Frequently Asked Questions in Mathematics

Deutsche Übersetzung

The Sci.Math FAQ Team.
Editor: Alex López-Ortiz
E-Mail: alopezo@unb.ca

3. April 2002

Vorwort der Übersetzer

Es war uns eine große Freude die vorliegende FAQ zu übersetzen. Die sci.math FAQ stellt eine umfangreiche Sammlung an Fragen und allgemeinem Wissen dar, die für jeden Mathematiker und Mathematikinteressierten von Nutzen sein kann.

Gerade aber auch das spezielle Thema gestaltete die Übersetzung häufig schwierig und sehr anspruchsvoll. So war es ein oft nicht einfaches Problem einen deutschen Begriff für den jeweiligen englischen Fachausdruck zu finden. Zudem denken viele Mathematiker in Englisch, so dass es bisweilen auch mehr Sinn macht, das englische Wort stehen zu lassen als eine verstümmelnde deutsche Übersetzung anzugeben. Wir hoffen hierbei einen guten Mittelweg gefunden zu haben.

Das Original ist sehr schön und humorvoll geschrieben, wir haben versucht dies auch im Deutschen so weit wie möglich einzufangen.

Nun bleibt uns noch zu hoffen, dass Sie beim Lesen genauso viel Freude und Begeisterung empfinden, wie wir sie beim Übersetzen hatten.

Obwohl wir viel Zeit und Sorgfalt in den Text investiert haben, ist es natürlich nicht auszuschließen, dass sich noch irgendwo Fehler verstecken. In diesem Fall bitten wir um eine kurze Mail an eine der untenstehenden Adressen.

Sven Blumberg	Tjark Weber
sven.b1@web.de	tjark.weber@gmx.de

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Warum gibt es diese Liste der Frequently Asked Questions?

Das Netz, wie viele User das Internet nennen, und inbesondere die Newsgruppen (z.B. das Usenet) erschufen eine unvergleichbare Nachfrage an Wissen seit der Erfindung des Zeitungsdruckes. Überraschenderweise hat die Art des Wissens, welches von und durch die Usenet-Gemeinde verlangt wird, in den meisten Fällen nur wenig gemeinsam – sowohl in Struktur als auch in Inhalt – mit derzeit erhältlichen gedruckten Medien. Dies definiert das Usenet als eine Alternative zu Büchern, stellenweise sogar als einen Ersatz[1].

Im Netz werden zumeist Fragen gestellt, die sich auf dem Level eines Amateurs bewegen - selbst in den Fällen, in denen Profis sie in die Runde stellen. Aus dem gleichen Grund variiert die Qualität der Antworten stark zwischen schlichtweg falsch oder unverschämt bis zu Zusammenfassungen des Stands der Forschung des Themas in der Frage.

Eine andere Charakteristik der Kommunikation im Netz begründet sich in den Einschränkungen des Mediums. Eine wichtige Einheit in diesem Zusammenhang ist ein Bildschirm voll mit Text (ein scrit, zusammengesetzt aus „screen“ und „bit“). Beiträge, die diese Grenze überschreiten, werden normalerweise ignoriert.

Der Mangel an Gedächtnis des Mediums erzeugt eine stete Wiederholung von Themen und damit eine Verärgerung der „alten Hasen“ des Netzes. FAQ-Listen beheben einige dieser Unzulänglichkeiten dadurch, dass sie eine

[1]Es kann darüber gestritten werden, ob Bücher ihren Sinn und Zweck zur Befriedigung aller erfüllen. Darum, obwohl das Netz Bücher grundsätzlich ersetzen könnte, haben sich die Menschen dagegen entschieden. Stattdessen ist die Domäne des Netzes dadurch definiert, sehr von Büchern verschieden zu sein.

Zusammenstellung relevanter Informationen anbieten, die gleichzeitig nicht veralten.

Dalum wird normalerweise eine Liste der frequently asked questions mindestens einmal im Monat „geposted“ und auch regelmäßig erweitert. Und, was das Wichtigste für ein informationsbasiertes Produkt sein muss, FAQ Listen „verfallen“ zu einem bestimmten Datum, wie auch jede andere verderbliche Ware.

1.2 Frequently Asked Questions in der Mathematik?

Wenn ich den Inhalt dieser FAQ zur Mathematik in einem Satz beschreiben müsste, würde ich es *mathematischen Klatsch* oder vielleicht *nicht triviale mathematische Bagatellen* nennen.

Die FAQ-Liste ist eine Zusammenstellung von Wissen, die sowohl für den Profi als auch für den Amateurmathematiker interessant ist; sie variiert zwischen fortgeschrittenen Themen wie Wiles’ vorgeschlagenem Beweis der Fermatschen Vermutung bis zu einer Liste der Gewinner der Fields-Medaille.

Kapitel 2

Grundlagen

2.1 Algebraische Strukturen

Wir wollen versuchen eine kurze Erklärung der folgenden Konzepte zu geben:

- $\mathbb{N}$ ist ein Monoid.
- $\mathbb{Z}$ ist ein nullteilerfreier Ring.
- $\mathbb{Q}$ ist ein Körper.
- $\mathbb{R}$ ist ein vollständig geordneter Körper.
- $\mathbb{C}$ ist ein algebraisch abgeschlossener Körper.

Wenn Sie von einem Kind gebeten worden sind, ihm arithmetische Probleme zu geben, damit es seine gerade erworbenen Fähigkeiten in Additon und Subtraktion demonstrieren kann, dann bin ich sicher, dass Sie nach ein paar Fragen wie 2+3, 9-5, 10+2 und 6-4 versucht haben, ihm eine etwas schwierigere Aufgabe zu stellen, wie 4-7. '*Das ist nicht erlaubt*' wird die Antwort gewesen sein.

Was Sie dabei nicht realisiert haben ist, dass Sie und das Kind nicht nur von verschiedenen Objekten des Denkens (negativen Zahlen) ausgegangen sind, sondern von komplett verschiedenen *algebraischen Systemen*. In anderen Worten, einer Menge von Objekten (dies können natürliche Zahlen, ganze Zahlen oder auch reelle Zahlen sein) und einer Menge von Operationen oder Regeln, die festlegen, wie diese Objekte miteinander kombiniert werden können.

Wir wollen uns nun auf eine Tour durch verschiedene algebraische Systeme begebene, aber bevor wir beginnen diese zu definieren, wollen wir eine Struktur definieren, die einige der notwendigen Eigenschaften für Beispiele und Gegenbeispiele liefert, was uns helfen kann einige Definitionen zu verdeutlichen.

Wir wissen, dass jede Zahl, die durch sechs dividiert wird, entweder dabei einen Rest lässt oder die Division aufgeht (d.h. einen Rest 0 lässt). Im folgenden wollen wir alle Zahlen, die bei Division durch sechs den Rest n lassen, mit $[n]$ bezeichnen. Das bedeutet, dass z.B. 7, 55 und 1 alle als [1] geschrieben werden, wobei wir [1] die *Klasse* nennen, zu der sie gehören: so ist $7 \in [1]$, $55 \in [1]$ oder ein wenig technischer gesagt, sie sind alle äquivalent zu 1 modulo 6. Die ganze Menge dieser Klassen beinhaltet sechs Elemente. Daher wird dies auch Partitionierung von Zahlen in äquivalente Klassen (bzw. Äquivalenzklassen) genannt, weil es alle Zahlen in diese sechs Klassen teilt (oder partitioniert), und jede einzelne Zahl in einer Klasse ist äquivalent zu jeder anderen in der gleichen Klasse.

Nun ist es interessant zu untersuchen, ob und wie wir diese Klassen addieren oder multiplizieren können. Was könnten $[1]+[3]$ bedeuten? Wir können einfach naiv ausprobieren, was dies in der „normalen" Arithmetik bedeutet: $[1] + [3] = [1 + 3] = [4]$. Soweit so gut, untersuchen wir nun ein zweites Beispiel: $25 \in [1]$ und $45 \in [3]$, ihre Summe ist 70, was sicherlich in [4] liegt . An dieser Stelle können wir sehen, was oben mit einer Äquivalenz gemeint war: 25 ist äquivalent zu 1, soweit man sich für diese Addition interessiert. Sicherlich ist dies nur ein Beispiel, aber glücklicherweise kann es formal bewiesen werden, dass die Summe zweier Klassen immer die Klasse der Summe ist.

Dies ist nun aber das gleiche, was wir alle von der Addition von Stunden kennen. So ist z.B. 7 (Uhr) plus 6 Stunden 1 (Uhr). Dies ist nichts anderes als Addition von Stunden (modulo 12).

Der nette Teil ist nun aber die Multiplikation, wie wir später sehen werden. An dieser Stelle sei darauf hingewiesen, dass $[4] \times [5] = [20] = [2]$ korrekt ist und auch bewiesen werden kann, dass das Produkt von zwei Klassen gleich der Klasse des Produktes ist.

2.1.1 Monoide und Gruppen

Wir wollen nun eine *Gruppe* definieren.

Wir betrachten eine Menge von Objekten und eine Regel (die auch binäre oder zweistellige Operation genannt wird), die eine Kombination von zwei Elementen ermöglicht. Addition oder die Operation AND in einer Computersprache sind Beispiele für eine solche Regel.

Die Menge muss abgeschlossen unter der Operation sein, d.h. dass beim Kombinieren von zwei Elementen das Ergebnis wieder ein Element der Menge sein muss. Betrachten wir z.B. die Menge der geraden Zahlen, so ergibt sich bei Addition von zwei Elementen wieder eine gerade Zahl, also ein Element der Menge. Gehen wir nun allerdings zu den ungeraden Zahlen über, so ist die Summe von zwei ungeraden Zahlen keine ungerade Zahl. Somit wissen wir im Gegenzug, dass die Menge der ungeraden Zahlen und die Addition keine Gruppe bilden können. Einige Bücher fordern die Abgeschlossenheit in der Definition der binären Operation, andere hingegen fügen sie zu den Gruppenaxiomen hinzu, die nun folgen.

Die Menge mit der zugehörigen Operation wird eine Gruppe genannte, wenn die binäre Operation die folgenden Kriterien erfüllt:

- Die Operation ist assoziativ. Dies bedeutet, dass es irrelevant ist, wie man die Elemente, auf denen man operiert, gruppiert. Im obigen Beispiel bedeutet dies, dass $[1] + ([3] + [4]) = ([1] + [3]) + [4]$ gilt.

- Es gibt ein 1-Element. Dies bedeutet, dass es ein Element gibt, so dass alle Element in der Menge invariant unter der Operation mit diesem Element sind. Dies trifft z.B. auf die 0 bei der Addition oder die 1 bei der Multiplikation zu.

- Jedes Element besitzt ein Inverses bezüglich der binären Operation. D.h. kombiniert man ein Element mit seinem Inversen, so ergibt sich das 1-Element.

(Vorsicht bei dem letzen Axiom: -3 ist das Inverse von 3 bezüglich der Addition, da ihre Summe 0 ergibt, allerdings ist $\frac{1}{3}$ das Inverse von 3 bezüglich der Multiplikation, da $3 \times \frac{1}{3} = 1$ das 1-Element der Multiplikation ergibt.)

Somit ergibt sich, dass die Menge der natürlichen Zahlen $\mathbb{N}$ (mit Addition) keine Gruppe ist, da es z.B. zu 5 kein Inverses gibt. (In anderen Worten, es gibt keine natürliche Zahl, deren Summe mit 5 gerade 0 ergibt.) Also ist das dritte Axiom verletzt. Allerdings besitzt $\mathbb{N}$ eine gewisse Struktur, wie wir später sehen werden.

Mengen mit assoziativen Operationen (das erste Axiom oben) werden Halbgruppen genannt. Besitzen sie darüber hinaus auch noch ein 1-Element (zweites Axiom), so nennt man sie Monoide.

Unsere Menge von natürlichen Zahlen $\mathbb{N}$ zusammen mit der Addition ist Beispiel eines Monoids, eine Struktur, welche nicht ganz eine Gruppe ist, weil die Existenz eines Inversen bezüglich der Operation fehlt. (Dies ist der Grund, warum in der Grundschule $4 - 7$ nicht erlaubt ist.)

Was ist nun mit der Menge der ganzen Zahlen $\mathbb{Z}$, bilden sie eine Gruppe?

Die Frage an sich ist nun schon Unsinn. Warum? Wir haben nicht festgelegt unter welcher Operation. OK, sagen wir die Menge der ganzen Zahlen mit der Addition.

Nun gut, Addition ist assoziativ, unter Operation mit der 0 sind alle Zahlen invariant, und zu allen Zahlen n können wir $-n$ addieren und erhalten 0. Somit ist $\mathbb{Z}$ eine Gruppe.

Genauer gesagt ist $\mathbb{Z}$ sogar eine spezielle Art von Gruppe. Wenn wir die Operation auf zwei Elementen in einer beliebigen Reihenfolge ausführen können (d.h. $a + b = b + a$), dann nennen wir die Gruppe kommutativ oder abelsch, zu Ehren des norwegischen Mathematikers Henrik Abel. Nicht jede Operation ist abelsch: So ist z.B. $3 - 2$ sicherlich nicht das gleiche wie $2 - 3$. Unsere Menge $\mathbb{Z}$ ist also zusammen mit der Addition eine abelsche Gruppe.

2.1.2 Ringe

Nehmen wir nun eine abelsche Gruppe (zur Erinnerung: eine Menge mit einer binären Operation) und definieren eine zweite Operation, so erhalten wir größere Struktur, als wir sie in einer Gruppe haben.

Ist nun die zweite Operation assoziativ und ist sie distributiv mit der ersten Operation, so liegt ein sogenannter Ring vor. Es sei angemerkt, dass die zweite Operation weder ein 1-Element haben muss, noch müssen Inverse für alle Elemente vorhanden sein. Distributivität bedeutet, dass $a \times (b+c) = (a \times b) + (a \times c)$ gilt.

Die Menge der ganzen Zahlen (mit Addition und Multiplikation) ist ein kommutativer Ring (sogar mit 1-Element für die Multiplikation).

Kommen wir noch einmal auf unsere Menge von Restklassen zurück. Was passiert, wenn wir z.B. $[5] \times [1]$ multiplizieren? Wir erhalten $[5]$. Insbesondere können wir zusätzlich noch feststellen, dass einige unserer obigen Definitionen zutreffen: $[5]$ ist sein eigenes Inverses und $[1]$ ist ein 1-Element. Ebenso sieht man einfach ein (durch Erstellen einer Multiplikationstabelle), dass die Multiplikation kommutativ ist. Nehmen wir nun aber $[3]$ und $[2]$, welche beide von $[0]$ verschieden sind, so erhalten wir $[3] \times [2] = [0]$. Dies bringt uns zu der nächsten Definition. Sei a ein von 0 verschiedenes Element in einem kommutativen Ring. Finden wir nun ein von 0 verschiedenes Element b, so dass $a \times b = 0$ gilt, dann nennen wir a Nullteiler.

