte (um 1700) ein mechanisches Modell des Sonnensystems bauen. Dabei musste er mit Zahnrädern mit möglichst wenigen Zähnen auskommen, um die Quotienten der Umlaufzeiten der Planeten und Monde möglichst gut zu approximieren.

Die Lösung ist natürlich die Kettenbruchentwicklung von α:

9.2 Theorem: Sei $\alpha \in \mathbb{R}$, $n > 1$ und $\frac{p_n}{q_n}$ der n-te Näherungsbruch. Sei $0 < d \leq q_n$ und $\frac{c}{d} \neq \frac{p_n}{q_n}$.
Dann gilt $\left|\frac{p_n}{q_n} - \alpha\right| < \left|\frac{c}{d} - \alpha\right|$ und sogar $|p_n - q_n\alpha| < |c - d\alpha|$, d.h. $\frac{p_n}{q_n}$ ist die beste Näherung.

Wie gut diese Näherungen sind, sieht man bei π: Der Kettenbruch beginnt $[3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, \ldots]$. Schon die ersten 5 Einträge $[3; \ldots, 292]$ approximieren π mit einem Fehler $< 10^{-5}$, bei $[3; \ldots, 14]$ ist der Fehler $< 10^{-15}$. Und auf 57 wissen wir in jedem Schritt, ob der Fehler positiv oder negativ ist.

Beweis von 9.2.: Sei $ggT(c, d) = 1$.
Aus 7.4 wissen wir schon: $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$
(7.5 ii: $\lim_{i\to\infty} \frac{p_i}{q_i}$)

Behauptung: (1) Die Folge $|p_n - q_n\alpha|$ ist streng monoton fallend.
(2) $\frac{1}{q_{n+2}} < \frac{1}{a_{n+1}q_n + q_{n-1}} < \frac{1}{q_{n+1}}$ (Erinnerung: q_n wächst streng monoton)

Beweis der Behauptung: Zuerst (2) mit Induktion.
ZZ $a_{n+1}q_n + q_{n-1} \in (q_{n+1}, q_{n+2})$
Induktionsanfang: $q_1 = a_1$, $q_2 = a_2 a_1 + 1$ ✓
In 7.4 haben wir schon gezeigt: $\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(q_n\alpha_{n+1} + q_{n-1})}$
und $a_{n+1} < \alpha_{n+1} < a_{n+1} + 1$ (es sei denn $\alpha_{n+1} = a_{n+1} + 1 \in \mathbb{Z}$, d.h. $\alpha \in \mathbb{Q}$, siehe unten)

Jetzt der Induktionsschritt: $q_{n+1} = a_{n+1} q_n + q_{n-1} < \alpha_{n+1} q_n + q_{n-1} <$

$< (a_{n+1}+1) q_n + q_{n-1} = \underbrace{(a_{n+1} q_n + q_{n-1})}_{q_{n+1}} + q_n \leq a_{n+2} q_{n+1} + q_n = q_{n+2} \Rightarrow (2)$

Nun folgt (1): (2) sagt $\frac{1}{q_{n+2}} < \underbrace{\frac{1}{\alpha_{n+1} q_n + q_{n-1}}}_{u} < \frac{1}{q_{n+1}}$

$\frac{q_n}{q_n(\alpha_{n+1} q_n + q_{n-1})} = q_n \left| \alpha - \frac{p_n}{q_n} \right| = |p_n - q_n \alpha| \Rightarrow (1)$

(Für $\alpha \in \mathbb{Q}$ stimmt das nicht ganz genau:
Wie bemerkt ist beim letzten Näherungsbruch $\alpha_{n+1} = a_{n+1} + 1$ – aber dann ist $\alpha = \frac{p_n}{q_n}$ und (1) ist klar.)

Die Folge $|p_n - q_n \alpha|$ fällt also streng monoton.

