DIOPHANTISCHE APPROXIMATION
SOMMERSEMESTER 2013

STEFFEN MÜLLER
BEREICH AZ
FACHBEREICH MATHEMATIK
UNIVERSITÄT HAMBURG

1. Klassische Diophantische Approximation

1.1. **Beste Approximationen.** Die klassische diophantische Approximation ist ein Teilgebiet der Zahlentheorie und beschäftigt sich mit der Frage, wie gut sich reelle Zahlen durch rationale Zahlen approximieren lassen. Hierbei muss zunächst präzisiert werden, was wir unter „gut" verstehen, denn die rationalen Zahlen liegen dicht in den reellen Zahlen, d.h. es gibt für jede reelle Zahl a und jede Schranke $\epsilon > 0$ unendlich viele rationale Zahlen p/q mit

$$\left|a - \frac{p}{q}\right| < \epsilon\,. \tag{1}$$

Eine Möglichkeit „gute" Approximationen zu definieren ist die folgende:

Definition 1.1. Sei $a \in \mathbb{R}$. Wir sagen, dass $p/q \in \mathbb{Q}$ mit $q \geq 1$ eine *beste Approximation* von a ist, wenn

$$|qa - p| < |q'a - p'|$$

für alle p', $q' \in \mathbb{Z}$ mit $|q'| < |q|$ gilt.

D.h. wir fordern von einer besten Approximation p/q von a, dass wir a nicht besser durch eine rationale Zahl mit kleinerem Nenner als q approximieren können.

Eine Motivation besteht darin, dass wir eine reelle Zahl a möglichst gut durch eine endliche Datenmenge beschreiben möchten. Hierzu kann man natürlich die Dezimalentwicklung von a verwenden und diese nach endlich vielen Stellen abschneiden; die besten Approximationen von a erlauben aber oft eine deutlich genauere Beschreibung von a bei ähnlicher Datenmenge und haben zusätzliche vorteilhafte mathematische Eigenschaften. Diese Sachverhalte werden wir in der Vorlesung präzisieren.

Beispiel 1.2. Die vier kleinsten besten Approximationen von π lauten

$$3,\ \frac{22}{7},\ \frac{333}{106},\ \frac{355}{113}.$$

Hierbei ist die Approximation 3 seit mindestens 3000 Jahren bekannt, die Approximationen $\frac{22}{7}$ und $\frac{355}{113}$ wurden von Archimedes (3. Jahrhundert v.Chr) bzw. Zu Chongzhi (5. Jahrhundert n. Chr.) gefunden.

Beispiel 1.3. (siehe auch [Wol13, §1.2]) Die Anzahl der Stunden des Sonnenjahres ist kein ganzzahliges Vielfaches von 24. Wie also findet man ein möglichst akkurates Kalendersystem? Das Sonnenjahr besteht aus ca. $365+a$ Tagen, wobei a eine reelle Zahl ist mit $a \approx \frac{419}{1730}$. Legt man also fest, dass ein Jahr aus 365 Tagen besteht, so verschiebt sich z.B. die Sommersonnenwende ca. alle 4 Jahre um einen Tag.
Der von Caesar eingeführte *Julianische Kalender* approximiert a durch $1/4$, es wird also alle 4 Jahre ein Schaltjahr eingefügt. Dieser Kalender wurde in Europa verwendet, bis 1582 von Papst Gregor XIII. der bis heute benutzte *Gregorianische Kalender* eingeführt wurde. Hier wird a durch $\frac{97}{400}$ approximiert; das Schaltjahr wird also in 400 Jahren genau dreimal weggelassen. Hierbei ist festzuhalten, dass $\frac{1}{4}$ und $\frac{194}{801}$ beste Approximationen von a sind (beachte $\frac{97}{400} = \frac{194}{800} \approx \frac{194}{801}$).