Ein kommutativer Ring wird nullteilerfrei genannt, wenn er keine Nullteiler besitzt. $\mathbb{Z}$ mit Addition und Multiplikation ist ein nullteilerfreier Ring. Unsere Menge von Restklassen hingegen ist, wie wir gesehen haben, kein nullteilerfreier Ring. Definieren wir eine ähnliche Menge von Restklassen bei der Division durch 5, so ergibt sich ein nullteilerfreier Ring.

Betrachten wir z.B. die Menge $\mathbb{Q}$ der rationalen Zahlen mit Addition und Multiplikation - ich verzichte auf den Beweis, dass dies ein Ring ist, aber denke, dass Sie in der Lage sein sollten, dies einfach mit obigen Axiomen nachzuweisen. $\mathbb{Q}$ zusammen mit der Addition ist sicherlich eine abelsche Gruppe.

Entfernen wir nun noch die 0, so ergibt sich zusammen mit der Multiplikation eine weitere abelsche Gruppe. Daher ist dies mehr als nur ein kommutativer Ring, wie wir im nächsten Abschnitt sehen werden.

2.1.3 Körper

Nun können wir einen Schritt weitergehen. Wenn die Elemente einen Ringes, außer der 0, eine abelsche Gruppe formen (mit der zweiten Operation), so ist dies ein Körper. Schreiben wir z.B. die Multiplikationstabelle von Resten bei der Division durch 5 auf, so sieht man, dass alle Anforderungen an eine Gruppe erfüllt sind:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(Sie haben sicherlich schon bemerkt, dass die Gruppe die Zahl fünf nicht enthält, da $[5] = [0]$ gilt.)

Warum ist nun aber die Menge der Restklassen bei Division durch sechs - ohne die 0 - unter Multiplikation keine Gruppe? Dies ist einfach: Da wir die 0 ausgeschlossen haben, ist das Ergebnis von $[2] \times [3]$ nicht in unserer Menge enthalten. Also ist die Operation nicht abgeschlossen.

2.1.4 Ordnungen

Einen gegebenen Ring können wir geordnet oder angeordnet nennen, wenn eine spezielle Teilmenge des Ringes sich in einer speziellen Art verhält. Wann immer zwei Elemente dieser speziellen Teilmenge addiert oder multipliziert werden, so ist das Ergebnis wieder in dieser speziellen Teilmenge enthalten. betrachten wir z.B. die negativen Zahlen in $\mathbb{R}$. Können sie solch eine spezielle Teilmenge sein? Zwar ist die Summe zweier negativer Zahlen stets negativ, doch ein Produkt negativer Zahlen ist positiv. Was ist aber mit den positiven Zahlen? Diese genügen unseren Anforderungen und werden in diesem Fall die Menge der positiven Elemente genannt. Nachdem wir nun die Definition eines angeordneten Ringes gegeben haben, können wir ebenso in der gleichen Weise einen angeordneten Körpers definieren.

Aber was soll dann ein vollständiger angeordneter Körper sein? Die Definition klingt ein wenig eklig: Der Körper ist vollständig, wenn jede nichtleere Teilmenge, die eine obere Schranke besitzt, auch eine kleinste obere Schranke hat.

Das bedarf nun zunächst einer Übersetzung, wobei wir so wenig Informationen wie möglich verlieren wollen. Eine Schranke ist etwas, das garantiert, dass alle Elemente einer Menge nur auf einer Seite von ihr sind. So sind z.B. alle negativen reellen Zahl kleiner als 100, also ist 100 eine Schranke (100 ist eine obere Schranke, da alle negativen Zahlen „unter ihr sind"). Es gibt allerdings viele andere Schranken: 1, 5, 26 wären andere Beispiele. Die Frage ist nun, welche von all diesen oberen Schranken ist die kleinste, das heißt, welche ist „der Rand"? Existiert diese immer?

Nehmen wir z.B. die rationalen Zahlen und betrachten die folgenden Zahlen:

$$1.4, 1.41, 1.414, 1.4142, 1.41421, \ldots$$

Jede dieser Zahlen ist rational (kann also als Bruch geschrieben werden), und sie nähern sich mehr und mehr einer Zahl an, die wir schon einmal gesehen haben (nehmen Sie z.B. einen Taschrechner und berechnen Sie die Quadratwurzel aus 2). Also können wir kurzerhand für diese Folge $\sqrt{2}$ schreiben. Sicherlich können wir eine obere Grenze für diese Folge finden: 3 wäre ein Beispiel, aber auch 1.5 oder 1.42. Was ist aber die kleinste? Es gibt keine! Zumindest keine rationale, denn egal welchen Bruch Sie mir geben, ich finde einen, der näher an $\sqrt{2}$ ist als Ihrer. Was ist aber mit $\sqrt{2}$ selber? $\sqrt{2}$ ist keine rationale Zahl (ich verzichte auf den Beweis, er ist aber nicht schwierig), somit kommt $\sqrt{2}$ nicht in Frage. Wollen Sie eine andere solche Folge, schauen Sie in das Kapitel m FAQ.

An dieser Stelle kommen die reellen Zahlen $\mathbb{R}$ ins Spiel. Zu jeder beschränkten Menge von reellen Zahlen gibt es eine kleinste obere Schranke (Diese kleinste obere Schranke wollen wir mit „sup" für Supremum bezeichnen.) Ebenso können wir nun auch alles herumdrehen und von unteren Schranken sprechen und von der größten unteren Schranke, die wir dann mit „inf" für Infimum bezeichnen wollen. Allerdings ist dabei das meiste vollkommen analog zu dem vorher über obere Schranken Gesagten.

Das sollte alles sein. Und über Jahre hinweg schien es tatsächlich so, als hätten wir alle Zahlen, die wir jemals brauchen würden.

Allerdings gab es ein kleines Manko, aber die meisten Leute schienen es einfach zu ignorieren. Nicht jede polynomiale Gleichung hatte eine Lösung. Ein einfaches Beispiel ist $x^2 + 1 = 0$. Obwohl dies so simpel ist, gibt es keine Lösung in $\mathbb{R}$. Es gab Antworten, welche auch Lösungen zu sein schienen. Allerdings konnte ihnen niemand Sinn zuschreiben, weshalb sie dann imaginäre Lösungen genannte wurden. Dies ist bedauernswert, denn diese Lösungen erhielten den Namen imaginäre Zahlen, der ihnen auch heutzutage anhaftet, obwohl wir längst realisiert haben, dass sie genauso wichtig wie die anderen Zahlen sind, die wir jahrhundertelang zuvor benutzt haben. Dies führt uns nun zu dem Höhepunkt unserer kleinen Exkursion: dem Körper der komplexen Zahlen, $\mathbb{C}$.

Wir können einen algebraisch abgeschlossenen Körper als einen Körper definieren, in dem jedes nicht-konstante Polynom eine Nullstelle besitzt. Huh! Kurzgesagt heißt das, dass so lange das Polynom keine konstante Zahl ist (was ohnehin nicht besonders spannend wäre), sondern z.B. wie $5x^3 - 2x^2 + 6$ aussieht, es immer eine Nullstelle besitzt, so lange man es als Polynom über $\mathbb{C}$ und nicht nur über $\mathbb{R}$ auffasst.

Es gibt eine weitere Definition, die genauso gut, aber möglicherweise einfacher ist: Ein Körper heißt algebraisch abgeschlossen, wenn jedes Polynom in Linearfaktoren zerfällt. Linearfaktoren sind Faktoren, in denen x in keiner Potenz größer gleich zwei vorkommt, also Ausdrücke der Form: $ax + b$. So kann z.B. x^2+x-6 als $(x+3)(x-2)$ faktorisiert werden. In $\mathbb{R}$ kann aber x^2+1 nicht faktorisiert werden. Über $\mathbb{C}$ hingegen haben wir $x^2 + 1 = (x + i)(x - i)$, wobei $i^2 = 1$ gilt.

2.2 Was sind Zahlen?

2.2.1 Einleitung

Informell:

- $\mathbb{N} = \{0, 1, ...\}$ oder $\mathbb{N} = \{1, 2, ...\}$
  Ob 0 in $\mathbb{N}$ enthalten ist, abhängig davon, wo Sie leben und was ihr Interessenschwerpunkt ist. Auf informeller Ebene ist es eher eine religiöse Frage.
- $\mathbb{Z} = \{..., -1, 0, 1, ...\}$
- $\mathbb{Q} = \{\frac{p}{q} |\ p, q \in \mathbb{Z} \text{ und } q \neq 0\}$
- $\mathbb{R} = \{d_0.d_1d_2...|\ d_0 \in \mathbb{Z} \text{ und } 0 \leq d_i \leq 9 \text{ für } i > 0\}$
- $\mathbb{C} = \{a + b \cdot i|\ a, b \in \mathbb{R} \text{ und } i^2 = -1\}$

2.2.2 Konstruktion von Zahlensystemen

Die Zahlen werden formal (der Hauptbewegung in der Mathematik folgend) aus den Axiomen der Mengenlehre nach Zermelo Fraenkel (a.k.a. ZF set theory) [Enderton77, Henle86, Hrbacek84] konstruiert. Die einzigen Dinge, die von den Axiomen abgeleitet werden können, sind Mengen mit der leeren Menge am unteren Ende der Hierarchie. Das bedeutet, dass jede Zahl eine

Menge ist (eine Menge ist das einzige, was von den Axiomen abgeleitet werden kann). Das bedeutet aber nicht, dass man immer die Mengennotation benutzen muss, wenn man mit Zahlen arbeitet: Man führt dazu einfach die Zahlen als Abkürzung der formalen Gegenstücke ein.

Die Konstruktion startet mit $\mathbb{N}$. Im algebraischen Sinn ist $\mathbb{N}$ mit seinen Operationen und seiner Ordnung eine schwache Struktur. In den folgenden Konstruktionen werden die Strukturen Schritt für Schritt wachsen. $\mathbb{Z}$ wird ein nullteilerfreier Ring sein, $\mathbb{Q}$ ein Körper, der Körper $\mathbb{R}$ wird vollständig und der Körper $\mathbb{C}$ wird algebraisch abgeschlossen sein.

Zunächst wollen wir aber einige Notationen einführen:

- Ein Paar ist $(a, b) = \{\{a\}, \{a, b\}\}$,
- eine Äquivalenzklasse ist $[a] = \{b|a \equiv b\}$,
- der Nachfolger von a ist $s(a) = a \cup \{a\}$.

Diese Notationen und die folgenden Konstruktionen sind de facto Standard. Es sind aber auch andere Definitionen möglich.

2.2.3 Konstruktion von $\mathbb{N}$

- $\{\} \in \mathbb{N}$.
- Ist $a \in \mathbb{N}$, dann ist auch $s(a) \in \mathbb{N}$.
- $\mathbb{N}$ ist kleinste mögliche Menge, so dass die vorstehenden Regeln gelten

Damit ist also $n = \{0, ..., n-1\}$ (also $0 = \{\},\ 1 = \{0\},\ 2 = \{0, 1\},\ 3 = \{0, 1, 2\}$). Wir wollen uns auf die Elemente von $\mathbb{N}$ beziehen, indem wir ihnen einen Index $_n$ geben. Die Relation $<_n$ definieren wir durch: $a_n <_n b_n :\Leftrightarrow a_n \in b_n$. Wir können zudem $+_n$ definieren als

- $a_n +_n 0_n = a_n$
- $a_n +_n +s(b_n) = s(a_n +_n b_n)$

Definiere weiter $*_n$ durch

- $a_n *_n 0_n = 0_n$
- $a_n *_n s(b_n) = (a_n *_n b_n) +_n a_n$

2.2.4 Konstruktion von $\mathbb{Z}$

Wir definieren eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$ durch

$$(a_n, b_n) \equiv_z (c_n, d_n) :\Leftrightarrow a_n +_n d_n = c_n +_n b_n.$$

$\equiv_z$ „simuliert" also eine Subtraktion in $\mathbb{N}$. Definiere $\mathbb{Z} := \{[(a_n, b_n)]_z | \ a_n, \ b_n \in \mathbb{N}\}$. Wir beziehen uns auf die Elemente von $\mathbb{Z}$ durch einen Index $_z$.

Die Elemente von $\mathbb{N}$ können nun folgendermaßen in $\mathbb{Z}$ eingebettet werden:

$$\begin{aligned} embed_z : \ \mathbb{N} &\rightarrow \mathbb{Z} \\ a_n &\mapsto [(a_n, 0_n)]_z \end{aligned}$$

Desweiteren definieren wir:

- $[(a_n, b_n)]_z <_z [(c_n, d_n)]_z$ genau dann, wenn $a_n +_n d_n <_n c_n +_n b_n$.
- $[(a_n, b_n)]_z +_z [(c_n, d_n)]_z := [(a_n +_n c_n, b_n +_n d_n)]_z$.
- $[(a_n, b_n)]_z *_z [(c_n, d_n)]_z := [((a_n *_n c_n) +_n (b_n *_n d_n), (a_n *_n d_n) +_n (c_n *_n b_n))]_z$.

2.2.5 Konstruktion von $\mathbb{Q}$

Wir definieren eine Äquivalenzrelation auf $\mathbb{Z} \times \mathbb{Z} \setminus \{0_Z\}$ durch $(a_z, b_z) \equiv_q (c_z, d_z)$ genau dann, wenn $a_z *_z d_z = c_z *_z b_z$ ist. $\equiv_q$ „simuliert" also eine Art Division in $\mathbb{Z}$. Definiere $\mathbb{Q} := \{[(a_z, b_z)]_q | \ a_z, \ b_z \in \mathbb{Z}, \ b_z \neq 0\}$. Wir beziehen uns auf die Elemente von $\mathbb{Q}$ durch einen Index $_q$. Die Elemente von $\mathbb{Z}$ können nun folgendermaßen in $\mathbb{Q}$ eingebettet werden:

$$\begin{aligned} embed_q : \ \mathbb{Z} &\rightarrow \mathbb{Q} \\ a_z &\mapsto [(a_z, 1_z)]_q \end{aligned}$$

Desweiteren definieren wir:

- $[(a_z, b_z)]_q <_q [(c_z, d_z)]_q$ genau dann, wenn $a_z *_z d_z <_z c_z *_z b_z$, wenn $0_z <_z b_z$ und $0_z <_z d_z$.
- $[(a_z, b_z]_q +_q [(c_z, d_z]_q = [((a_z *_z d_z +_z c_z *_z b_z), b_z *_z d_z)]_q$.
- $[(a_z, b_z)]_q *_q [(c_z, d_z)]_q = (a_z *_z c_z, b_z *_z d_z)_q$.

2.2.6 Konstruktion von $\mathbb{R}$

Die Konstruktion von $\mathbb{R}$ ist nun verschieden (und auch schwieriger zu verstehen), da wir sicherstellen müssen, dass die Kardinalität von $\mathbb{R}$ größer als die von $\mathbb{Q}$ ist.

