

Von Daumen mal π zur Diophantischen Approximation

Wenn ein Mathematiker heute an die reellen Zahlen denkt, so assoziiert er damit das zweigestrichene \mathbb{R} , hat als Bild die Zahlengerade im Kopf und abstrahiert sie vielleicht zu dem bis auf Isomorphie eindeutig bestimmten totalgeordneten vollständigen Körper. Wie auch immer, wir müssen uns der Tatsache bewusst sein, dass hinter diesen Sichtweisen gut zweieinhalbtausend Jahre mathematischer Evolution stecken, die jeder Mathematiker im Laufe seiner Ausbildung quasi im Zeitraffer individuell nachvollzieht.

Um die Diophantische Approximation vorzustellen, das Gebiet der Mathematik, das sich mit der Approximation reeller Zahlen durch rationale Zahlen beschäftigt, möchte ich daher beginnen mit einem Rückblick in eine Zeit, als der Begriff *Zahl* noch vom *Zählen* kam, als Mathematik nicht nur eine Wissenschaft, sondern eine Art Philosophie und Weltanschauung war.

Im 5. Jahrhundert vor Christus beruhte die Philosophie der Pythagoräer auf der Anschauung, dass alle Dinge in Verhältnissen ganzer Zahlen ausgedrückt werden können. Anders ausgedrückt: man war der Überzeugung, dass zu je zwei Grössen a und b eine gemeinsame Masseinheit e existiert, sodass beide jeweils ganzzahlige Vielfache dieser Einheit sind, also $a = m \cdot e$, $b = n \cdot e$ und somit $a : b = m : n$ einem Verhältnis ganzer Zahlen entspricht. Die beiden Grössen sind somit kommensurabel.

Als Hippasus von Metapont das Ordenssymbol der Pythagoräer, das Pentagramm, näher geometrisch untersuchte und bemerkte, dass gerade darin zwei nicht kommensurable Strecken vorkommen, muss dies die Mathematik und das Weltbild seiner Zeit dermassen erschüttert haben, dass er der Legende nach mit dem Fluch der Götter bestraft wurde.

Was genau hatte er entdeckt? Gehen wir von einem regelmässigen Fünfeck aus und zeichnen darin alle Diagonalen ein: der entstehende Stern ist gerade das fragliche Pentagramm. Hippasus war nun aufgefallen, dass für die Längenverhältnisse in dieser Figur

$$\text{Diagonale} : \text{Seite} = \text{Seite} : (\text{Diagonale} - \text{Seite})$$

gilt und selbiges auch für das kleinere Pentagon zutrifft, das die Diagonalen im Zentrum des Sterns begrenzen. Er schloss daraus, dass das Verfahren des wechselweisen Abtragens (also der später so genannte Euklidische Algorithmus) für die beiden Ausgangsgrössen nie abbricht und die beiden Strecken somit nicht kommensurabel sein können.

Damit war die erste irrationale Zahl (der goldene Schnitt $\frac{1+\sqrt{5}}{2}$) entdeckt, auch wenn damals noch niemand so weit ging, Verhältnisse ganzer Grössen selbst als Zahlen anzusehen.

Von da an war es nicht mehr lang bis zur Geburtsstunde der Approximationstheorie in Form von Näherungswerten für inkommensurable Verhältnisse wie etwa 3 für das Verhältniss vom Kreisumfang zu dessen Radius oder auch $1\frac{25}{60}$ für das Verhältniss von der Diagonale zur Seite des Quadrats. Die heutigen Bezeichnungen π und $\sqrt{2}$ wären in diesem Zusammenhang natürlich Anachronismen.

Weitere Fortschritte wurden durch Euklid und Archimedes im 4. und 3. Jahrhundert vor Christus erzielt. Ersterer gab den ersten wirklichen Beweis der Tatsache, dass Diagonale und Seite des Quadrats inkommensurabel sind, indem er den Beweis durch Widerspruch (*reductio ad absurdum*) erfand, eine Beweistechnik, die gerade auf dem Gebiet der Diophantischen Approximation ganz wesentlich verwendet wird. Zweiterer betrachtete regelmässige n -Ecke, die einem Kreis eingeschrieben bzw. umschrieben werden und zeigte damit, dass man den Kreisumfang (also im Wesentlichen π) beliebig genau durch Brüche approximieren kann. Am Beispiel des 96-Ecks fand er

$$3\frac{10}{71} < \pi < 3\frac{1}{7}.$$

Man beachte, dass darin implizit die erste Fehlerabschätzung einer Approximation enthalten ist!