Nun stellt sich die Frage, wie man beste Approximationen zu einer reellen Zahl a finden kann. Das von Lagrange 1770 bewiesene Gesetz der besten Approximationen sagt aus, dass eine rationale Zahl p/q genau dann eine beste Approximation von a ist, wenn sie ein Näherungsbruch der sogenannten *Kettenbruchentwicklung* von a ist. Wir werden die Theorie der Kettenbruchentwicklungen ausführlich behandeln. Sie liefert neben Anwendungen in der diophantischen Approximation auch eine Möglichkeit, die reellen Zahlen aus den rationalen Zahlen zu konstruieren.

1.2. **Approximationsexponenten.** Eine andere klassische Fragestellung der diophantischen Approximation besteht darin zu untersuchen, ,,wieviele" teilerfremde Paare (p, q) die Ungleichung (1) erfüllen, wenn ϵ von q abhängt.

Definition 1.4. Wir sagen $a \in \mathbb{R}$ ist *approximierbar von Ordnung* n durch rationale Zahlen, wenn es eine Konstante $c = c(a, n)$ gibt, sodass unendlich viele teilerfremde Paare $(p, q) \in \mathbb{Z}^2$ die Ungleichung

$$\left| a - \frac{p}{q} \right| < \frac{c}{q^n} \tag{2}$$

erfüllen. Wir nennen das Supremum $\mu(a) \in \mathbb{R} \cup \{\infty\}$ der Menge aller positiven reellen Zahlen n sodass a approximierbar von Ordnung n ist, den *Approximationsexponenten* von a.

Genauer werden wir uns mit folgenden Problemen beschäftigen:

(I) Gegeben $a \in \mathbb{R}$, finde eine obere Schranke für den Approximationsexponenten $\mu(a)$.
(II) Gegeben $a \in \mathbb{R}$, finde eine untere Schranke für den Approximationsexponenten $\mu(a)$.
(III) Welche Rückschlüsse auf Eigenschaften von a lassen obere/untere Schranken für $\mu(a)$ zu?

Wir listen nun die Hauptresultate zu den Problemen (I) und (II) auf. Nicht alle werden in der Vorlesung bewiesen werden, wir werden jedoch stets versuchen, wenigstens die ungefähre Beweisidee zu besprechen. Für einige dieser Resultate benötigen wir folgende Begriffe, die insbesondere in der algebraischen Zahlentheorie eine wichtige Rolle spielen.

Definition 1.5. Sei $a \in \mathbb{C}$. Wir sagen a ist *algebraisch*, falls es ein Polynom $P(x) \in \mathbb{Q}[x]\setminus\{0\}$ gibt, sodass a eine Nullstelle von P ist. Andernfalls nennen wir a *transzendent*. Ist $P(x) \in \mathbb{Q}[x] \setminus \{0\}$ irreduzibel mit $P(a) = 0$, dann nennen wir $\deg(P)$ den *Grad* von a und schreiben $\deg(a) = \deg(P)$.

(i) Ist $a \in \mathbb{Q}$, so ist $\mu(a) = 1$.
(ii) Ist $a \in \mathbb{R}$ irrational, so gilt $\mu(a) \geq 2$ (Dirichlet, 1842).
(iii) Ist $a \in \mathbb{R}$ algebraisch, so gilt
  (1) $\mu(a) \leq \deg(a)$ (Liouville, 1844),
  (2) $\mu(a) \leq \deg(a)/2 + 1$ (Thue, 1909),
  (3) $\mu(a) \leq 2$ (Roth, 1955).

Hierbei sind die Sätze von Thue und Roth natürlich Verbesserungen des Satzes von Liouville. Aus (i) und (iii) folgt, dass sich rationale und, allgemeiner, algebraische Zahlen nicht besonders gut durch rationale Zahlen approximieren lassen. Diese Ergebnisse sind natürlich auch im Kontext von Problem (III) interessant. Z.B. kann man durch ihre Anwendung die Irrationalität oder sogar Transzendenz bestimmter reeller Zahlen beweisen. Wir werden auf diese Frage in Abschnitt 2 zurückkommen.