Eine Menge c heißt Dedekindscher Schnitt genau dann, wenn

- $\{\} \subsetneq c \subsetneq \mathbb{Q}$.
- c ist nach unten abgeschlossen, d.h. ist $a_q \in c$ und $b_q <_q a_q$, dann ist auch $b_q \in c$.
- c besitzt kein größtest Element, d.h. es gibt kein Element $a_q \in c$, so dass $b_q <_q a_q$ für alle $a_q \neq b_q \in c$.

Solch einen Schnitt man sich vorstellen, indem man eine Schere nimmt und $\mathbb{Q}$ in zwei Hälften zerteilt, in einen Teil, der alle kleinen Zahlen, und einen, der alle großen Zahlen enthält. Ist die Zerteilung derart vorgenommen, dass die Menge der kleinen Zahlen kein größtes Element besitzt, so wird dies als Dedekind Schnitt bezeichnet.

Wir definieren damit nun $\mathbb{R} := \{c|\ \text{c ist ein Dedekindscher Schnitt}\ \}$. Elemente von $\mathbb{R}$ werden wir wiederum durch einen Index $_r$ kennzeichnen.

Eine Einbettung der Elemente von $\mathbb{Q}$ kann folgendermaßen geschehen:

$$\begin{array}{rcl} embed_q : \mathbb{Q} & \rightarrow & \mathbb{R} \\ embed_q(a_q) & \mapsto & \{b_q|\ b_q <_q a_q\} \end{array}$$

Desweiteren definieren wir:

- $a_r <_r b_r$ genau dann, wenn $a_r \subsetneq b_r$.
- $a_r +_r b_r = \{c_q +_q d_q|\ c_q \in a_r \text{ und } d_q \in b_r\}$.
- $-_r a_r = \{b_q|$ es gibt ein $c_q \in \mathbb{Q}$, so dass $b_q <_q c_q$ und $(-1)_q *_q c_q \notin a_r\}$.
- $|a_r|_r = a_r \cup (-_r a_r)$
- $*_r$ ist definiert durch:
  - Gilt weder $a_r <_r 0_r$ noch $b_r <_r 0_r$, so ist $a_r *_r b_r = 0_r \cup \{c_q *_q d_q|\ c_q \in a_r \text{ und } d_q \in b_r\}$.
  - Ist $a_r <_r 0_r$ und $b_r <_r 0_r$, dann ist $a_r *_r b_r = |a_r|_r *_r |b_r|_r$.
  - Sonst definieren wir $a_r *_r b_r = -_r(|a_r|_r *_r |b_r|_r)$.

Es gibt auch eine alternative Definiton von $\mathbb{R}$, die Cauchy-Folgen verwendet. Eine Cauchy-Folge ist eine Abbildung $s: \mathbb{N} \to \mathbb{Q}$, so dass $s(i_n) +_q ((-1)_q *_q s(j_n))$ nahe an 0_q liegt, wenn nur i_n und j_n gross genug sind. Wir definieren auf der Menge aller Cauchy-Folgen eine Äquivalenzrelation durch: $r \equiv_r s$ genau dann, wenn $r(m_n) +_q ((-1)_q *_q s(m_n))$ nahe an 0_q liegt, wenn nur m_n gross genug ist. Wir definieren dann $\mathbb{R} = \{[s]_r | \ s \text{ ist eine Cauchy-Folge}\}$. Es sei bemerkt, dass diese Definition ähnlich der dezimalen Expansion ist.

2.2.7 Konstruktion von $\mathbb{C}$

$\mathbb{C} := \mathbb{R} \times \mathbb{R}$. Die Elemente von $\mathbb{C}$ wollen wir mit einem Index $_c$ hervorheben. Die Elemente von $\mathbb{R}$ können folgendermaßen in $\mathbb{C}$ eingebettet werden.

$$\begin{aligned} embed_r : \ \mathbb{R} &\to \mathbb{C} \\ embed_r(a_r) &\mapsto (a_r, 0_r) \end{aligned}$$

Desweiteren definieren wir

- $(a_r, b_r) +_c (c_r, d_r) = (a_r +_r c_r, b_r +_r d_r)$
- $(a_r, b_r) *_c (c_r, d_r) = ((a_r *_r c_r) +_r -_r(b_r *_r d_r), (a_r *_r c_r) +_r (b_r *_r c_r))$

Es gibt eine alternative Definion über Ideale. Ein wenig schwammig: $\mathbb{C} = \mathbb{R}[x]/ < x *_r x +_r 1_r >$, d.h. $\mathbb{C}$ ist der Quotientenring des Ideals $< x *_r x +_r 1_r >$ aus dem Ring $\mathbb{R}[x]$ der Polynome über $\mathbb{R}$.

Der schwammige Teil dabei ist, dass wir eigentlich zunächst Konzepte wie einen Quotientenring, Ideale und Polynomringe definieren müssten. Man bemerkt, dass diese Definition nahe an $i^2 = -1$ ist, denn $x *_r x + 1_r = 0_r$ kann zu $(x *_r x) = (-1_r)$ umgeschrieben werden.

2.2.8 Abrundung

An dieser Stelle ist $\mathbb{N}$ keine Teilmenge von $\mathbb{Z}$, $\mathbb{Z}$ keine von $\mathbb{Q}$ etc. Allerdings können wir diese Inklusionen erreichen, wenn wir die eingebetteten Kopien von $\mathbb{N}$, $\mathbb{Z}$, etc. betrachten. Sei dazu

- $\mathbb{N}' = \text{Bild}(embed_r \circ embed_q \circ embed_z \circ embed_n)$
- $\mathbb{Z}' = \text{Bild}(embed_r \circ embed_q \circ embed_z)$
- $\mathbb{Q}' = \text{Bild}(embed_r \circ embed_q)$
- $\mathbb{R}' = \text{Bild}(embed_r)$

Für diese Mengen haben wir nun $\mathbb{N}' \subset \mathbb{Z} \subset \mathbb{Q}' \subset \mathbb{R}' \subset \mathbb{C}$. Desweiteren haben diese Mengen all die Eigenschaften, die die uns bekannten Zahlen besitzen.

2.2.9 Ausblick

Für einige eher fremde Teile der Mathematik kann man nun die Zahlsysteme zu anderen exotischen Zahlen erweiteren. Wir wollen einige anführen:

- Kardinal- und Ordinalzahlen

  Kardinal- und Ordinalzahlen sind in der ZF Mengentheorie enthalten [Enderton77, Henle86, Hrbacek84], sind somit also Mengen. Kardinalzahlen sind Zahlen, welche die Größe von Mengen repräsentieren; Ordinalzahl hingegen sind Zahlen, die wohlgeordnete Mengen repräsentieren.

  Endliche Kardinalzahlen und Ordinalzahlen sind das gleiche wie die natürlichen Zahlen. Interessant - und teilweise ein wenig trickreich - werden sie und ihre Arithmetik allerdings im Zusammenhang mit unendlichen Mengen.

- Hyperreelle Zahlen

  Diese Zahlen werden durch Ultrafilter [Henle86] definiert und in der Non-Standard-Analysis benutzt. Mit Hyperreellen Zahlen kann man Zahlen so behandeln, wie Leibniz und Newton es getan haben - unter Verwendung infinitesimaler Größen.

- Quaternionen und Oktonionen

  Normalerweise werden diese mit algebraischen Mitteln konstruiert (ähnlich der alternativen Definition von $\mathbb{C}$ durch Ideale) [Shapiro75, Dixon94]. Quaternionen werde verwendet, um Rotationen in drei Dimensionen zu modellieren. Oktonionen, besser bekannt als Cayley-Zahlen, sind lediglich esoterische Artifakte :-) Na ja, wenn Sie eine Verwendung kennen, dürfen Sie diese gerne dem FAQ beisteuern.

- Verschiedene

  Nur um noch einige weitere zu nennen: algebraische Zahlen [Shapiro75], p-adische Zahlen [Shapiro75], und surreale Zahlen (a.k.a. Conway-Zahlen) [Conway76].

Kardinal- und Ordinalzahlen werden in der Mathematik häufig benutzt. Viele Normalsterbliche werden niemals mit hyperreellen Zahlen, Quaternionen oder Oktonionen zu tun haben (geschweige denn diese benutzen).

Referenzen

J.H. Conway. *On Numbers and Games*, L.M.S. Monographs, vol. 6. Academic Press, 1976.
H.B. Enderton. *Elements of Set Theory*. Academic Press, 1977.
G.M. Dixon. *Division Algebras; Octonions, Quaternions, Complex Numbers and the Algebraic Design of Physics*. Kluwer Academic, 1994.
J.M. Henle. *An Outline of Set Theory*. Springer Verlag, 1986.
K. Hrbacek and T. Jech. *Introduction to Set Theory*. M. Dekker Inc., 1984.
L. Shapiro. *Introduction to Abstract Algebra*. McGraw-Hill, 1975.

Send comments and or corrections relating to this part to `J.P.M.deVreught@cs.tudelft.nl`

Kapitel 3

Zahlentheorie

3.1 Fermat's letzter Satz

3.1.1 Die Geschichte von Fermat's letztem Satz

Pierre de Fermat (1601-1665) war ein Anwalt und Amateurmathematiker. Im Jahre 1637 schrieb er folgende Bemerkung auf den Rand seiner Kopie von Bachet's Übersetzung der Arithmetica von Diophant:

> Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Sinngemäß ins Deutsche übersetzt bedeutet dies

> Es gibt keine positiven ganzen Zahlen, so dass $x^n + y^n = z^n$, wenn $n > 2$ ist. Ich habe einen wirklich bemerkenswerten Beweis gefunden, aber der Rand [dieses Buches] bietet nicht genug Rand, um ihn aufzuschreiben.

Fermat hat niemals einen Beweis dieser Vermutung veröffentlicht. Somit wurde es zu der bekannten Fermatschen Vermutung (im Folgenden FV abgekürzt), nicht weil es ein Teil seiner letzten Arbeit war, sondern vielmehr weil es die letzte Vermutung in der Liste von Fermat's Arbeit ist, die noch zu beweisen war. Alle anderen wurden schon lange zuvor bewiesen oder widerlegt.

3.1.2 Was ist der aktuelle Stand der FV?

Theorem 1
(Fermat's letzter Satz) Es gibt keine positiven ganzen Zahlen x, y, z und $n > 2$ mit

$$x^n + y^n = z^n$$

Andrew Wiles, Forscher in Princeton, scheint einen Beweis gefunden zu haben. Er präsentierte den Beweis in Cambridge, UK während eines dreitägigen Seminars den führenden Experten auf diesem Gebiet. Der Beweis schien korrekt zu sein. Im Sommer 1994 gestand Prof. Wiles die Existenz einer Lücke ein. Am 25. Oktober 1994 veröffentlichte Prof. Andrew Wiles zwei Preprints, *Modular elliptic curves and Fermats Last Theorem*, von Andrew Wiles und *Ring theoretic properties of certain Hecke algebras*, von Richard Taylor und Andrew Wiles.

Der erste (lange) Artikel präsentiert, neben anderen Dingen, einen Beweis der FV. Ein entscheidender Beweisschritt basiert auf dem zweiten Artikel. Der Beweis, der von Wiles in Canbridge präsentiert wurde, hatte eine große Lücke, nämlich in der Konstruktion eines Euler-Systems. Nach vielen erfolglosen Versuchen diese Lücke zu schließen, entschloss sich Wiles zu einem andere Ansatz zurückzukehren, den er zu Gunsten der Idee mit dem Euler-System verworfen hatte. Er war nun in der Lage einen Beweis unter der Vorraussetzung zu erbringen, dass bestimmte Hecke-Algebren lokal vollständige Unterteilungen sind. Dies und die anderen Ideen, die Wiles in Cambrige beschrieb, sind im ersten Artikel enthalten. Glücklicherweise waren Taylor und Wiles in der Lage, in dem oben angesprochenen zweiten Artikel alle notwendigen Eigenschaften der Hecke-Algebren zu zeigen.

Der neue Zugang scheint nun auch signifikant einfacher und kürzer als der ursprüngliche zu sein, aufgrund des Entfernens des Euler-Systems. (In der Tat scheint Faltings, kurz nachdem er diese neuen Artikel gesehen hat, eine weitere signifikante Vereinfachung in diesem Teil des Beweises gefunden zu haben.)

Die Artikel wurden 1995 in der Mai-Ausgabe der *Annals of Mathematics* veröffentlicht. Für einzelne Kopien senden Sie eine E-Mail an `jlorder@jhunix.hcf.jhu.edu` für weitere Informationen.

Zusammenfassung:

Beide Artikel wurden veröffentlicht. Tausende Menschen haben sie inzwischen gelesen. Ungefähr einhundert verstehen sie sehr gut. Faltings hat das Argument vereinfacht; Diamond hat es verallgemeinert. Jeder kann die Artikel lesen. Die unglaublich komplizierte Geometrie im Beweis wurde durch einfachere Algebra ersetzt. Der Beweis ist mittlerweile allgemein als korrekt akzeptiert. Zwar war auch im zweiten Beweis eine Lücke, die aber schon im

Oktober 1994 geschlossen wurde.

3.1.3 Verwandte Vermutungen

Eine verwandte Vermutung stammt von Euler

$$x^n + y^n + z^n = c^n \quad \text{hat keine Lösung für } n \geq 4$$

Noam Elkies fand ein Gegenbeispiel mit $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$. Darüber hinaus fand Roger Frye die absolut kleinste Lösung, mehr oder weniger durch Ausprobieren: $95800^4 + 217519^4 + 414560^4 = 422481^4$. *Several years*, Math. Comp. 51 (1988) 825-835. Diese Zusammenfassung ist sicherlich sehr kurz, ein kompletter Überblick würde allerdings zu viele Seiten einnehmen.

Referenzen

[1] *J.P.Butler, R.E.Crandall,& R.W.Sompolski*, **Irregular Primes to One Million**. Math. Comp., 59 (October 1992) pp. 717-722.
Fermats Last Theorem, A Genetic Introduction to Algebraic Number Theory. *H.M. Edwards*. Springer Verlag, New York, 1977.
Thirteen Lectures on Fermats Last Theorem. *P. Ribenboim*. Springer Verlag, New York, 1979.
Number Theory Related to Fermats Last Theorem. *Neal Koblitz*, editor. Birkhäuser Boston, Inc., 1982, ISBN 3-7643-3104-6

3.1.4 Hatte Fermat selber einen Beweis?

Nein, hatte er wohl nicht. Fermat behauptete in einem frühen Stadium seiner Karriere, er hätte einen Beweis der Vermutung. Einige Zeit später verwendete er viel Zeit und Aufwand, die Fälle $n = 4$ und $n = 5$ nachzuweisen. Hätte er einen Beweis der Vermutung früher schon gehabt, hätte es keinen Grund gegeben diese Spezialfälle zu untersuchen.

Femat könnte z.B. einen der folgenden „Beweise“ besessen haben, als er seinen berühmten Kommentar schrieb.