Aus $|p_n - q_n \alpha| < |p_{n-1} - q_{n-1} \alpha|$ folgt auch: wenn $d \leq q_{n-1}$, dann ist schon $\frac{p_{n-1}}{q_{n-1}}$ besser als $\frac{c}{d}$ und damit $\frac{p_n}{q_n}$ erstrecht.

Deshalb können wir $q_{n-1} < d \leq q_n$ annehmen. Es bleiben zwei Fälle:

Erster Fall: $d = q_n$. Aus $\frac{c}{d} \neq \frac{p_n}{\underbrace{q_n}_{=d}}$ folgt $\left| \frac{p_n}{q_n} - \frac{c}{q_n} \right| \geq \frac{1}{q_n}$ weil $c \neq p_n$.

Aber $\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{2 q_n}$

(wegen $1 \leq q_n < q_{n+1}$). Dreiecksungleichung $\Rightarrow \left| \alpha - \frac{p_n}{q_n} \right| < \left| \alpha - \frac{c}{d} \right|$.

Zweiter Fall: $q_{n-1} < d < q_n \Rightarrow \frac{p_{n-1}}{q_{n-1}} \neq \frac{c}{d} \neq \frac{p_n}{q_n}$ (alle Brüche sind gekürzt)

Das Gleichungssystem (↑ und immer mit positivem Nenner)

$$x p_n + y p_{n-1} = \pm c \quad \text{mit} \quad \det \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \pm 1$$
$$x q_n + y q_{n-1} = \pm d$$

hat eindeutige ganzzahlige Lösungen $x = \pm (c q_{n-1} - d p_{n-1})$ und $y = \pm (c q_n - d p_n)$

x und y sind beide ungleich 0 ($x = 0 \Rightarrow c q_{n-1} = d p_{n-1} \Rightarrow \frac{c}{d} = \frac{p_{n-1}}{q_{n-1}}$ ↯
$y = 0 \Rightarrow \frac{c}{d} = \frac{p_n}{q_n}$ ↯)

$d = x q_n + y q_{n-1} < q_n \Rightarrow x$ und y haben entgegengesetzte Vorzeichen

Auch $\alpha - \frac{p_n}{q_n}$ (nach 7.5) wechselt das Vorzeichen (mit $(-1)^n$) $\Rightarrow$

$p_n - q_n \alpha$ und $p_{n-1} - q_{n-1} \alpha$ haben auch verschiedene Vorzeichen

$\Rightarrow x (p_n - q_n \alpha)$ und $y (p_{n-1} - q_{n-1} \alpha)$ haben dasselbe Vorzeichen

$$x(p_n - q_n\alpha) + y(p_{n-1} - q_{n-1}\alpha) = \overbrace{(xp_n + yp_{n-1})}^{c} - \overbrace{(xq_n + yq_{n-1})}^{d}\alpha$$
$$= c - d\alpha$$
$$\Rightarrow |c - d\alpha| > |y(p_{n-1} - q_{n-1}\alpha)| > |p_{n-1} - q_{n-1}\alpha|$$
$$\text{und } |c - d\alpha| > |x(p_n - q_n\alpha)| > |p_n - q_n\alpha| \quad \square$$
$y \neq 0$, $x \neq 0$

Die Näherungsbrüche in der Kettenbruchentwicklung produzieren also beste Näherungen. Wir wissen aber noch nicht, ob es für andere Nenner ($\neq q_n$) auch beste Näherungen gibt. Was sagt der Beweis von 9.2 dazu? Sei $\frac{c}{d}$ eine beste Näherung (bezüglich d als Nenner). Dann existiert n: $q_{n-1} \leq d \leq q_n$. Im ersten Fall, $d = q_n$, ist $\frac{p_n}{q_n}$ die beste Näherung, also $\frac{c}{d} = \frac{p_n}{q_n}$. Im zweiten Fall, $q_{n-1} < d < q_n$ folgt aus dem Beweis von 9.2. Wenn $\frac{c}{d}$ eine beste Näherung ist bezüglich d, also auch bezüglich q_{n-1}, muß $\frac{c}{d} = \frac{p_{n-1}}{q_{n-1}}$ sein oder der nachfolgende Näherungsbruch $\frac{p_n}{q_n}$.