Schließlich lassen sich alle oben gestellten Fragen auch auf den mehrdimensionalen Fall ausdehnen; man spricht in diesem Kontext von *simultaner Approximation* eines Tupels $(a_1, \ldots, a_n) \in \mathbb{R}^n$. Wir werden uns allerdings aus Zeitgründen auf den eindimensionalen Fall konzentrieren und Aussagen über simultane Approximation lediglich erwähnen.

2. Transzendenztheorie

2.1. **Transzendenz und Irrationalität.** Aus den Cantorschen Diagonalargumenten folgt, dass die Menge der rationalen Zahlen abzählbar, die der reellen Zahlen jedoch überabzählbar ist. Also sind die meisten reellen Zahlen a irrational. Die Irrationalität einer gegebenen reellen Zahl nachzuweisen ist jedoch außer in Ausnahmefällen (z.B. $a = \sqrt{2}$) ein schwieriges Problem. So konnte die Irrationalität von e erst 1737 von Euler und die Irrationalität von π erst 1761 von Lambert nachgewiesen werden. Bis heute ist nicht bekannt ob $e \pm \pi$, $e \cdot \pi$ oder e/π irrational sind, dies wird allerdings vermutet.

Wir haben bereits in Abschnitt 1.2 *algebraische* und *transzendente* Zahlen definiert (siehe Definition 1.5). Es ist klar, dass eine transzendente Zahl irrational sein muss. Damit erhalten wir die Irrationalität einer gegebenen reellen Zahl a, wenn wir zeigen können, dass a transzendent ist. Nebenbei bemerkt sind die meisten reellen Zahlen transzendent; man sieht relativ leicht, dass die Menge $\overline{\mathbb{Q}}$ der algebraischen Zahlen abzählbar ist.

Allerdings ist es (wenig überraschend) i.d.R. schwieriger, die Transzendenz einer Zahl a nachzuweisen als ihre Irrationalität. Ein möglicher Ansatz sieht folgendermaßen aus: Man versucht den Approximationsexponenten $\mu(a)$ (siehe Definition 1.4) von unten abzuschätzen. Verletzt diese untere Schranke die Abschätzungen, welche sich aus den Sätzen von Liouville oder Roth ergeben, so kann a nicht algebraisch, sondern muss transzendent sein.

Mit dieser Methode konnte Liouville 1844 die Transzendenz sogenannter Liouville-Zahlen nachweisen, wobei eine reelle Zahl *Liouville-Zahl* heißt, wenn

$\mu(a) = \infty$ ist. Man kann zeigen, dass Liouville-Zahlen existieren, allerdings sind sie selten (die Menge der Liouville-Zahlen ist überabzählbar, hat aber Lebesgue-Maß 0). Da sie aber die ersten Zahlen waren, deren Transzendenz bewiesen wurde, kommt ihnen dennoch eine wichtige Rolle zu.

2.2. **Transzendenz von e und π.** Um die Transzendenz ,,natürlich" auftretender Zahlen nachzuweisen, braucht man aber meistens andere Methoden als die von Liouville. Allerdings werden wir sehen, dass dennoch ein starker Zusammenhang zwischen diophantischer Approximation und Transzendenztheorie besteht, der sich vor allem in der Ähnlichkeit der verwendeten Methoden äußert. Die erste ,,natürlich" auftretende Zahl, deren Transzendenz bewiesen werden konnte, ist die Eulersche Zahl e.

Satz 2.1. *(Hermite, 1873) Die Eulersche Zahl e ist transzendent.*

Neben der Relevanz des Resultats ist vor allem die Beweistechnik interessant, die sich in Grundzügen allerdings schon bei Liouville findet. Hermite konstruiert sogenannte *Hilfsfunktionen*, die unter der Annahme, dass e algebraisch ist, Eigenschaften haben, welche einander widersprechen. Daher muss e transzendent sein.