- Fermat erforschte und verwendete die Methode des unendlichen Abstiegs, die tatsächlich benutzt werden kann, um die FV für $n = 4$ zu beweisen. Sie kann sogar für eine schärfere Version der FV in $n = 4$ benutzt werden: $x^4 + y^4 = z^2$ hat keine nicht-triviale ganzzahlige Lösung. Es könnte möglich sein, dass er einen falschen Beweis der FV mit dieser Methode hatte, als er sein famoses Theorem niederschrieb.

- Er hatte einen falschen Beweis im Kopf. Der folgende Beweis wurde von Lamé als korrekt befunden. Erst Liouville und Kummer, der später ein Experte auf diesem Feld wurde, fanden einen Fehler. Der Beweis basierte auf der Annahme, dass die Primzahlzerlegung stets eindeutig sei.

  Dabei geht der Beweis ungefähr folgendermaßen:

  Es genügt Primzahl-Exponenten zu betrachten (dies ist in der Tat richtig). Betrachten wir also $x^p + y^p = z^p$. Sei r eine primitive p-te Einheitswurzel (eine komplexe Zahl). Dann ist diese Gleichung äquivalent zu:

  $$(x+y)(x+ry)(x+r^2y)...(x+r^{p-1}y) = z^p$$

  Nun betrachte einen Ring der Form:

  $$a_1 + a_2r + a_3r^2 + ... + a_pr^{p-1}$$

  mit ganzzahligen a_i.

  Ist dieser Ring nun ein Ring mit eindeutiger Primfaktorzerlegung (im folgenden UFR, für unique factorization ring), dann ist jeder der obigen Faktoren irreduzibel.

  Von hier aus kann bewiesen werden, dass jeder Faktor eine p-te Potenz ist, woraus die FV folgt. Dies kann geschehen, indem wir zwei Fälle unterscheiden. Der erste Fall ist, dass p keine Zahl von x, y, z teilt; der zweite, wenn p eine der Zahlen x, y, z teilt. Zum ersten Fall: Ist $x + yr = u * t^p$, wobei $u, t \in \mathbb{Z}[r]$ und u eine Einheit ist, dann folgt, dass $x = y(\mod p)$ ist. Schreiben wir nun die Ausgangsgleichung als $x^p + (-y)^p = (-z)^p$, dann folgt analog, dass auch $x = -z(\mod p)$ ist. Daher ist $2 * x^p = x^p + y^p = z^p = -x^p(\mod p)$ und damit $3 * x^p = 0(\mod p)$, also teilt p x oder $3|x^p$. Da aber $p > 3$ und p nicht x teilt, folgt der Widerspruch. Der zweite Fall ist schwerer.

  Das Problem ist, dass der obige Ring im Allgemeinen kein UFR ist.

Ein anderes Argument dafür, dass Fermat wohl keinen Beweis hatte - und sogar dafür, dass er auch **wusste**, dass er keinen besitzt - ist, dass die Anmerkung auf dem Rand von Bachet's Diophant das einzige Auftreten dieser Behauptung ist. Hätte er wirklich geglaubt einen Beweis zu besitzen, hätte er dies auch veröffentlicht oder englische Mathematiker herausgefordert ebenfalls einen zu finden. Es ist anzunehmen, dass er eine Lücke in seinem eigenen Beweis gefunden hatte, bevor er dazu kam seine Vermutung zu veröffentlichen, und dass er die Anmerkung niemals weggewischt hatte, da er annahm, dass sie niemals jemand sehen würde.

Einige andere bekannte Mathematiker haben über diese Frage spekuliert. So schreibt Andre Weil

> Only on one ill-fated occasion did Fermat ever mention a curve of higher genus $x^n + y^n = z^n$, and then hardly remains any doubt that this was due to some misapprehension on his part [...] for a brief moment perhaps [...] he must have deluded himself into thinking he had the principle of a general proof.

Winfried Scharlau und Hans Opolka äußern sich dazu:

> Whether Fermat knew a proof or not has been the subject of many speculations. The truth seems obvious ... [Fermats marginal note] was made at the time of his first letters concerning number theory [1637] ... as far as we know he never repeated his general remark, but repeatedly made the statement for the cases n = 3 and 4 and posed these cases as problems to his correspondents [...] he formulated the case n = 3 in a letter to Carcavi in 1659 [...] All these facts indicate that Fermat quickly became aware of the incompleteness of the [general] proof of 1637. Of course, there was no reason for a public retraction of his privately made conjecture.

Es ist jedoch wichtig sich zu vergegenwärtigen, dass Fermat's „Beweis“ der „Publish or Perish“[1]-Periode in der wissenschaftlichen Forschung vorangeht, in der wir heute immer noch leben.

Referenzen

From Fermat to Minkowski: lectures on the theory of numbers and its historical development. *Winfried Scharlau, Hans Opolka.* New York, Springer, 1985.
Basic Number Theory. *Andre Weil.* Berlin, Springer, 1967

3.2 Primzahlen

3.2.1 Welches ist die größte bekannte Mersennesche Primzahl?

Mersennesche Primzahlen sind Primzahlen der Form $2^p - 1$. Damit $2^p - 1$ prim sein kann, muss auch p eine Primzahl sein.

$2^{2976221} - 1$ ist die derzeit größte bekannte Primzahl. Sie wurde 1997 gefunden.

[1] etwa „Publiziere oder gehe zugrunde“

3.2.2 Welches ist die größte bekannte Primzahl?

Die größte bekannte Mersennesche Primzahl wurde zuvor beschrieben; die größte bekannte nicht-Mersennesche Primzahl ist $391581 * 2^{216193} - 1$. Sie wurde von Brown, Noll, Parady, Smith, Smith und Zarantonello gefunden.

Bisher waren die größten bekannten Primzahlen fast immer Mersennesche Primzahlen; die Periode zwischen der Entdeckung von Brown et al. im August 1989 und Slowinski's & Gage's Fund im März 1992 ist eine von wenigen Ausnahmen.

Auch Sie können helfen weitere Primzahlen zu finden. Näheres unter: The Great Internet Mersenne Prime Search home page (`http://www.mersenne.org`)

Referenzen

Brown, Noll, Parady, Smith, Smith, und Zarantonello. **Letter to the editor**. American Math-ematical Monthly, vol. 97, 1990, p. 214.

3.2.3 Was ist der größte bekannte Primzahlzwilling?

Der größte bekannte Primzahlzwilling ist $242206083 * 2^{38880} \pm 1$ mit 11713 Ziffern, gefunden von Indlekofer und Jarai im November 1995. Zugleich ist dies auch der erste bekannte gigantische Primzahlzwilling (das sind Primzahlen mit mehr als 10.000 Stellen).

Bisherige Rekordhalter waren:

- $190.116 * 3.003 * 10^{5120} \pm 1$ mit 5.120 Stellen, gefunden von Harvey Dubner.
- $697.053.813 * 2^{16352} \pm 1$ mit 4.932 Stellen, gefunden von Indlekofer und Ja'rai im Jahre 1994.
- $1.691.232 * 1001 * 10^{4020} \pm 1$ mit 4030 Stellen, gefunden von Harvey Dubner.

Die zwei größten bekannten Sophie Germain-Primzahlen (das sind Primzahlen, für die sowohl p als auch $2p+1$ prim sind), sind $p = 2.687.145 * 3.003 * 10^{5072} - 1$ und $q = 2p+1$, gefunden von Harvey Dubner am 3. Oktober 1995.

Referenzen

B. K. Parady und J. F. Smith und S. E. Zarantonello, Smith, Noll und Brown. **Largest known twin primes**. Mathematics of Computation, vol.55, 1990, pp. 381-382.

3.2.4 Welches ist die größte bekannte Fermatsche Primzahl mit bekannter Faktorisierung?

$F_{11} = (2^{(2^{11})}) + 1$, die von Brent & Morain im Jahr 1988 faktorisiert wurde. $F_9 = (2^{(2^9)}) + 1 = 2^{512} + 1$ wurde von A.K. Lenstra, H.W. Lenstra Jr., M.S. Manasse & J.M. Pollard 1990 faktorisiert. F_{10} wurde von Richard Brent faktorisiert, der einen 40-stelligen Faktor von $2^{1024} + 1$ am 20. Oktober 1995 fand. Der Kofaktor ist eine 252-stellige Zahl, eine im allgemeinen nicht einfach zu faktorisierende Zahl. Glücklicherweise war diese Zahl ebenfalls eine Primzahl.

3.2.5 Algorithmen zur Faktorisierung von ganzen Zahlen

Es gibt einige bekannte Algorithmen, die eine nicht-exponentielle Laufzeit besitzen, dies sind z.B.:

- Der Continued fraction-Algorithmus,
- der Quadratic sieve-Algorithmus,
- der Class Group-Algorithmus,
- der Elliptic curve-Algorithmus,
- der Number field sieve-Algorithmus,
- Dixon's Random squares-Algorithmus,
- Valle's Two-thirds-Algorithmus und
- Seysen's Class group-Algorithmus.

Referenzen

A.K. Lenstra, H.W. Lenstra Jr. Algorithms in Number Theory. J. van Leeuwen (ed.), Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity Elsevier, pp. 673-715, 1990.

3.2.6 Primzahltests

Primzahltests und Faktorisierungen sind zwei verschiedene Probleme. Konzentrieren wir uns nur auf einen Primzahltest, so müssen wir zu keinem Zeitpunkt den tatsächlichen Faktor kennen. Die einzige Frage, die beantwortet werde muss ist „Ist die vorliegende Zahl prim oder zusammengesetzt?“.

Wilsons Theorem: Eine ganze Zahl p ist prim genau dann, wenn $(p-1)!$ kongruent zu $-1(\mod p)$ ist.

Allerdings gibt es keine bekannte Methode $(N-1)!(\mod N)$ mit logarithmischen Aufwand auszuwerten. Daher ist Wilson's Charakterisierung von Primzahlen in der Praxis für einen Primzahltest von N nicht geeignet.

Es gibt viele verschiedene Testverfahren, man kann sie auf drei Arten charakterisieren:

1. Tests für Zahlen einer speziellen Form
   gegenüber
   Tests für beliebige Zahlen

2. Tests mit gesicherter Grundlage
   gegenüber
   Auf Vermutungen basierende Test

3. Deterministische Tests
   gegenüber
   Wahrscheinlichkeits- oder Monte Carlo-Tests

Millers Test

1976 entwickelte G. L. Miller einen Primzahltest, der eine verallgemeinerte Form der Riemannschen Vermutung benutzt.

Der APR-Test

Der von L. M. Adleman, C. Pomerance and R. S. Rumely im Jahre 1983 entwickelte Test, der auch als APR-Test bekannt ist, stellt einen Durchbruch dar:

1. Der Test ist auf beliebige natürliche Zahlen N anwendbar, ohne eine Faktorisierung von $N-1$ oder $N+1$ zu kennen.

2. Die Laufzeit $t(N)$ ist nahezu polynomial.

3. Der Test ist rigoros, und zum ersten Mal auf diesem Feld flossen tiefe Resultate aus der Theorie der algebraischen Zahlen ein; der Test beinhaltet Berechnungen mit Einheitswurzeln und das allgemeine Reziprozitätsgesetz für das power residue symbol.

Die Laufzeit stellt derzeit einen Weltrekord für deterministische Primzahltests dar.

Kurze Zeit später (1984) modifizierten H. Cohen & A. K. Lenstra den APR-Test, machten ihn flexibler, verwendeten gaußsche Summen anstatt des Reziprozitätsgesetzes im Beweis, und für praktische Anwendungen programmierten sie den neuen Test. Es war der erste Test, der mühelos mit 100-stelligen Zahlen zurechtkommt; dafür benötigt er etwa 45 Sekunden.

Monte Carlo-Methoden

Ribenboim nennt drei Monte Carlo-Tests, nach R. Baillie & Wagstaff, Jr. (1980), R. Solovay & V. Strassen (1977), und M. O. Rabin (1976, 1980).

Elliptic Curves Primality Proving, ECPP

ECPP steht für „Elliptic Curves and Primality Proving“. Der Algorithmus wird beschrieben in:

A. O. L. Atkin and F. Morain
„Elliptic curves and primality proving“
To appear.

Dies ist ein deterministischer Algorithmus, der Zahlen bis zu einer Größenordnung von 10^{1000} testen kann.

Referenzen

[1] A. O. L. Atkin and F. Morain
„Elliptic curves and primality proving“
To appear in Math. Comp.
Lieven Marchand ¡mal@bewoner.dma.be¿
[2] F. Morain
„Courbes elliptiques et tests de primalite“
These, Universite de Lyon I, 1990.
Erhältlich unter:
`http://lix.polytechnique.fr/~morain/english-index.html`

3.2.7 Rekordlisten

Chris Caldwell (caldwell@utm.edu) pflegt eine Liste ‘The Largest Known Primes’ (‘Die größten bekannten Primzahlen’). Erhältlich unter:

```
web: http://www.utm.edu/research/primes/largest.html
gopher: unix1.utm.edu, directory1/user/Public_FTP/pub/math/primes
ftp: math.utm.edu, directory /pub/math/primes
```

`finger primes@math.utm.edu` für einige Rekordprimzahlen und die gegenwärtigen Möglichkeiten eine Liste zu erhalten. Chris ist sehr an neuen sogenannten Titanen-Primzahlen interessiert (das sind Primzahlen mit mehr als 1000 Stellen), damit er diese seiner Liste hinzufügen kann.

3.2.8 Welche Mersenne-Primzahlen gibt es?

Die folgenden Mersenne-Primzahlen sind bekannt:

Nummer	p	Jahr	Finder
1-4	2,3,5,7	vor 1500	
5	13	1461	Anonymous
6-7	17,19	1588	Cataldi
8	31	1750	Euler
9	61	1883	I.M. Pervushin
10	89	1911	Powers
11	107	1914	Powers
12	127	1876	Lucas
13-14	521,607	1952	Robinson
15-17	1279,2203,2281	1952	R. M. Robinson
18	3217	1957	Riesel
19-20	4253,4423	1961	Hurwitz & Selfridge
21-23	9689,9941,11213	1963	Gillies
24	19937	1971	Tuckerman
25	21701	1978	Noll & Nickel
26	23209	1979	Noll
27	44497	1979	Slowinski & Nelson
28	86243	1982	Slowinski
29	110503	1988	Colquitt & Welsh
30	132049	1983	Slowinski
31	216091	1985	Slowinski
32	756839	1992	Slowinski & Gage
33	859433	1994	Slowinski & Gage
34	1257787	1996	Slowinski & Gage
35	1398269	1996	Armengaud, Woltman, und andere
36???	2976221	1996	Spence, Woltman, und andere

Ein Weg zu testen, ob $2^p - 1$ prim ist, ist der Lucas-Lehmer-Test:

```
Lucas_Lehmer_Test(p):
  u := 4
```

```
for i from 3 to p do
  u := u^2-2 mod 2^p-1
od
if u == 0 then
  2^p-1 is prime
else
  2^p-1 is composite
fi
```

Alle Exponenten kleiner als 1.481.800 sind inzwischen mindestens einmal getestet worden.