Um den Ursprung der Bezeichnung *diophantische* Approximation zu rechtfertigen, muss nun wohl noch auf den Beitrag von Diophantus von Alexandria (2. Jahrhundert nach Christus) eingegangen werden. Ihm war es vorbehalten, Verhältnisse ganzer Zahlen erstmals als gleichberechtigte Zahlen anzusehen, was ihm in seinem Studium der Lösbarkeit von Gleichungen in ganzzahligen Verhältnissen zu Gute kommt. Sein diesbezügliches Werk *Arithmetica* wurde bis ins 17. Jahrhundert von den bedeutendsten Mathematikern studiert und Fermat soll am Rande einer der Seiten des Buches seine berühmte Vermutung über die Unlösbarkeit der Gleichung $X^n + Y^n = Z^n$ für $n > 2$ in ganzen Zahlen geschrieben haben.

Das rechtfertigt allerdings noch nicht die Verbindung seines Namens mit der Theorie der Approximation reeller Zahlen durch rationale, in der Tat sollte die Erkenntnis des Zusammenhangs zwischen der Lösbarkeit von Gleichungen und der Güte der Approximierbarkeit von gewissen Zahlen der Mathematik des 20. Jahrhunderts vorbehalten bleiben, wie wir noch sehen werden.

Machen wir also einen Sprung in die Neuzeit, genauer gesagt in die Mitte des 19. Jahrhunderts. Die Mathematik hat unzählige Fortschritte gemacht, unter anderem was den Zahlbegriff und die Algebra betrifft.

So hat sich etwa die Dezimalentwicklung von Zahlen durchgesetzt, die Entwicklung reeller Zahlen in Kettenbrüche wurde untersucht. Das Studium von Gleichungen und deren Lösbarkeit hat die Theorie der algebraischen Körpererweiterungen entstehen lassen und die Zahlen in diesen Erweiterungen tragen den Namen *algebraische Zahlen*. Die genaue Beschreibung dieser Zahlen liefert folgende

Definition 1. Sei F ein über \mathbb{Q} irreduzibles Polynom vom Grad d mit ganzen Koeffizienten. Ist $\alpha \in \mathbb{R}$ eine Nullstelle von F , d.h. $F(\alpha) = 0$, so heisst α eine algebraische Zahl vom Grad d .

So sind etwa die rationalen Zahlen genau die algebraischen Zahlen vom Grad 1 als Lösungen der linearen Gleichung $bX - a = 0$, was $X = \frac{a}{b}$ bedingt. Lösungen von quadratischen Gleichungen sind algebraische Zahlen vom Grad 2, sofern sie nicht rational sind, usw. Die obige Definition ermöglicht demnach eine Klassifikation aller algebraischen Zahlen und zwei Fragen drängen sich geradezu auf: welche Eigenschaften unterscheiden Zahlen von verschiedenem Grad und sind alle reelle Zahlen, also etwa auch π und e , algebraisch?

Hinsichtlich der ersten Frage liefert die Kettenbruchentwicklung eine partielle Antwort: rationale Zahlen entsprechen genau den endlichen Kettenbrüchen und dank Legendre war bereits bekannt, dass eine reelle Zahl genau dann quadratisch irrational ist, wenn ihre Kettenbruchentwicklung periodisch ist.

Erstaunlicherweise ermöglicht aber auch eine Approximationseigenschaft, die rationalen Zahlen von allen anderen zu unterscheiden: Dirichlet zeigte 1842 den

Satz 2. Sei α eine reelle Irrationalzahl. Dann existieren unendlich viele $p, q \in \mathbb{Z}$, $q > 0$ und $\text{ggt}(p, q) = 1$ mit

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Was kann man allgemein über die Approximierbarkeit von algebraischen Zahlen vom Grad d aussagen? Lässt sich vielleicht eine Eigenschaft finden, die algebraische Zahlen vom Grad d erfüllen müssen und von der man zeigen kann, dass es reelle Zahlen gibt, die diese Eigenschaft für kein festes d erfüllen? Dies würde die zweite gestellte Frage dahingehend beantworten, dass nicht alle reellen Zahlen Nullstellen von Polynomen mit ganzen Koeffizienten sind. In der Tat hat Liouville 1842 solch eine Eigenschaft gefunden, nämlich die in folgendem Sinne schlechte Approximierbarkeit algebraischer Zahlen durch rationale:

Satz 3. Sei α eine reelle algebraische Zahl vom Grad d . Dann existiert eine Konstante $c(\alpha)$, sodass für alle $p, q \in \mathbb{Z}$, $q > 0$, gilt:

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha)}{q^d}.$$

In der Tat ermöglicht dieser Satz die Konstruktion von nicht algebraischen reellen Zahlen wie zum Beispiel

$$z := \sum_{i=1}^{\infty} 10^{-i!} = 0,11000100000\dots,$$

eine Zahl bei der die Anzahl der Nullen zwischen zwei aufeinanderfolgenden Einsen faktoriell anwächst. Das bewirkt, dass z "zu gut" durch die rationalen Zahlen der Gestalt

$$\sum_{i=1}^N 10^{-i!}$$

approximierbar ist, um einem Polynom von festem Grad d zu genügen.

Wir haben also bisher ein positives (Dirichlet) und ein negatives (Liouville) Ergebnis hinsichtlich der Approximierbarkeit kennengelernt und wir wollen an dieser Stelle kurz die wesentlichen Punkte dieser Resultate festhalten.

- Die Güte der Approximierbarkeit von α durch eine rationale Zahl $\frac{p}{q}$ wird optimal durch eine Funktion des Nenners q ausgedrückt
- $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ hat für alle $\alpha \in \mathbb{R}$ unendlich viele Lösungen
- $|\alpha - \frac{p}{q}| < \frac{1}{q^{d+\epsilon}}$ hat für alle $\epsilon > 0$ und beliebige α vom Grad $\leq d$ höchstens endlich viele Lösungen
- Für $d = 2$ ist der Exponent 2 im Nenner bestmöglich.
 $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$ ist die schärfste Ungleichung, die für alle α unendlich viele Lösungen besitzt. (Hurwitz)

Wenn man die Punkte 2 und 3 der obigen Liste betrachtet, so kann man anhand der Formulierung der beiden Ungleichungen erkennen, dass die Approximierbarkeit einer Zahl auf folgende Weise ein Mass für die Irrationalität dieser Zahl liefert:

Definition 4. Sei $\alpha \in \mathbb{R}$ und M die Menge der $\mu \in \mathbb{R}^+$ für die

$$0 < |\alpha - \frac{p}{q}| < \frac{1}{q^\mu}$$

nur endlich viele Lösungen hat.

Dann heisst $\mu(\alpha) := \inf\{M\}$ das **Irrationalitätsmass** von α .

Das soeben eingeführte Mass definiert nun eine neue Hierarchie auf der Menge aller reellen Zahlen und es stellt sich die Frage, wie diese für algebraische Zahlen mit der durch den Grad bestimmten kompatibel ist. Um diese zu beantworten, muss die genaue Abhängigkeit von $\mu(\alpha)$ mit dem Grad von α geklärt werden, ein Unterfangen, das die Entwicklung der gesamten Zahlentheorie der ersten Hälfte des 20. Jahrhunderts geprägt hat. Die folgende Tabelle gibt Aufschluss über die Fortschritte hinsichtlich der Abschätzung von $\mu(\alpha)$ für algebraische Zahlen α vom Grad d :

- Axel Thue (1909): $\mu(\alpha) \leq d/2 + 1$
- C.L. Siegel (1921): $\mu(\alpha) \leq 2\sqrt{d}$
- G. Dyson (1947): $\mu(\alpha) \leq \sqrt{2d}$
- K.F. Roth (1955): $\mu(\alpha) = 2$

Das letzte Ergebnis ist der berühmte Satz von Roth, für dessen Beweis seinem Autor die Fieldsmedaille verliehen wurde. Die genaue Formulierung lautet:

Satz 5. *Sei α eine reelle algebraische Zahl vom Grad $d \geq 2$. Dann hat für alle $\epsilon > 0$ die Ungleichung*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\epsilon}}$$

höchstens endlich viele rationale Lösungen $\frac{p}{q}$.

Unabhängig von deren Grad gilt also $\mu(\alpha) = 2$ für alle irrationalen algebraischen Zahlen. Im Unterschied zum Satz von Liouville im Fall $d = 2$ bedeutet dies aber *nicht*, dass für jedes α eine Konstante $c(\alpha)$ existiert, sodass

$$\left| \alpha - \frac{p}{q} \right| > \frac{c(\alpha)}{q^2}.$$

Insofern besteht doch ein kleiner Unterschied zwischen quadratischen Irrationalzahlen und algebraischen Zahlen vom Grad grösser als 2.