Fast alle bis heute bekannten Transzendenzbeweise laufen nach einem ähnlichen Muster; auch einige wichtige Sätze aus der diophantischen Approximation, wie z.B. die oben erwähnten Sätze von Thue und Roth, wurden nach einem ähnlichen Schema bewiesen. Dies macht für viele Mathematiker sowohl ein Problem als auch eine große Chance dieses Forschungsgebiets aus: Im Prinzip werden seit 1844 ähnliche Ideen variiert bzw. verfeinert (allerdings mit immer ausgeklügelteren Methoden, die z.B. Roth und Baker die Fieldsmedaille einbrachten). Eine grundlegend neue Idee könnte also sofort zu bahnbrechenden Ergebnissen führen.

Neben der Transzendenz von e wurde im 19. Jahrhundert besonders nach einem Beweis für die Transzendenz von π gesucht. Der Hauptgrund hierfür war folgendes Problem, welches seit den alten Griechen von vielen als eines der Hauptprobleme der Geometrie angesehen wurde:

Problem 2.2. *(Quadratur des Kreises) Man konstruiere in endlich vielen Schritten mit Zirkel und Linear zu einem gegebenen Kreis S ein Quadrat, das den gleichen Flächeninhalt wie S hat.*

Bis ins 17. Jahrhundert gab es nur sehr wenige nennenswerte Fortschritte. Durch die Methoden der von Descartes entwickelten analytischen Geometrie konnte man zeigen: Ist die Quadratur des Kreises möglich, so ist $\sqrt{\pi}$ (und damit auch π) algebraisch.

Der folgende Satz wurde 1882 von Lindemann bewiesen;

Satz 2.3. *(Lindemann, 1842) Sei α eine algebraische Zahl. Dann ist e^{α} transzendent.*

Hieraus folgt:

Korollar 2.4. *Die Kreiszahl π ist transzendent.*

Beweis. Wegen $i^2+1=0$ ist $i \in \mathbb{C}$ algebraisch. Wäre π algebraisch, so wäre auch πi algebraisch, also müsste nach Satz 2.3 ebenfalls

$$-1 = e^{\pi i}$$

transzendent sein, was aber offensichtlich falsch ist. $\square$

Korollar 2.5. *Die Quadratur des Kreises ist unmöglich.*

Trotz dieses Resultats gibt es bis heute immer wieder Veröffentlichung (i.d.R. von Nichtmathematikern), in denen die Möglichkeit der Quadratur des Kreises behauptet oder sogar „bewiesen" wird. Der amerikanische Arzt Edwin J. Goodwin veröffentlichte 1894 eine solche Arbeit und versuchte sogar deren Richtigkeit im Bundesstaat Indiana per Gesetz festlegen zu lassen (die sogenannte „Indiana Pi Bill")! Aus seiner Arbeit lässt sich allerdings $\pi = 3.2$ ableiten...

2.3. **Neuere Entwicklungen.** Weierstraß bewies 1885 eine wichtige allgemeinere Version von Satz 2.3. David Hilbert hat in einer berühmten Rede vor dem Internationalen Mathematikerkongress 1900 in Paris eine Liste von 23 Problemen vorgestellt, von denen er erwartete, dass sie die Entwicklung der Mathematik des 20. Jahrhunderts stark beeinflussen würden. Das siebte Problem auf dieser Liste wurde damals als das wichtigste Problem der Transzendenztheorie erachtet.

Problem 2.6. *(Hilberts siebtes Problem, 1900) Man beweise, dass α^β stets transzendent ist, wenn $\alpha \neq 0, 1$ algebraisch und β irrational und algebraisch ist.*

Hilbert hielt dies für eines der schwierigsten Probleme auf seiner Liste, allerdings wurde es bereits 1934 von Gelfond und Schneider unabhängig voneinander bewiesen.