Referenzen

An introduction to the theory of numbers. *G.H. Hardy, E.M. Wright*. Fifth edition, 1979, Oxford.

3.2.9 Formeln zur Berechnung von Primzahlen

Es gibt kein Polynom, das alle Primzahlen liefert. Dies zu zeigen ist eine einfache Übung. Es gibt kein nicht-konstantes Polynom, das lediglich Primzahlen liefert. Der Beweis ist so einfach, dass er wahrscheinlich von einem Schüler gefunden werden könnte (vgl. z.B. Ribenboims Buch *The Book of Prime Number Records*).

Es sei dennoch angemerkt, dass durch die Arbeit von Jones, Sato, Wada und Wiens ein Polynom in 26 Variablen gefunden werden konnte, so dass die Menge der Primzahlen mit der Menge der positiven Werte dieses Polynoms zusammenfällt. Vgl. Ribenboim, S. 147-150.

Aber die meisten Menschen verstehen unter „Formel“ nicht nur ein Polynom. Können wir nicht Summen, die Fakultät und die floor-Funktion in unserer Formel verwenden? Unter diesen Voraussetzungen gibt es tatsächlich Formeln für Primzahlen. Einige von ihnen sind weiter unten aufgefhrt.

Eine vernünftige Interpretation des Wortes „Formel“ ist einfach „Eine Turingmaschine, die zu jeder Eingabe ein Ergebnis liefert“. Mit dieser Interpretation können sicherlich anhaltende Turingmaschinen angegeben werden, welche die n. Primzahl zurückgeben. Allerdings ist derzeit noch keine Möglichkeit bekannt, solch eine „Formel“ zu programmieren, die die n. Primzahl in einer Zeit liefert, die polynomial in $\log n$ ist. Ob dies möglich ist, ist eine immer noch offene Frage.

Herb Wilf hat die Frage ‘What is a formula?’ in seinem Artikel ‘What is an answer?’ adressiert, der im American Mathematical Monthly, 89 (1982), 289-292 erschien. Darin unterschied er zwischen einer „Formel“ und einer „guten Formel“. Jeder der behauptet, es könne keine Formel für Primzahlen geben, sollte diesen Artikel lesen.

Folgende Referenzen sind Artikel, die „Formeln“ für Primzahlen besprechen. Fast alle benötigen keine Berechnung von vorhergehenden Primzahlen und die meisten basieren auf den Standardfunktionen.

Referenzen

C. Isenkrahe. Math. Annalen 53 (1900), 42-44.
W. H. Mills. Bulletin of the American Mathematical Society 53 (1947), 604.
L. Moser. Mathematics Magazine 23 (1950), 163-164.
E. M. Wright. American Mathematical Monthly 58 (1951), 616-618. (Correction, 59 (1952), 99.)
E. M. Wright. Journal of the London Mathematical Society 29 (1954), 63-71.
B. R. Srinivasan. Journal of the Indian Mathematical Society 25 (1961), 33-39.
C. P. Willans. Mathematics Gazette 48 (1964), 413-415.
V. C. Harris. Nordisk Mat. Tidskr. 17 (1969), 82.
U. Dudley. American Mathematical Monthly 76 (1969), 23-28.
C. Vanden Eynden. American Mathematical Monthly 79 (1972), 625.
S. W. Golomb. American Mathematical Monthly 81 (1974), 752-754.
Algorithmic Number Theory. *J.O. Shallit, E. Bach*. (to be published, MIT Press).
A Course in Computational Algebraic Number Theory. *Henri Cohen*. Springer-Verlag, Graduate Texts in Math, 1993.

Kapitel 4

Spezielle Funktionen und Zahlen

4.1 Wie kann man π berechnen?

Symbolische Mathematiksoftware wie *Maple* oder *Mathematica* kann 10.000 Stellen von π innerhalb eines Cursorblinkens berechnen und ca. 20.000-1.000.000 weitere Stellen innerhalb einer Nacht (die Stellenzahl hängt von der verwendeten Hardware ab).

Es ist möglich, mehr als 1.25 Million Stellen von π via anonymous ftp von der Seite wuarchive.wustl.edu in den Dateien pi.doc.Z und pi.dat.Z zu erhalten, welche im Unterverzeichnis doc/misc/pi zu finden sind. New Yorks Chudnovsky-Brüder haben 2 Milliarden Stellen von π auf einem Heimcomputer berechnet ....

Der derzeitige Rekord wird von Yasumasa Kanada und Daisuke Takahashi von der University of Tokyo mit 51 Milliarden Stellen (51.539.600.000 Dezimalstellen, um genau zu sein) gehalten.

Nick Johnson-Hill bietet eine interessante Seite zu π unter: `http://www.users.globalnet.co.uk/~nickjh/Pi.htm`.

Der neue Rekord von berechneten und verifizierten Dezimalstellen von π wurde am 28. August 1995 mit immerhin 4,29496 Milliarden Dezimalstellen aufgestellt.

Verwandte Dokumente sind via anonymous ftp unter www.cc.u-tokyo.ac.jp erhältlich.

`ftp://www.cc.u-tokyo.ac.jp/`

Diese Berechnung wurde von Yasumasa Kanada an der University of Tokyo angefertigt.

Insgesamt gibt es drei verschiedene Methoden π derart genau zu berechnen:

1. Eine der ältesten Methode benutzt die Potenzreihenentwicklung des $\arctan(x) = x - x^3/3 + x^5/5 - \ldots$ mit Formeln wie $\pi = 16 * \arctan(1/5) - 4 * \arctan(1/239)$. Dies ergibt ca. 1,9 Dezimalstellen pro Term.

2. Eine zweite Möglichkeit ist es, Formeln basierend auf arithmetischen und geometrischen Mitteln zu benutzen. Eine wunderschöne Zusammenfassung solcher Formeln finden sich in dem Buch π und dem AGN (s. dazu die Referenzen). Diese Formeln besitzen im allgemeinen eine quadratische Konvergenz, z.B. verdoppelt sich pro Iteration die Anzahl der Dezimalstellen. Dies bedeutet, dass ca. 20 Iteration für 1.000.000 Dezimalstellen nötig sind. Nachteilig jedoch ist, dass FFT-artige (Schnelle Fourier-Transformation) Multiplikationen für eine annehmbare Geschwindigkeit benötigt werden, diese aber nicht einfach zu programmieren sind.

3. Eine dritte Methode stammt aus der Theorie der komplexen Multiplikation von elliptischen Kurven. Diese von S. Ramanujan entdeckte Möglichkeit ergibt eine Vielzahl von Formeln, aber die nützlichste hierbei wurde nicht von Ramanujan, sondern von den Chudnovskys entwickelt. Dies ist die folgende:

   Sei $k_1 = 545140134$; $k_2 = 13591409$; $k_3 = 640320$; $k_4 = 100100025$; $k_5 = 327843840$; $k_6 = 53360$.

   Dann ist $\pi = \dfrac{k_6\sqrt{k_3}}{S}$, wobei

   $$S = \sum_{n=0}^{\infty} (-1)^n \frac{(6n!)(k_2 + nk_1)}{n!^3 (3n)! (8k_4k_5)^n}$$

   Die großen Vorteile diese Formel sind

   (a) Sie konvergiert (nur linear, aber) mit mehr als 14 Stellen pro Iteration.

   (b) Die Zusammensetzung der Formel und alle Operationen um S zu berechnen können einfach implementiert werden. Dies ist auch der Grund, warum im Nenner statt 262.537.412.640.768.000 der Term $8k_4k_5$ benutzt wird. Auf diesem Weg konnten die Chudnovskys viele Milliarden Stellen berechnen.

Eine interessante neue Methode wurde vor kurzem von David Bailey, Peter Borwein und Simon Plouffe vorgeschlagen. Diese kann auf effiziente Weise die n. *hexadezimale* Ziffer von π ohne Berechnung der $n-1$-ten bestimmen. Diese Methode basiert auf der Formel

$$\pi = \sum_{i=0}^{\infty} \left(\frac{4}{8i+1} - \frac{2}{8i+1} - \frac{1}{8i+5} - \frac{1}{8i+6} \right),$$

die mit einem Zeitaufwand von $O(n)$ und $O(\log(n))$ Speicherplatz arbeitet. (vgl. Referenzen)

Das folgende 160 Buchstaben lange C-Programm, welches von Dik T. Winter am CWI entwickelt wurde, berechnet π auf 800 Stellen genau.

```
int a=10000,b,c=2800,d,e,f[2801],g;main(){for(;b-c;)f[b++]=a/5;
for(;d=0,g=c*2;c-=14,printf("%.4d",e+d/a),e=d%a)for(b=c;d+=f[b]*a,
f[b]=d%--g,d/=g--,--b;d*=b);}
```

Referenzen

P. B. Borwein, and D. H. Bailey. **Ramanujan, Modular Equations, and Approximations to π** American Mathematical Monthly, vol. 96, no. 3 (March 1989), p. 201-220.

D. H. Bailey, P. B. Borwein, and S. Plouffe. **A New Formula for Picking off Pieces of Pi**, Science News, v 148, p 279 (Oct 28, 1995). also at `http://www.cecm.sfu.ca/ pbor`

J.M. Borwein and P.B. Borwein. **The arithmetic-geometric mean and fast computation of elementary functions**. SIAM Review, Vol. 26, 1984, pp. 351-366.

J.M. Borwein and P.B. Borwein. **More quadratically converging algorithms for π**. Math- ematics of Computation, Vol. 46, 1986, pp. 247-253.

Shlomo Breuer and Gideon Zwas **Mathematical-educational aspects of the computation of π** Int. J. Math. Educ. Sci. Technol., Vol. 15, No. 2, 1984, pp. 231-244.

David Chudnovsky and Gregory Chudnovsky. **The computation of classical constants.** Columbia University, Proc. Natl. Acad. Sci. USA, Vol. 86, 1989.

Classical Constants and Functions: Computations and Continued Fraction Expansions *D.V.Chudnovsky, G.V.Chudnovsky, H.Cohn, M.B.Nathanson,* eds. Number Theory, New York Seminar 1989-1990.

Y. Kanada and Y. Tamura. **Calculation of π to 10.013.395 decimal places based on the Gauss-Legendre algorithm and Gauss arctangent relation**. Computer Centre, University of Tokyo, 1983.

Morris Newman and Daniel Shanks. **On a sequence arising in series for π.** Mathematics of computation, Vol. 42, No. 165, Jan 1984, pp. 199-217.
E. Salamin. **Computation of π using arithmetic-geometric mean**. Mathematics of Com-putation, Vol. 30, 1976, pp. 565-570
David Singmaster. **The legal values of π.** The Mathematical Intelligencer, Vol. 7, No. 2, 1985. Stan Wagon. Is normal? The Mathematical Intelligencer, Vol. 7, No. 3, 1985.
A history of π. *P. Beckman.* Golem Press, CO, 1971 (fourth edition 1977)
π and the AGM - a study in analytic number theory and computational complexity. *J.M. Borwein and P.B. Borwein.* Wiley, New York, 1987.

4.1.1 Die Eulersche Formel

Die Definition und der Definitionsbereich der Potenzfunktion wurden schon mehrere Male verändert. Die Operation x^y wurde ursprünglich für positive y definiert. Der Definitionsbereich dieser Operation wurde zwar ausgedehnt, aber nicht so weit wie es möglich gewesen wäre; dies begründet sich darin, dass ansonsten Eigenschaften der ursprünglichen Operation verlorengegangen wären. In diesem Teil sind die Definitionen lediglich Vereinbarungen, die aus ästhetischen Gründen und aus Gründen der Nützlichkeit getroffen werden.

Die ursprüngliche Definition der Potenzfunktion ist, dass

$$x^y = 1 * x * x * ... * x$$

wobei 1 mit x genau y-mal multipliziert wird. Dies ist aber lediglich eine sinnvolle Definition für $y = 1, 2, ...$ (auf den Fall $y = 0$ wollen wir später zurückkommen, auch wenn er an dieser Stelle durchaus zulässig zu sein scheint). Diese Operation hat eine Vielzahl von Eigenschaften, einige von diesen sind:

1. $x^1 = x$.

2. Für alle x, n und m ist $x^n * x^m = x^{n+m}$.

3. Ist x positiv, so ist auch x^n positiv.

   An dieser Stelle können wir nun untersuchen, wie weit wir den Definitionsbereich dieser Operation ausdehnen können, ohne dabei obige Eigenschaften (und auch weitere) zu verlieren. Dies führt auf natürliche Weise zur Definition von x^y für positives x und $y \in \mathbb{Q}$, wobei wir

   $$x^{p/q} = \sqrt[q]{x^p}$$

setzen. Diese Definition fällt mit der ursprünglichen Potenzfunktion auf deren gemeinsamem Definitionsbereich zusammen und erfüllt zudem noch 1., 2. und 3. Dies ist sogar die einzige Funktion, die diese Eigenschaften auf diesem Definitionsbereich erfüllt. Die Operation hat nun noch einige andere Eigenschaften:

4. Ist $x > 1$, dann ist x^y eine wachsende Funktion in y.

5. Ist $0 < x < 1$, so ist x^y eine fallende Funktion in y.

   Wiederum können wir uns an dieser Stelle fragen, ob und wie wir die Potenzfunktion ausweiten können unter Beibehaltung der Eigenschaften 1. - 5. Dies führt in natürlicher Weise zu $x \in \mathbb{R}^+$ und $y \in \mathbb{R}$ durch:

   Ist $x > 1$, so definieren wir x^y als $\sup\{q \in \mathbb{Q} \text{ mit } q \leq y | \; x^q\}$.

   Ist $x < 1$, so definieren wir x^y als $\inf\{q \in \mathbb{Q} \text{ mit } q \geq y | \; x^q\}$.

   Ist $x = 1$, so definieren wir $x^y := 1$.

   Wie zuvor erfüllt die Operation die Eigenschaften 1. - 5. und ist dadurch auf diesem Definitionsbereich eindeutig bestimmt.

   Die nächste Erweiterung ist um einiges schwieriger. Benutzen wir die Erkenntnisse der Analysis oder Wahrscheinlichkeitsrechnung, so können wir zeigen, dass, wenn wir e als

$$e := 1 + 1/1! + 1/2! + ... = 2,71828...$$

   definieren, für jede reelle Zahl x

6. $e^x = 1 + x/1! + x^2/2! + ...$ gilt. e^x wird auch häufig mit $\exp(x)$ bezeichnet. (Diese Reihe ist absolut konvergent).

   Nun kann man auch eine Operation $\ln(x)$ auf den positiven reellen Zahlen definieren, welche die inverse Operation zur Potenzierung von e ist. D.h. dass $\exp(\ln(x)) = x$ für alle positiven x ist.