9.3 Korollar: Jede beste Näherung für $\alpha \in \mathbb{R}$ ist ein Näherungsbruch von α.
(Dies braucht 9.1 – andere Definitionen führen nicht zu dieser Eindeutigkeit)

Wie gut oder schlecht sind die besten Näherungen?
Übungsblatt 9, Aufgabe 1: Sei $|\alpha - \frac{p}{q}| < \frac{1}{2q^2} \Rightarrow \frac{p}{q}$ ist ein Näherungsbruch.
Umgekehrt: Von zwei aufeinanderfolgenden Näherungsbrüchen erfüllt mindestens einer die Ungleichung $|\frac{p}{q} - \alpha| < \frac{1}{2q^2}$.
(siehe §7)
oder der Fehler dabei

Die Approximation ist also immer $< \frac{1}{q^2}$, oft $< \frac{1}{2q^2}$. Könnte es im Allgemeinen noch viel besser sein? Nein, es gibt auch untere Schranken für den Fehler:

9.4 Proposition: Sei $\alpha \in \mathbb{R} - \mathbb{Q}$ mit $\alpha = [a_0; a_1, \ldots]$, so daß es ein $A \geq 1$ gibt mit $a_i \leq A \; \forall i \geq 0$. Dann gilt für alle $p \in \mathbb{Z}, q \in \mathbb{N}$:

$$|\alpha - \frac{p}{q}| > \frac{1}{A+2} \frac{1}{q^2}$$

Der goldene Schnitt $\frac{1+\sqrt{5}}{2} = [1;1,1,\dots]$ ist also besonders schlecht approximierbar. Und quadratische Irrationalitäten (mit periodischen Kettenbrüchen) sind generell schlecht approximierbar.

Beweis von 9.4: Das ist wieder ein gesticktes Arrangieren von Gleichungen und Ungleichungen, die wir schon kennen.

$\frac{p_{n+2}}{q_{n+2}}$ liegt immer zwischen α und $\frac{p_n}{q_n}$

$$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| > \left|\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n}\right| = |A_{n+2} - A_n| = \frac{a_{n+2}}{q_{n+2}\cdot q_n}$$

$$\Rightarrow |q_n\alpha - p_n| > \frac{a_{n+2}}{q_{n+2}}$$

Außerdem $\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n} \Rightarrow |q_n\alpha - p_n| < \frac{1}{q_{n+1}}$

$$\Rightarrow \frac{a_{n+2}}{q_{n+2}} < |q_n\alpha - p_n| \leq \frac{1}{q_{n+1}}$$

$$\Rightarrow \frac{q_{n+2}}{a_{n+2}} > \frac{1}{|q_n\alpha - p_n|} > q_{n+1} \Rightarrow \frac{1}{q_n|q_n\alpha - p_n|} > \frac{q_{n+1}}{q_n} = \frac{q_n a_{n+1} + q_{n-1}}{q_n} =$$

$$= a_{n+1} + \frac{q_{n-1}}{q_n} \geq a_{n+1}$$

und $\Downarrow$ $\frac{q_{n+2}}{a_{n+2}q_n} > \frac{1}{|q_n\alpha - p_n|q_n}$

$$= \frac{q_{n+1}a_{n+2} + q_n}{q_n a_{n+2}} \leq \frac{q_{n+1}}{q_n} + 1 = \frac{q_n a_{n+1} + q_{n-1}}{q_n} + 1 \leq a_{n+1} + 2$$

Insgesamt: $a_{n+1} \leq \frac{1}{q_n|q_n\alpha - p_n|} < a_{n+1} + 2$ (*)

und $q_n|q_n\alpha - p_n| > \frac{1}{a_{n+1}+2} \Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{a_{n+1}+2}\cdot\frac{1}{q_n^2} \geq \frac{1}{A+2}\cdot\frac{1}{q_n^2}$ □

Aus (*) folgt auch $q_n|q_n\alpha - p_n| \leq \frac{1}{a_{n+1}}$

$$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2}\cdot\frac{1}{a_{n+1}}$$

Falls $a_{n+1} = A$ das Maximum annimmt, sind obere und untere Schranke nicht sehr weit voneinander entfernt.