Das wichtigste seitdem bewiesene Transzendenzresultat stammt von Baker (1970) und impliziert insbesondere die Transzendenz von Zahlen der Form

$$\alpha_1^{\beta_1} \cdots \alpha_n^{\beta^n},$$

wobei alle $\alpha \neq 0, 1$ algebraisch sind, die β_i ebenfalls algebraisch sind und die zusätzliche Bedingung erfüllen, dass

$$\{1, \beta_1, \ldots, \beta_n\}$$

linear unabhängig über $\mathbb{Q}$ ist. Allgemeiner nennt man die Bakersche Theorie auch *Theorie der Linearformen in Logarithmen.* Sie ist bis heute eines der aktivsten Forschungsgebiete der Zahlentheorie.

3. Anwendung: Diophantische Gleichungen

3.1. **Diophantische Gleichungen.** Die Resultate der diophantischen Approximation und der Transzendenztheorie werden besonders erfolgreich im Gebiet der *diophantischen Gleichungen* angewandt. Wir definieren hier eine diophantische Gleichung als eine Gleichung

$$A : P(x_1, \ldots, x_n) = 0\,,$$

wobei $n \in \mathbb{N}$ und $P \in \mathbb{Q}[x_1, \ldots, x_n]$ sind. Allerdings können und werden wir stets o.B.d.A. $P \in \mathbb{Z}[x_1, \ldots, x_n]$ annehmen. Typischerweise stellt man sich folgende Fragen:

(a) Hat A eine rationale Lösung $(x_1, \ldots, x_n) \in \mathbb{Q}^n$?
(b) Hat A eine ganzzahlige Lösung $(x_1, \ldots, x_n) \in \mathbb{Z}^n$?
(c) Hat A endlich viele rationale/ganzzahlige Lösungen?
(d) Falls A endlich viele rationale/ganzzahlige Lösungen hat, kann man sie alle angeben?
(e) Falls A unendlich viele rationale/ganzzahlige Lösungen hat, kann man sie parametrisieren oder aus endlich vielen Lösungen konstruieren?

Das 10. Problem auf der bereits erwähnten Liste von Hilbert lässt sich folgendermaßen formulieren:

Problem 3.1. *(Hilberts zehntes Problem, 1900) Man gebe einen Algorithmus an, der für eine beliebige diophantische Gleichung entscheidet, ob sie eine ganzzahlige Lösung hat.*

Es dauerte bis 1970, bis Matiyasevich schließlich in seiner Dissertation beweisen konnte, dass dieses Problem unlösbar ist (eine Möglichkeit, die Hilbert gar nicht erst in Betracht zog): Es gibt Polynome $P \in \mathbb{Z}[x_1, \ldots, x_n]$, für die sich nicht entscheiden lässt ob sie eine ganzzahlige Lösung besitzen. Man kann solche Polynome sogar explizit konstruieren; die minimale Anzahl von Variablen eines derzeit bekannten solchen Polynoms lautet 11 (konstruiert von Sun).

Nichtsdestotrotz kann man darauf hoffen, die aufgelisteten Fragen (a)–(e) beantworten zu können, wenn man die Anzahl der Variablen beschränkt. Für $n = 1$ gibt es einen offensichtlichen Algorithmus, der Frage (b) für alle $P \in \mathbb{Z}[x_1]$ beantwortet. Für $n = 2$ gibt es eine Vermutung von Stoll, die besagt, dass es einen Algorithmus gibt, der Frage (b) für alle $P \in \mathbb{Z}[x_1, x_2]$ beantwortet.

3.2. **Diophantische Gleichungen und diophantische Approximation.** Wir werden im Wesentlichen zwei Anwendungen der diophantischen Approximation auf diophantische Gleichungen besprechen. Zunächst lassen sich die Resultate (iii.1)–(iii.3) verwenden um die Endlichkeit der Lösungsmenge in ganzen Zahlen bestimmter diophantischer Gleichungen zu zeigen. Wir geben hier nur ein Beispiel an:

Satz 3.2. *(Thue) Seien a, b, $c \in \mathbb{Z}$ mit $abc \neq 0$. Dann hat die Gleichung*

$$ax^3 + by^3 = c$$

nur endlich viele Lösungen $(x, y) \in \mathbb{Z}^2$.