7. Noch mehr: Ist x positiv, so gilt $x^y = \exp(y \ln(x))$. An dieser Stelle wollen wir nun die Potenzierung auf komplexe Potenzen ausweiten, indem wir

$$\exp(z) = 1 + z/1! + z^2/2! + ...$$

   für alle komplexen Exponenten z definieren. Damit definieren wir nun

$$x^z := \exp(z \ln(x))$$

   für positives reelles x und komplexes z.

Diese Funktion ist nun wiederum eindeutig unter Berücksichtigung der Eigenschaften 1. - 7.; aus diesem Grund ist dies die allgemein akzeptierte moderne Definition der Potenzfunktion.

Betrachten wir nun die Identitäten

$$\cos(x) = 1 - x^2/2! + x^4/4! - ...$$

und

$$\sin(x) = x/1! - x^3/3! + x^5/5!...$$

welche die Potenzreihenentwicklung der trigonometrischen Sinus- und Cosinus-Funktion sind, so erhalten wir für reelle x

8. $\exp(ix) = \cos(x) + i\sin(x)$.

Daraus erhalten wir Eulers Formel

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

und damit

$$e^{2i\pi} = e^0 = 1$$

Außerdem können die bekannten Additionstheoreme für Sinus und Cosinus aus den Eigenschaften 1. bis 8. hergeleitet werden.

Alle obige Erweiterungen sind auf reelle und positive Basen beschränkt. Würden wir hierauf verzichten und allgemein reelle Basen zulassen, so ergäben sich Mehrdeutigkeiten. Z.B. könnte $(-1)^{1/2}$ entweder i oder $-i$ sein, $(-1)^{1/3}$, könnte -1, $\frac{1}{2}+\frac{\sqrt{3}i}{2}$, $\frac{1}{2}-\frac{\sqrt{3}i}{2}$ sein und so weiter. Einige Werte von y und x lassen sogar unendlich viele Möglichkeiten für die Definition von x^y zu, alle gleich plausibel. Selbstverständlich hat der Fall $x = 0$ seine eigenen Probleme.

Diese Probleme können alle darauf zurückgeführt werden, dass die Exponentialfunktion exp in $\mathbb{C}$ nicht mehr injektiv ist, also ln außerhalb bestimmter Streifen nicht mehr wohldefiniert ist. Es gibt viele Wege diese Schwierigkeiten zu umgehen (z.B. verschiedene Zweige von ln zu betrachten), darauf wollen wir aber nicht weiter eingehen.

Die Operation der Potenzierung kann auch auf andere Systeme wie Matrizen und Operatoren ausgeweitet werden. Der Schlüssel hierbei ist, eine jeweilige Exponentialfunktion wie in 6. zu definieren.

Referenzen

Complex Analysis. *Ahlfors, Lars V.* McGraw-Hill, 1953.

4.1.2 Was ist 0^0?

Um uns einigen Analysisbüchern anzuschließen, 0^0 ist eine „undefinierte Form“. Um nun einen Grenzwert der Form 0^0 auszuwerten, müssen häufig spezielle Techniken wie die L'Hospital-Regel angewendet werden. Andererseits scheint $0^0 = 1$ eine der am meisten verbreiteten Wahlen zu sein. Diese Konvention erlaubt es, viele Definitionen in verschiedenen Bereichen der Mathematik vorzunehmen ohne 0 als Spezialfall auszuweisen. Es sei angemerkt, dass 0^0 eine Unstetigkeitsstelle der Funktion x^y darstellt. Viel wichtiger aber ist es, sich vor Augen zu führen, dass der Wert einer Funktion und der zugehörige Grenzwert nicht zusammenfallen müssen und dass Funktionen nicht stetig sein müssen (vgl. z.B. die Diracsche Deltafunktion).

Dies bedeutet, dass man abhängig vom Kontext an einigen Stellen 0^0 als 1, an anderen aber als undefiniert oder nicht existent setzen möchte.

Einige Menschen hingegen empfinden es als sehr unelegant einer Funktion einen Wert zuzuweisen, der zu einer essentiellen Unstetigkeit führt, wie es bei x^y in (0,0) der Fall ist. Andere verweisen durchaus zu Recht darauf, dass in der Mathematik einfache Handhabung und Konsistenz äußerst wichtig sind und unter diesen Voraussetzungen $0^0 = 1$ eine natürliche Wahl ist.

Das folgende ist eine Liste von Gründen, warum 0^0 als 1 gesetzt werden sollte.

Rotando und Korn zeigen, dass sich, wenn f und g reelle Funktionen sind, die im Urpsrung verschwinden und analytisch sind (unendlich oft differenzierbar reicht an dieser Stelle nicht aus), $f(x)^{g(x)}$ dem Wert 1 annähert, wenn x von rechts gegen 0 läuft.

Aus Concrete Mathematics S.162 (R. Graham, D. Knuth, O. Patashnik):

> Some textbooks leave the quantity 0^0 undefined, because the functions x^0 and 0^x have different limiting values when x decreases to 0. But this is a mistake. We must define $x^0 = 1$ for all x, if the binomial theorem is to be valid when $x = 0$, $y = 0$, and/or $x = -y$. The theorem is too important to be arbitrarily restricted! By contrast, the function 0^x is quite unimportant.

Erschienen bei Addison-Wesley, 2nd printing, Dezember 1988.

Als Faustregel könnte man sagen, dass $0^0 = 1$, aber $0.0^{0.0}$ undefiniert ist. Dies soll andeuten, dass es darauf ankommt, welchen Grenzwert (ob links- oder rechtsseitig) man betrachtet. Aber Kahan führt an, dass $0.0^{0.0} = 1$ ist, sind nämlich f und g analytische Funktionen, mit $f(x), g(x) \to 0$, wenn $x \to a$, dann konvergiert auch $f(x)^{g(x)} \to 1$ für $x \to a$.

Die Diskussion um 0^0 ist sehr alt. Euler argumentierte für $0^0 = 1$, da $a^0 = 1$ für $a \neq 0$ gilt. Die Kontroverse wütete hauptsächlich im 19. Jahrhundert, allerdings eher auf den Seiten der unbedeutenderen Zeitschriften „Grunerts Archiv“ und „Schlomilch’s Zeitschrift für Mathematik und Physik.“ geführt. Inzwischen wurde Konsens darüber erreicht, $0^0 = 1$ zu setzen.

Der italienische Mathematiker Guglielmo Libri schrieb über den Nutzen der Funktion 0^{0^x}:

[T]he paper [33] did produce several ripples in mathematical waters when it originally appeared, because it stirred up a controversy about whether 0^0 is defined. Most mathematicians agreed that $0^0 = 1$, but Cauchy [5, page 70] had listed 0^0 together with other expressions like $0/0$ and $\infty - \infty$ in a table of undefined forms. Libris justification for the equation $0^0 = 1$ was far from convincing, and a commentator who signed his name simply S rose to the attack [45]. August Möbius [36] defended Libri, by presenting his former professors reason for believing that $0^0 = 1$ (basically a proof that $\lim\limits_{x\to 0+} x^x = 1$). Möbius also went further and presented a supposed proof that $\lim\limits_{x\to 0+} f(x)^{g(x)}$ whenever $\lim\limits_{x\to 0+} f(x) = \lim\limits_{x\to 0+} g(x) = 0$.

Of course S then asked [3] whether Mobius knew about functions such as $f(x) = e^{-1/x}$ and $g(x) = x$. (And paper [36] was quietly omitted from the historical record when the collected words of Möbius were ultimately published.) The debate stopped there, apparently with the conclusion that 0^0 should be undefined.

But no, no, ten thousand times no! Anybody who wants the binomial theorem

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

to hold for at least one nonnegative integer n must believe that $0^0 = 1$, for we can plug in $x = 0$ and $y = 1$ to get 1 on the left and 0^0 on the right.

The number of mappings from the empty set to the empty set is 0^0 . It has to be 1.

On the other hand, Cauchy had good reason to consider 0^0 as an undefined limiting form, in the sense that the limiting value of $f(x)^{g(x)}$ is not known a priori when $f(x)$ and $g(x)$ approach 0 independently. In this much stronger sense, the value of 0^0 is less defined than, say, the value of $0 + 0$. Both Cauchy and Libri were right, but Libri and his defenders did not understand why truth was on their side.

[3] *Anonymous and S.* . . Bemerkungen zu den Aufsatze überschrieben, Beweis der Gleichung 0^0 =1, nach J. F. Pfaff, im zweiten Hefte dieses Bandes, S. 134, Journal f ur die reine und angewandte Mathematik, 12 (1834), 292294.
[5] OEuvres Compl‘etes. *Augustin-Louis Cauchy.* Cours dAnalyse de lEcole

Royale Polytechnique (1821). Series 2, volume 3.
[33] *Guillaume Libri*. Memoire sur les fonctions discontinues, Journal für die reine und angewandte Mathematik, 10 (1833), 303316.
[36] *A. F. Möbius*. Beweis der Gleichung $0^0 = 1$, nach J. F. Pfaff. Journal f ur die reine und angewandte Mathematik, 12 (1834), 134136.
[45]S. . . Sur la valeur de 0^0 . Journal fur die reine und angewandte Mathematik 11, (1834), 272273.

Referenzen

Knuth. **Two notes on notation**. (AMM 99 no. 5 (May 1992), 403422).
H. E. Vaughan. **The expression** 0^0. Mathematics Teacher 63 (1970), pp.111-112.
Kahan, W. Branch Cuts for Complex Elementary Functions or Much Ado about Nothings Sign Bit, The State of the Art in Numerical Analysis, editors A. Iserles and M. J. D. Powell, Clarendon Press, Oxford, pp. 165212.
Louis M. Rotando and Henry Korn. The Indeterminate Form 0 0 . Mathematics Magazine,Vol. 50, No. 1 (January 1977), pp. 41-42.
L. J. Paige,. A note on indeterminate forms. American Mathematical Monthly, 61 (1954), 189-190; reprinted in the Mathematical Association of Americas 1969 volume, Selected Papers on Calculus, pp. 210-211.
Baxley & Hayashi. A note on indeterminate forms. American Mathematical Monthly, 85 (1978), pp. 484-486.
Crimes and Misdemeanors in the Computer Algebra Trade. Notices of the American Mathematical Society, September 1991, volume 38, number 7, pp.778-785

4.1.3 Warum ist 0,9999...=1?

In der modernen Mathematik stellt die Zeichenkette 0,9999... eine Abkürzung für die unendliche Summe $9/10 + 9/100 + 9/1000 + ...$ dar. Benutzt man die wohlbekannte $\epsilon - \delta$-Methode um den Grenzwert dieser Summe zu bestimmen, so ergibt sich (wie man leicht in jedem Analysis-Buch nachlesen kann), dass der Grenzwert 1 ist. Die Schreibweise $0,9999... = 1$ ist somit eine Abkürzung für die folgende Zeile

$$0,9999... = \sum_{j=1}^{\infty} \frac{9}{10^j} = \lim_{m\to\infty} \sum_{j=1}^{m} \frac{9}{10^j} = 1.$$

Um nun wirklich alle Zweifel auszuräumen wollen wir diesen Nachweis erbringen.

Sei also $\epsilon > 0$ beliebig. Wir setzen $\delta = \frac{1}{-\log_{10}(\epsilon)}$, also ist $\epsilon = 10^{-1/\delta}$. Damit haben wir dann für jedes $m > 1/\delta$

$$\left| \sum_{n=1}^{m} \frac{9}{10^n} - 1 \right| = \frac{1}{10^m} < \frac{1}{10^{1/\delta}} = \epsilon$$

Somit ist nach der $\epsilon - \delta$ Definition

$$\sum_{n=1}^{m} \frac{9}{10^m} = 1.$$

Reicht das immer noch nicht? In diesem Fall müssen wir zurück zur Konstruktion der Zahlsysteme gehen. Nachdem man nun die reellen Zahlen konstruiert hat (Cauchy-Folgen sind hierfür sehr gut geeignet, vgl. [Shapiro75]), kann man die Schlussfolgerung 0,9999...=1 aus dem obigen ableiten.

Ein anderer „Beweis“ (allerdings mehr informeller Natur) kann durch die folgenden Operationen gegeben werden:

$$\begin{aligned} x &= 0,9999... \\ 10x &= 10 \cdot 0,9999.... \\ 10x &= 9,9999... \\ 10x - x &= 9,9999... - 0,9999... \\ 9x &= 9 \\ x &= 1 \end{aligned}$$

Also ist 0,9999...=1.

Ein zweites, einfacheres Argument ist, $0,3333... = 1/3$ auf beiden Seiten mit 3 zu multiplizieren. Dies führt zu

$$0,9999... = 3/3 = 1.$$

Ein drittes Argument wäre festzustellen, dass sich alle periodischen Zahlen, so wie 0,4646... , als Bruch darstellen lassen, wenn man ihre Periode durch die gleiche Anzahl an 9en teilt. So ist z.B. $0,4646... = \frac{46}{99}$. Damit wird dann $0,9999... = \frac{9}{9} = 1$.

Alle drei obigen Argumente mögen dafür sprechen, dass 0,9999...=1 richtig ist, und sie mögen auch überzeugend wirken, dennoch stellen sie keine vollständigen Beweise dar. Zudem sind es auch ziemlich umständliche Methoden zu zeigen, dass 0,9999...=1 ist. Der direkte Beweis ist wesentlich einfacher.

Man erhält diesen einfach, indem man eine der umständlichen Methoden von oben ein wenig modifiziert. Betrachten wir z.B die erste Methode. Der erste Schritt besagt, dass 0,9999... eine reelle Zahl ist. Dies kann man wie zu Beginn dieses Abschnitts zeigen. Damit hat man dann aber sofort als Korollar, dass 0,9999...=1 ist. Damit ist der Rest der Argumentation irrelevant, da man schon gezeigt hat, was man beweisen wollte.

Referenzen

R.V. Churchill and J.W. Brown. *Complex Variables and Applications*. 5 th ed., McGraw-Hill, 1990.
E. Hewitt and K. Stromberg. *Real and Abstract Analysis*. Springer-Verlag, Berlin, 1965.
W. Rudin. *Principles of Mathematical Analysis*. McGraw-Hill, 1976.
L. Shapiro. *Introduction to Abstract Algebra*. McGraw-Hill, 1975.

4.2 Wie heißt die Funktion $f(x)^{f(x)} = x$

Löst man die Gleichung nach f auf, so erhält man einen Kettenbruch

$$f(x) = \frac{\log(x)}{\log\left(\frac{\log(x)}{\log\left(\frac{\log(x)}{\log\ldots}\right)}\right)}$$

Die Frage wurde schon oft gestellt, allerdings schien noch nie jemand eine Arbeit zu diesem Thema veröffentlich zu haben, genauso wie niemand dieser Funktion einen Namen gegeben hatte.

Die Funktion ist das Inverse zu $g(x) = x^x$. Man mag an dieser Stelle argumentieren, dass die Beschreibung „Das Inverse der Funktion $g(x) = x^x$“ ausreichend und genügend ist.