Der Satz von Roth liefert auch ein sehr gutes Beispiel dafür, wie die Approximierbarkeit algebraischer Zahlen ausgenutzt werden kann, um gewisse Gleichungen zu untersuchen und so die (späte) Rechtfertigung für die Bezeichnung Diophantische Approximation.

Um dies zu erläutern zeigen wir die folgende, erstmals von Thue bewiesene Behauptung:

Satz 6. *Sei $F(x, y)$ ein homogenes irreduzibles Polynom vom Grad $d \geq 3$.*

Dann hat die Gleichung

$$F(x, y) = m$$

für festes m nur endlich viele Lösungen.

Wir schreiben zunächst $F(x, y) = y^d f\left(\frac{x}{y}\right)$, wobei f ein irreduzibles Polynom vom Grad d in einer Variable ist. Der Fundamentalsatz der Algebra liefert über \mathbb{C} die Zerlegung

$$f\left(\frac{x}{y}\right) = a \left(\frac{x}{y} - \alpha_1\right) \cdots \left(\frac{x}{y} - \alpha_d\right).$$

Dabei ist a der führende Koeffizient von f und wir bemerken, dass die Tatsache, dass alle α_i verschieden sind (f ist ja irreduzibel) bewirkt, dass der Betrag $|\alpha_i - \frac{x}{y}|$ für alle bis auf höchstens einen Index i grösser sein muss als $\frac{1}{2} \min_{i \neq j} |\alpha_i - \alpha_j|$. Nennen wir diese Grösse c und nehmen

an, dass gerade der erste Faktor womöglich sehr klein ist, so erhalten wir:

$$|F(x, y)| \geq |a|c^{d-1}|\alpha_1 - \frac{x}{y}||y^d|.$$

Nun kommt der Satz von Roth ins Spiel: er garantiert, dass

$$|\alpha_1 - \frac{x}{y}| > \frac{c(\alpha_1, \epsilon)}{|y|^{2+\epsilon}}$$

und wir können dies in der Abschätzung von $|F(x, y)|$ verwenden. Fasst man $|a|c^{d-1}$ unter der Bezeichnung C zusammen, so folgt:

$$|F(x, y)| \geq C|y|^{d-2-\epsilon}.$$

Nun sind wir aber an Lösungen von $F(x, y) = m$ interessiert, das heisst die linke Seite der obigen Ungleichung ist beschränkt und somit auch die rechte. Da laut Voraussetzung $d \geq 3$ ist und ϵ kleiner als 1 gewählt werden kann, ist der Exponent von $|y|$ allerdings positiv, was wiederum bewirkt, dass y , und in der Folge auch x , beschränkt sein muss. Es gibt also nur endlich viele Lösungen (x, y) der besagten Gleichung, wie behauptet.

Zugegeben, das ist eine sehr spezielle Gleichung, aber auch die Approximationstheorie hat sich enorm weiterentwickelt. Oft treten Probleme auf, bei denen es darauf ankommt, zwei oder mehr Zahlen gleichzeitig, d.h. durch rationale Zahlen mit demselben Nenner, zu approximieren. Man spricht dann von *simultaner Approximation*. Eine Verallgemeinerung des Satzes von Roth im zweidimensionalen Fall lautet zum Beispiel:

$$\begin{aligned} |\alpha_1 - \frac{p_1}{q}| &< \frac{1}{q^{\frac{3}{2}+\epsilon}} \\ |\alpha_2 - \frac{p_2}{q}| &< \frac{1}{q^{\frac{3}{2}+\epsilon}} \end{aligned}$$

hat nur endlich viele Lösungen, wenn 1, α_1 und α_2 linear unabhängig über \mathbb{Q} sind.

Diese Aussage wiederum ist ein Spezialfall des *Teilraumsatzes* von W. Schmidt, der umfassendsten Verallgemeinerung des Ergebnisses von Roth. Dieser Satz hat die Untersuchung von ganzen Klassen diophantischer Gleichungen revolutioniert und stellt auch heute noch eines der wichtigsten Forschungsgebiete innerhalb der Diophantischen Approximation dar.

Die mathematische Evolution schreitet also auch auf diesem Gebiet mit grossen Schritten voran und der Einblick, den der vorliegende Artikel geben soll, stellt eher einen Rückblick als einen Ausblick dar. Letzterer lässt sich allerdings umso besser geniessen, je genauer man seinen Hintergrund kennt!