Mit dem Satz von Roth und der Theorie der Linearformen in Logarithmen von Baker lässt sich die Endlichkeit der Lösungsmenge in ganzen Zahlen vieler weiterer diophantischer Gleichungen zeigen. Je nach verfügbarer Zeit werden wir weitere Beispiele in der Vorlesung behandeln.

Allerdings möchte man, wenn man die Endlichkeit der Lösungsmenge erst einmal bewiesen hat, natürlich auch Problem (iv) lösen, d.h. man sucht nach einem Algorithmus, der alle ganzzahligen Lösungen auflistet. Das Hauptproblem ist hierbei, dass fast alle aus der diophantischen Approximation und der Transzendenztheorie verwendeten Argumente letzlich Widerspruchsargumente sind. Insbesonders liefern sie keine oberen Schranken für die ,,Größe" der ganzzahligen Lösungen.

Eine Ausnahme bildet hier die Bakersche Theorie. Diese liefert ebenfalls effektive obere Schranken für den maximalen Absolutbetrag der Koordinaten einer ganzzahligen Lösung, sodass sich diese im Prinzip alle auflisten lassen; allerdings sind diese Schranken typischerweise viel zu groß (ca. $10^{10^{600}}$) für praktische Anwendungen. Deshalb haben einige Zahlentheoretiker in den letzten Jahrzehnten versucht, kleinere Schranken zu erhalten und haben hierbei bemerkenswerte Fortschritte erzielt.

3.3. **Pellsche Gleichungen.** Eine weitere wichtige Anwendung besteht darin, Lösungen der *Pellschen Gleichung*

$$x^2 - dy^2 = 1 \tag{3}$$

für $d \in \mathbb{Q}$ zu parametrisieren, sofern diese unendlich viele Lösungen hat. Hierzu wird die oben bereits erwähnte Kettenbruchentwicklung von $\sqrt{d}$ verwendet. Mit ihrer Hilfe lässt sich eine sogenannte Fundamentallösung konstruieren, aus der sich alle anderen Lösungen generieren lassen. Der englische Mathematiker Pell, nach dem die Pellsche Gleichung (durch Euler) benannt wurde, hatte übrigens nichts mit ihnen zu tun. Diese Gleichungen wurden schon im 7. Jahrhundert von Indischen Mathematikern betrachtet. Die Pellschen Gleichungen sind besonders wichtig im Bereich der algebraischen Zahlentheorie und tauchen aber auch immer wieder in verschiedenen anderen Kontexten auf.

Beispiel 3.3. Das sogenannte Rinderproblem des Archimedes (es ist nicht klar, ob es tatsächlich auf Archimedes zurückgeht) ist ein klassisches Problem in der Theorie der diophantischen Gleichungen. Es besteht darin, aus einer Liste von Bedingungen die Anzahl der Rinder in der Herde des Sonnegottes abzuleiten. Dieses Problem wurde 1880 von Amthor durch Angabe einer Lösung der Pellschen Gleichung

$$x^2 - 4729494y^2 = 1 \tag{4}$$

lösen. Allerdings folgt aus dieser Lösung, dass die Herde des Sonnengottes mindestens ca. $7,76 \times 10^{206544}$ Rinder haben muss!

Literatur

[Bak90] Alan Baker. *Transcendental number theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1990.

[Lan95] Serge Lang. *Introduction to Diophantine approximations*. Springer-Verlag, New York, second edition, 1995.

[Sch80] Wolfgang M. Schmidt. *Diophantine approximation*, volume 785 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Ste05] Jörn Steuding. *Diophantine analysis*. Chapman & Hall/CRC, Boca Raton, FL, 2005.

[Wol13] Jürgen Wolfart. Diophantische Approximation, Vorlesungsskript. `http://www.math.uni-frankfurt.de/~wolfart/Lehre/Dioph.pdf`, 2013.