Ein anderer möglicher Name wäre $lx(x)$. Dies begründet sich darin, dass das Inverse e^x die Funktion $\ln(x)$ ist, also könnte das Inverse von x^x auch $lx(x)$ genannt werden.

Allerdings ist f keine analytische Funktion.

Die Kettenbruchform ist zudem noch numerisch äußert instabil in der Umgebung des Minimums bei $\frac{1}{e}$, ausserhalb konvergiert der Kettenbruch allerdings ausreichend gut. Um den Wert in der Nähe von $\frac{1}{e}$ zu bestimmen, kann das Bisektionsverfahren benutzt werden, was sehr gute Ergebnisse liefert. Allerdings konvergiert das Bisektionsverfahren an anderen Stellen wesentlich langsamer als der Kettenbruch, also ist ein hybrides Verfahren zu empfehlen. Es sei angemerkt, dass die Funktion für reelle Werte zwei- und für komplexe Werte sogar mehrdeutig ist.

Eine ähnliche Funktion ist die in MAPLE integrierte Funktion $W(x)$, die auch Lamberts W-Funktion genannt wird. MAPLE schlägt für f auch eine Lösung in Termen von W in geschlossener Form vor (wie die erf Funktion). W wird durch $W(x)\exp(W(x)) = x$ definiert.

So ist $f(x) = \exp(W(\log(x)))$ die Lösung von $f(x)^{(x)} = x$.

Eine ausführliche Behandlung der bekannten Eigenschaften der Lambertschen W-Funktion ist per anonymous FTP unter `dragon.uwaterloo.ca at /cs-archive/CS-93-03` erhältlich.

4.3 Bekannte mathematische Konstanten

Eine Tabelle von ca. 120 bekannten mathematischen Konstanten, wie π, w, $\sqrt{2}$, die Parking–Konstanten, die Feigenbaum–Konstante, . . ., kann mit Referenz und 1.024 Stellen – soweit möglich – beim Centre for Experimental and Constructive Mathematics, Simon Fraser University unter `http://www.cecm.sfu.ca/projects/ISC.htm` gefunden werden.

Eine andere von Steve Finche bereitgestellte Quelle ist unter

`http://www.mathsoft.com/asolve/constant/constant.html`

erhältlich.

Kapitel 5

Menschliches Interesse

5.1 Indiana setzt den Wert von π per Erlass auf 3

Der Gesetzesentwurf *House Bill No. 246, Indiana State Legislature, 1897* setzt den Wert von π auf einen falschen (angenäherten) rationalen Wert fest.

Dies ist der Text des Gesetzes:

> HOUSE BILL NO. 246 A bill for an act introducing a new mathematical truth and offered as a contribution to education to be used only by the State of Indiana free of cost by paying any royalties whatever on the same, provided it is accepted and adopted by the official action of the legislature of 1897.
>
> Section 1. Be it enacted by the General Assembly of the State of Indiana: It has been found that a circular area is to the square on a line equal to the quadrant of the circumference, as the area of an equilateral rectangle is to the square on one side. The diameter employed as the linear unit according to the present rule in computing the circles area is entirely wrong, as it represents the circles area one and one-fifths times the area of a square whose perimeter is equal to the circumference of the circle. This is because one-fifth of the diameter fils to be represented four times in the circles circumference. For example: if we multiply the perimeter of a square by one-fourth of any line one-fifth greater than one side, we can, in like manner make the squares area to appear one fifth greater than the fact, as is done by taking the diameter for the linear unit instead of the quadrant of the circles circumference.

> Section 2. It is impossible to compute the area of a circle on the diameter as the linear unit without trespassing upon the area outside the circle to the extent of including one-fifth more area than is contained within the circles circumference, because the square on the diameter produces the side of a square which equals nine when the arc of ninety degrees equals eight. By taking the quadrant of the circles circumference for the linear unit, we fulfill the requirements of both quadrature and rectification of the circles circumference. Furthermore, it has revealed the ratio of the chord and arc of ninety degrees, which is as seven to eight, and also the ratio of the diagonal and one side of a square which is as ten to seven, disclosing the fourth important fact, that the ratio of the diameter and circumference is as five-fourths to four; and because of these facts and the further fact that the rule in present use fails to work both ways mathematically, it should be discarded as wholly wanting and misleading in its practical applications.
>
> Section 3. In further proof of the value of the authors proposed contribution to education, and offered as a gift to the State of Indiana, is the fact of his solutions of the trisection of the angle, duplication of the cube and quadrature having been already accepted as contributions to science by the American Mathematical Monthly, the leading exponent of mathematical thought in this country. And be it remembered that these noted problems had been long since given up by scientific bodies as unsolvable mysteries and above mans ability to comprehend.

Will E. Edington veröffentlichte einen Artikel in den Proceedings of the Indiana Academy of Science, in dem er das Schicksal des Gesetzes in den Komitees der Legislative Indianas schildert. Zunächst wurde es dem House Committee on Canals vorgelegt, auch als Committee on Swamp Lands bekannt. Erwähnt wurde das Gesetz im Indianapolis Journal und dem Indianapolis Sentinel am 19. Januar 1897, beide beschrieben es als Gesetz, das die Quadratur des Kreises erlaubt. Am gleich Tage noch schickte der Abgeordnete M.B.Butler aus Steuben County, Vorsitzender des Committee on Canals, den folgenden Bericht:

> 'Your Committee on Canals, to which was referred House Bill No.246, entitled an act for the introduction of a mathematical truth, etc., has had the same under consideration and begs leave to report the same back to the House with the recommendation that said bill be referred to the Committee on Education.'

Am nächsten Tag erschien der folgende Artikel im Indianapolis Sentinel:

> „To SQUARE THE CIRCLE Claims Made That This Old Problem Has Been Solved. The bill telling how to square a circle, introduced in the House by Mr.Record, is not intended to be a hoax. Mr. Record knows nothing of the bill with the exception that he introduced it by request of Dr.Edwin Goodwin of Posey County, who is the author of the demonstration. The latter and State Superintendent of Public Instruction Geeting believe that it is the long-sought solution of the problem, and they are seeking to have it adopted by the legislature. Dr. Goodwin, the author, is a mathematician of note. He has it copyrighted and his proposition is that if the legislature will indorse the solution, he will allow the state to use the demonstration in its textbooks free of charge. The author is lobbying for the bill.
>
> On February 2, 1897, ...Representative S.E. Nicholson, of Howard County, chairman of the Committee on Education, reported to the House.
>
> Your Committee on Education, to which was referred House Bill No.246, entitled a a bill for an act entitled an act introducing a new mathematical truth, has had same under consideration, and begs leave to report the same back to the House with the recommendation that said bill do pass.
>
> The report was concurred in, and on February 8, 1897, it was brought up for the second reading, following which it was considered engrossed. Then Mr. Nicholson moved that the constitutional rule requiring bills to be read on three days be suspended, that the bill may be read a third time now. The constitutional rule was suspended by a vote of 72 to 0 and the bill was then read a third time. It was passed by a vote of 67 to 0, and the Clerk of the House was directed to inform the Senate of the passage of the bill.'

Die Zeitungen berichteten sachlich über die Aufhebung der konstitutionellen Regeln und die unglaubliche Passage dieses Gesetzes, ausgenommen einer Zeile im Indianapolis Journal, in dem es hieß, dass dies eines der seltsamsten Gesetze sei, das die „Indiana Assembly“ jemals verabschiedet habe.

Das Gesetz wurde schließlich am 10. Februar 1897 dem Senat vorgelegt und am 1. Februar das erste Mal verlesen und an das Committee on Temperance weitergeleitet. Am 12. Februar verlas Senator Harry S. New, of Marion

County, Vorsitzender des Committee on Temperance, seinen Report im Senat:

> „Your committee on Temperance, to which was referred House Bill No.246, introduced by Mr.Record, has had the same under consideration and begs leave to report the same back to the Senate with the recommendation that said bill do pass.“

Das Senate Journal erwähnt lediglich, dass das Gesetz am 12. Februar ein zweites Mal verlesen wurde und dass es einen erfolglosen Versuch gab, das Gesetz durch Ausstreichen der Klausel, letztendlich wurde es auf unbestimmte Zeit verschoben. Dass das Gesetz schließlich doch nicht in Kraft trat, scheint mehr ein glücklicher Zufall zu sein als der höheren Weisheit des Senats zuzuschreiben. Es ist wahr, dass das Gesetz weitstens in Indiana und anderes Staaten belächelt und bespöttelt, aber was letztendlich den Ausschlag gegen das Gesetz brachte, ist von Prof. C.A. Waldo in einem Artikel zusammengefasst, den er in den Proceedings der Indiana Academy of Science 1916 schrieb. Der eigentliche Grund, den er kennt, ist, dass es sich begab, dass er sich im Foyer des State Capitols für die Anweisung der Indiana Academy of Science befand, an dem Tag, als das House Bill 246 es passierte. Als er in den Fundus ging, war die Debatte um House Bill 246 schon im Gang. In seinem Artikel schreibt er übereinstimmend mit Edington

> „An ex-teacher from the eastern part of the state was saying: 'The case is perfectly simple. If we pass this bill which establishes a new and correct value for , the author offers to our state without cost the use of his discovery and its free publication in our school text books, while everyone else must pay him a royalty.“.

Die Gesetzesrolle wurde dann aufgerufen und passiert die dritte und letzte Lesung im Unterhaus. Ein Mitglied zeigte dem Schreiber eine Kopie des Gesetzes und sagte, dass er für den Autor des Gesetzes gerne eine Einweisung hätte. Er lehnte diese Höflichkeit mit Dank ab und verwies darauf, dass er mit genauso vielen verrückten Leuten bekannt war, wie er kannte.

> 'That evening the senators were properly coached and shortly thereafter as it came to its final reading in the upper house they threw out with much merriment the epoch making discovery of the Wise Man from the Pocket.'

Das Gesetz nennt vier verschiedene Werte für π und einen für $\sqrt{2}$, wie folgt:

$$\pi' = 16/\sqrt{3}, 2\sqrt{5\pi/6}, 16\sqrt{2}/7, 16/5 \text{ (bzw. 9.24, 3.236, 3.232, 3.2) und}$$
$$\sqrt{2}' = 10/7.$$

> It has been found that a circular area is to the square on a line equal to the quadrant of the circumference, as the area of an equilateral rectangle is to the square on one side.

$\pi' : (\pi'/2)^2 = \sqrt{3}/4 : 1$, z.B. $\pi' = 16/\sqrt{3} = 9.24$.

> The diameter employed as the linear unit according to the present rule in computing the circles area is entirely wrong, as it represents the circles area one and one-fifths times the area of a square whose perimeter is equal to the circumference of the circle. This is because one-fifth of the diameter fails to be represented four times in the circles circumference.

Ein wenig schwierig zu verstehen, aber es scheint sagen zu wollen, dass $(2\pi'/4)^2 6/5 = \pi$ z.B. $\pi' = 2\sqrt{5\pi/6} = 3.236$ ist

> Furthermore, it has revealed the ratio of the chord and arc of ninety degrees, which is as seven to eight,

$\sqrt{2} : \pi/2 = 7 : 8$ z.B. $\pi = 16\sqrt{2}/7 = 3.232$

> and also the ratio of the diagonal and one side of a square which is as ten to seven

z.B $\sqrt{2} = 10/7 = 1.429$

> that the ratio of the diameter and circumference is as five-fourths to four

z.B. $\pi = 16/5 = 3.2$.

5.2 Die Fieldsmedaille

5.2.1 Historische Einführung

Dies ist der Originalbrief, den Fields schrieb, eine Auszeichnung mit einer Medaille, die seinen Namen trägt, zu erschaffen. Man vermutet, dass er diesen Brief einige Monate vor seinem Tod schrieb. Es sei angemerkt, dass keine Altersbeschränkung erwähnt wird (derzeit gibt es eine eine Beschränkung auf 40 Jahre) und dass die Medaille nicht den Namen einer Person tragen sollte.

It is proposed to found two gold medals to be awarded at successive International Mathematical Congress for outstanding achievements in mathematics. Because of the multiplicity of the branches of mathematics and taking into account the fact that the interval between such congresses is four years it is felt that at least two medals should be available. The awards would be open to the whole world and would be made by an International Committee.

The fund for the founding of the medals is constituted by balance left over after financing the Toronto congress held in 1924. This must be held in trust by the Government or by some body authorized by government to hold and invest such funds. It would seem that a dignified method for handling the matter and one which in this changing world should most nearly secure permanency would be for the Canadian Government to take over the fund and appoint as his custodian say the Prime Minister of the Dominion or the Prime Minister in association with the Minister of Finance. The medals would be struck at the Mint in Ottawa and the duty of the custodian would be simply to hand over the medals at the proper time to the accredited International Committee.

As things are at present a practical course of procedure would seem to be for the Executive Committee of a Congress to appoint a small international committee authorized to add to its number and call into consultation other mathematicians as it might deem expedient. The Committee would be expected to decide on the ones to whom the awards should be made thirty months in advance of the following Congress.

Its decisions would be communicated to the President and Secretary of the Organizing Committee of the Congress, this Committee having the duty of communicating to the Prime Minister of Canada the names of the recipients in order that the medal might be prepared in time and forwarded to the president of the Organizing Commit-tee. Immediately on the appointment of the Executive Committee of the Congress the medals would be handed over to its President. The presentation of the medals would constitute a special feature at some general meeting of the Congress. In the above arrangements the role of the Organizing Committee might be taken over by the Executive of the International Mathematical Union at some time in the future when that organization has been generally accepted.

In coming to its decision the hands of the IC should be left as free as possible. It would be understood, however, that in making the awards while it was in recognition of work already done it was at the same time intended to be an encouragement for further achievement on the part of the recipients and a stimulus to renewed effort on the part of others.

In commenting on the work of the medalists it might be well to be conservative in ones statements to avoid envidious comparisons explicit or implied. The Committee might ease matters by saying they have decided to make the awards along certain lines not alone because of the outstanding character of the achievement but also with a view to encouraging further development along these lines. In this connection the Committee might say that they had elected to select subjects in Analysis, in Geometry, in the Theory of Groups, in the Theory of Numbers etc. as the case might be. When the Committee had come to an agreement in this sense the claims for recognition of work done along the special lines in question could be considered in detail by two smaller groups or subcommittees with specialized qualifications who would have authority to take into consultation or add to the subcommittees other mathematicians of specialized knowledge.

With regard to the medals themselves, I might say that they should each contain at least 200 dollars worth of gold and be of a fair size, probably 7.5 centimeters in diameter. Because of the international character the language to be employed it would seem should be Latin or Greek? The design has still to be definitely determined. It will have to be decided on by artists in consultation with mathematicians. The suggestions made in the preceding are tentative and open to consideration on the part of mathematicians.

It is not contemplated to make an award until 1936 at the Congress following that at Zurich during which an international Medal Committee should be named.