Ist gute Approximierbarkeit eine Eigenschaft, in der sich algebraische und transzendente Zahlen zumindest manchmal voneinander unterscheiden?

Eine wesentliche Verbesserung von 9.4, mit einer schöneren Bedingung, ist:

9.5 Theorem (Approximationssatz von Liouville): Sei $\alpha \in \mathbb{R}$ algebraisch mit Minimalpolynom $f(x) \in \mathbb{Z}[x]$ und $\partial(\alpha)$ der Grad von f. Dann existiert ein $c(\alpha) > 0$, so daß für alle $p \in \mathbb{Z}, q \in \mathbb{N}$ und $\frac{p}{q} \neq \alpha$ gilt:

$$|\alpha - \tfrac{p}{q}| \geq c(\alpha)\, q^{-\partial(\alpha)}.$$

($c(\alpha)$ wird im Beweis angegeben)

Diesen Satz kennen wir von Übungsblatt 4. Jetzt sehen wir ihn in einem natürlichen Kontext.

Beweis von 9.5: (anders als auf Blatt 4)

$\alpha \in \mathbb{Q} \Rightarrow f(x) = x - \alpha$, $f(\frac{p}{q}) \neq 0$. Für $\alpha \notin \mathbb{Q}$ kann $f(\frac{p}{q}) = 0$ auch nicht passieren, weil das Minimalpolynom irreduzibel vom Grad ≥ 2 ist und keine rationale Nullstelle haben darf (die man wegdividieren könnte)

$\Rightarrow f(\frac{p}{q}) \neq 0$ (, $a_n = 1$)

Sei $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, alle $a_i \in \mathbb{Z}$

$f(\frac{p}{q}) \neq 0 \Rightarrow q^n f(\frac{p}{q}) = \underbrace{p^n + a_{n-1}p^{n-1}q + \dots + a_0 q^n}_{\in \mathbb{Z}, \text{ also Betrag mindestens } 1} \neq 0$

$$-f(\tfrac{p}{q}) = f(\alpha) - f(\tfrac{p}{q}) = \sum_{i=0}^{n} a_i (\alpha^i - (\tfrac{p}{q})^i) = \sum_{i=1}^{n} a_i \underbrace{(\alpha^i - (\tfrac{p}{q})^i)}_{(\alpha - \frac{p}{q})(\alpha^{i-1} + ?)} =$$

$$= (\alpha - \tfrac{p}{q}) \sum_{i=1}^{n} a_i (\alpha^{i-1} + \alpha^{i-2}\tfrac{p}{q} + \dots + (\tfrac{p}{q})^{i-1})$$

Für $0 < |\alpha - \frac{p}{q}| < 1$ gilt $|\frac{p}{q}| < 1 + |\alpha| \Rightarrow$ (mit $q^n |f(\frac{p}{q})| \geq 1$)

$$\frac{1}{q^n} \leq |f(\tfrac{p}{q})| = |-f(\tfrac{p}{q})| = |\alpha - \tfrac{p}{q}| \cdot |\sum_{i=1}^{n} a_i (\alpha^{i-1} + \dots)| \leq$$

$$\leq |\alpha - \tfrac{p}{q}| \underbrace{\sum_{i=1}^{n} |a_i| \sum_{j=0}^{i-1} |\alpha|^j (1 + |\alpha|)^{i-1-j}}_{V}$$

V sei das $1/c(\alpha)$ ($|\frac{p}{q}|$)

Alle $|a_i| \in \mathbb{N}_0$, nicht alle 0 (V hängt nur von α ab, nicht von $\frac{p}{q}$)

und $|\Sigma - | \geq 1 \Rightarrow \frac{1}{c(\alpha)} \geq 1 \Rightarrow c(\alpha) \leq 1$

$\Rightarrow c(\alpha) \cdot q^{-n} \leq |\alpha - \frac{p}{q}|$. Falls $|\frac{p}{q} - \alpha| \geq 1$: $1 \geq \frac{1}{q}$, also auch ✓ □

Was bedeutet das für Näherungsbrüche?
Im Beweis von 9.4 haben wir gezeigt: $|\alpha - \frac{p_m}{q_m}| < \frac{1}{q_m^2} \cdot \frac{1}{a_{m+1}}$ $\forall m$
$\Rightarrow a_{m+1} < \frac{1}{c(\alpha)} q_m^{\partial(\alpha)-2}$ ($|\alpha - \frac{p_m}{q_m}| < c(\alpha) q_m^{-\partial(\alpha)}$, α ist quadratische Irrationalität)
Spezialfall: $\partial(\alpha)=2$ (α quadratische Irrationalität) $\Rightarrow$ alle $a_m < \frac{1}{c(\alpha)}$!
die a_m sind beschränkt (wie in 9.4), was noch nicht Lagranges Satz über Periodizität impliziert.

Auf Blatt 4 haben wir transzendente Zahlen gesehen. Jetzt können wir transzendente Zahlen durch Kettenbrüche angeben, die $a_{m+1} < \frac{1}{c(\alpha)} q_m^{\partial(\alpha)-2}$ verletzen. Beispiel: Sei $\limsup_{i\to\infty} \frac{\ln a_{i+1}}{\ln q_i} = \infty$ (Beispiele folgen gleich).
$\Rightarrow \forall \delta \in \mathbb{R}_+$ $\exists \infty$ viele i mit
$\frac{\ln a_{i+1}}{\ln q_i} > \delta$, also $\ln a_{i+1} > \ln q_i \cdot \delta \Rightarrow a_{i+1} > q_i^{\delta}$. Aber für großes δ
kann $q_i^{\delta} < a_{i+1} < \frac{1}{c(\alpha)} q_i^{\partial(\alpha)-2}$ nicht gelten $\Rightarrow \alpha$ transzendent.
Wie sollen wir die a_i wählen? $q_i = a_i q_{i-1} + q_{i-2} \le (a_i+1) q_{i-1}$
Induktion $\Rightarrow$ $q_i \le \prod_{j=1}^{i} (a_j+1)$

$\rightsquigarrow$ Wir wählen $g \in \mathbb{N}$, $g \ge 2$, $a_i := g^{i!}$, das wächst schnell genug:

$$\ln q_i \le \sum_{j=1}^{i} \ln(a_j+1) = \sum_{j=1}^{i} \ln(g^{j!}+1) \le \sum_{j=1}^{i} \ln(2 \cdot g^{j!}) =$$
$$= i \ln 2 + \sum_{j=1}^{i} j! \ln g \le i \ln 2 + i! \ln g \sum_{j=1}^{i} \frac{j!}{i!} \le$$
$$\le i + i! \ln g \sum_{u=0}^{i-1} \frac{1}{u!(u)} \le 3 \ln g \cdot i! \quad \text{für } i \text{ groß genug}$$

während $\ln a_{i+1} = (i+1)! \ln g = (i+1) \ln g \cdot i!$ $\Rightarrow \limsup_{i\to\infty} \frac{\ln a_{i+1}}{q_i} = \infty$

$\Rightarrow$ Kettenbrüche $[a_0; g^{1!}, g^{2!}, \ldots]$ definieren transzendente, nicht algebraische Zahlen.

Stärkere Approximationssätze wurden von Thue, Siegel und Roth bewiesen, sie werden z.B. in Bundschuhs Buch erklärt.