The above programme means a new departure in the matter of international scientific cooperation and is likely to be the precursor of moves along like lines in other sciences than mathematics.

One would hear again emphasized the fact that the medals should be of a character as purely international and impersonal as possible. There should not be attached to them in any way the name

> of any country, institution or person.
>
> Perhaps provision could be made as soon as possible after the appointment of the Executive of the Zurich Congress for the consideration by it of the subject of the medals, and the appointment without undue delay of a Committee and the awards of the medals to be made in connection with the Congress of 1936.
>
> Suggestions with regard to the design of the medals will be welcome.
>
> (signed) J.C. Fields Research Professor of Mathematics University of Toronto

Weitere Informationen können unter

`URL: http://www.math.toronto.edu/fields.html`

gefunden werden.

5.2.2 Tabelle der Preisträger

Jahr	Name	Geburtsort	Land	Alter
1936	Ahlfors, Lars	Helsinki	Finnland	29
1936	Douglas, Jesse	New York, NY	USA	39
1950	Schwartz, Laurent	Paris	Frankreich	35
1950	Selberg, Atle	Langesund	Norwegen	33
1954	Kodaira, Kunihiko	Tokyo	Japan	39
1954	Serre, Jean-Pierre	Bages	Frankreich	27
1958	Roth, Klaus	Breslau	Deutschland	32
1958	Thom, Rene	Montbeliard	Frankreich	35
1962	Hormander, Lars	Mjallby	Schweden	31
1962	Milnor, John	Orange, NJ	USA	31
1966	Atiyah, Michael	London	UK	37
1966	Cohen, Paul	Long Branch, NJ	USA	32
1966	Grothendieck, Alex.	Berlin	Deutschland	38
1966	Smale, Stephen	Flint, MI	USA	36
1970	Baker, Alan	London	UK	31
1970	Hironaka, Heisuke	Yamaguchi-ken	Japan	39
1970	Novikov, Serge	Gorki	USSR	32
1970	Thompson, John	Ottawa, KA	USA	37
1974	Bombieri, Enrico	Milan	Italien	33
1974	Mumford, David	Worth, Sussex	UK	37
1978	Deligne, Pierre	Brussels	Belgien	33
1978	Fefferman, Charles	Washington DC	USA	29
1978	Margulis, Gregori	Moscow	USSR	32
1978	Quillen, Daniel	Orange, NJ	USA	38
1982	Connes, Alain	Draguignan	Frankreich	35
1982	Thurston, William	Washington DC	USA	35
1982	Yau, Shing-Tung	Kwuntung	China	33
1986	Donaldson, Simon	Cambridge	UK	27
1986	Faltings, Gerd	1954	Deutschland	32
1986	Freedman, Michael	Los Angeles	USA	35

Jahr	Name	Geburtsort	Land	Alter
1990	Drinfeld, Vladimir	Kharkov	USSR	36
1990	Jones, Vaughan	Gisborne	Neuseeland	38
1990	Mori, Shigefumi	Nagoya	Japan	39
1990	Witten, Edward	Baltimore	USA	38
1994	Pierre-Louis Lions	????	Frankreich	38
1994	Jean-Chrisophe Yoccoz	????	Frankreich	37
1994	Jean Bourgain	Oostende	Belgien	40
1994	Efim Zelmanov	Novosibirsk	USSR	39

Jahr	Name	Institution	Land
1936	Ahlfors, Lars	Harvard University	USA
1936	Douglas, Jesse	MIT	USA
1950	Schwartz, Laurent	Universite de Nancy	Frankreich
1950	Selberg, Atle	Institute for Advanced Study, Princeton	USA
1954	Kodaira, Kunihiko	Princeton University	USA
1954	Serre, Jean-Pierre	College de Frankreich	Frankreich
1958	Roth, Klaus	University of London	UK
1958	Thom, Rene	University of Strasbourg	Frankreich
1962	Hormander, Lars	University of Stockholm	Schweden
1962	Milnor, John	Princeton University	USA
1954	Serre, Jean-Pierre	College de Frankreich	Frankreich
1958	Roth, Klaus	University of London	UK
1958	Thom, Rene	University of Strasbourg	Frankreich
1962	Hormander, Lars	University of Stockholm	Schweden
1962	Milnor, John	Princeton University	USA
1966	Atiyah, Michael	Oxford University	UK
1966	Cohen, Paul	Stanford University	USA
1966	Grothendieck, Alex	University of Paris	Frankreich
1966	Smale, Stephen	University of California at Berkeley	USA
1970	Baker, Alan	Cambridge University	UK
1970	Hironaka, Heisuke	Harvard University	USA
1970	Novikov, Serge	Moscow University	USSR
1970	Thompson, John	University of Chicago	USA
1974	Bombieri, Enrico	Univeristy of Pisa	Italien
1974	Mumford, David	Harvard University	USA
1978	Deligne, Pierre	IHES	Frankreich
1978	Fefferman, Charles	Princeton University	USA
1978	Margulis, Gregori	InstPrblmInfTrans	USSR
1978	Quillen, Daniel	MIT	USA
1982	Connes, Alain	IHES	Frankreich
1982	Thurston, William	Princeton University	USA
1982	Yau, Shing-Tung	Institute for Advanced Study, Princeton	USA
1986	Donaldson, Simon	Oxford University	UK
1986	Faltings, Gerd	Princeton University	USA
1986	Freedman, Michael	University of California at San Diego	USA

Jahr	Name	Institution	Land
1990	Drinfeld, Vladimir	Phys.Inst.Kharkov	USSR
1990	Jones, Vaughan	University of California at Berkeley	USA
1990	Mori, Shigefumi	University of Kyoto?	Japan
1990	Witten, Edward	Princeton/Institute for Advanced Study	USA
1994	Pierre-Louis Lions	Universite de Paris-Dauphine	Frankreich
1994	Jean-Chrisophe Yoccoz	Universite de Paris-Sud	Frankreich
1994	Jean Bourgain	Institute for Advanced Study	USA
1994	Efim Zelmanov	University of Wisconsin	USA

Referenzen

International Mathematical Congresses, An Illustrated History 1893-1986. *Donald J.Alberts, G. L. Alexanderson and Constance Reid*. Revised Edition, Including 1986, Springer Verlag, 1987.

Tropp, Henry S. The origins and history of the Fields Medal. Historia Mathematica, 3(1976), 167-181.

5.3 Die Erdöszahl

Wir betrachten einen ungerichteten Graphen, in dem die Knoten Akademiker sind und es eine Kante zwischen den Knoten X und Y gibt, wenn X einen Artikel gemeinsam mit Y veröffentlicht hat. Die Erdöszahl von X ist dann die Länge des kürzesten Pfades von X zu Erdös.

Erdös selber hat Erdöszahl 0. Koautoren von Erdös haben Erdöszahl 1. Damit hätte dann Einstein Erdöszahl 2, da er mit Ernst Strauss einige Artikel schrieb und dieser viele mit Erdös.

Die erweiterte Erdöszahl ist definiert für Koautoren von Erdös, die mehr als einen Artikel mit ihm veröffentlicht haben. Für diese ist die erweiterte Erdöszahl definiert als $1/\#\{ArtikelalsKoautorvonErdös\}$.

Wen interessiert so etwas?

Niemand scheint darauf eine vernünftige Antwort zu haben ...

Wer ist Paul Erdös?

Paul Erdös war ein ungarischer Mathematiker. Er erhielt seinen Doktortitel von der University of Manchester und verbrachte sehr viel Zeit damit, „kleine“ Probleme und Vermutungen zu untersuchen, die sich mit Graphentheorie, Kombinatorik, Geometrie oder Zahlentheorie beschäftigten.

Er war einer der fleißigsten Schreiber von Papers und ein unermüdlicher Reisender.

Paul Erdös starb am 20. September 1996.

Zur Zeit wird die Zahl der Menschen mit Erdöszahl 2 oder kleiner auf ca. 4.750 geschätzt, wie man den Archiven von Professor Jerrold W. Grossman entnehmen kann. Diese Archive können via anonymous ftp unter vela.acs.oakland.edu im Verzeichnis pub/math/erdos oder im Internet unter `http://www.acs.oakland.edu/~grossman/erdoshp.html` eingesehen werden. Diese Archive enthalten eine Liste aller Koautoren von Erdos und aller Koautoren dieser.

Zu diesem Thema schreibt Grossman:

> Let E_1 be the subgraph of the collaboration graph induced by people with Erdös number 1. We found that E_1 has 451 vertices and 1145 edges. Furthermore, these collaborators tended to collaborate a lot, especially among themselves. They have an average of 19 other collaborators (standard deviation 21), and only seven of them collaborated with no one except Erdös. Four of them have over 100 co-authors. If we restrict our attention just to E_1, we still find a lot of joint work. Only 41 of these 451 people have collaborated with no other persons with Erdös number 1 (i.e., there are 41 isolated vertices in E_1), and E_1 has four components with two vertices each. The remaining 402 vertices in E_1 induce a connected subgraph. The average vertex degree in E_1 is 5, with a standard deviation of 6; and there are four vertices with degrees of 30 or higher. The largest clique in E_1 has seven vertices, but it should be noted that six of these people and Erdös have a joint seven-author paper. In addition, there are seven maximal 6-cliques, and 61 maximal 5-cliques. In all, 29 vertices in E_1 are involved in cliques of order 5 or larger. Finally, we computed that the diameter of E_1 is 11 and its radius is 6.
>
> Three quarters of the people with Erdös number 2 have only one co-author with Erdös number 1 (i.e., each such person has a unique path of length 2 to p). However, their mean number of Erdös number 1 co-authors is 1.5, with a standard deviation of 1.1, and the count ranges as high as 13.
>
> Folklore has it that most active researchers have a finite, and fairly small, Erdös number. For supporting evidence, we verified that all the Fields and Nevanlinna prize winners during the past three cycles (19861994) are indeed in the Erdös component, with Erdös number at most 9. Since this group includes people working in theoretical physics, one can conjecture that most physicists are also in the Erdös component, as are, therefore, most scientists in

> general. The large number of applications of graph theory to the social sciences might also lead one to suspect that many researchers in other academic areas are included as well. We close with two open questions about C, restricted to mathematicians, that such musings suggest, with no hope that either will ever be answered satisfactorily: What is the diameter of the Erdös component, and what is the order of the second largest component?

Referenzen

Caspar Goffman. **And what is your Erdos number?** American Mathematical Monthly, v. 76 (1969), p. 791.

Tom Odda (alias for Ronald Graham) On Properties of a Well–Known Graph, or, What is Your Ramsey Number? Topics in Graph Theory (New York, 1977), pp. [166-172].

5.4 Warum gibt es keinen Nobelpreis in Mathematik?

Die Nobelpreise wurden durch das Testament des schwedischen Chemikers Alfred Nobel begründet.

Einer der am meisten genannten – aber dennoch unzutreffenden – Gründe, warum Nobel keinen Preis für Mathematik vorgesehen hat, ist, dass seine Frau/Lebensgefährtin ihn wegen/mit einem berühmten Mathematiker verlassen/betrogen hat. Es wird in diesem Zusammenhang vermutet, dass Gosta Mittag-Leffler der Mathematiker gewesen sei.

Allerdings gibt es keine historische Grundlage, die diese Vermutung unterstützen.

Zum einem war Nobel niemals verheiratet.

Es gibt mehrere wahrscheinlichere Gründe, warum Nobel für Mathematik keinen Preis vorgesehen hat. Eine der wichtigsten scheint zu sein, dass er sich nicht für Mathematik interessierte und sie zudem auch nicht als praktische Wissenschaft ansah, die der Menschheit nützen könnte (eine der wichtigsten Gründe für die Gründung der Nobel Foundation).

Zudem gabe es zu dieser Zeit schon einen sehr bekannten skandinavischen Preis für Mathematiker. Hätte Nobel davon gewußt, dann ist klar, dass er weniger Interesse daran hatte, ebenfalls einen Preis für Mathematiker in seinem Testament vorzusehen.

> [...] As professor ordinarius in Stockholm, Mittag-Leffler began a

> 30-year career of vigorous mathematical activity. In 1882 he founded the Acta Mathematica, which a century later is still one of the worlds leading mathematical journals. Through his in uence in Stockholm he persuaded King Oscar II to endow prize competitions and honor various distinguished mathematicians all over Europe. Hermite, Bertrand, Weierstrass, and Poincare were among those honored by the King. [...]

Quelle: The Mathematics of Sonya Kovalevskaya by Roger Cooke (Springer-Verlag, New York etc., 1984, II.5.2, p. 90-91.

Hier sind noch einige relevante Fakten:

- Nobel war nie verheiratet, also gab es keine „Frau". (Allerdings hatte er eine Lebensgefährtin, die Wienerin Sophie Hess).
- Gosta Mittag-Leffler war ein wichtiger Mathematiker in Schweden im späten 19ten bis zum frühen 20sten Jahrhundert. Er war Begründer des Journals Acta Mathematica, spielte eine wichtige Rolle in der Unterstützung der Karriere von Sonya Kovalevskaya und war schlielich Vorsitzender der Stockholm Hogskola, dem Vorläufer der Stockholmer Universität. Dennoch scheint es äußerst unwahrscheinlich, dass er einer der führenden Kandidaten für einen ersten Nobelpreis in Mathematik gewesen wäre, hätte es einen gegeben – Poincare, Hilbert und andere wären dafür eher in Frage gekommen.
- Es gibt keinen Beweis dafür, dass Mittag-Leffler viel Kontakt mit Nobel gehabt haben könnte (der die letzten Jahre seines Lebens in Paris verbrachte), geschweige denn für eine Feindschaft zwischen den beiden aus welchem Grund auch immer. Im Gegenteil, Mittag-Leffler war bemüht, Nobel in seinen letzten Jahren davon zu überzeugen, einen wesentlichen Teil seines Vermögens der Hogskola zu vermachen. Es scheint sehr unwahrscheinlich, dass er so etwas getan hätte, wenn es vorher böses Blut zwischen ihnen gegeben hätte. Scheinbar wollte Nobel zunächst auch auf Mittag-Lefflers Ersuchen eingehen, dann kam er aber schließlich auf die Idee des Nobelpreises - sehr zum Missfallen der Hogskola, gar nicht zu reden von Nobels Verwandten und Fräulein Hess.
- Nach der sehr interessanten Studie von Elisabeth Crawford, The Beginnings of the Nobel Institution, Cambridge Univ. Press, 1984, pages 52-53:

  > Although it is not known how those in responsible positions at the Hogskola came to believe that a large bequest was

> forthcoming, this indeed was the expectation, and the disappointment was keen when it was announced early in 1897 that the Hogskola had been left out of Nobels final will in 1895. Recriminations followed, with both Pettersson and Arrhenius [academic rivals of Mittag-Leffler in the administration of the Hogskola] letting it be known that Nobels dislike for Mittag-Leffler had brought about what Pettersson termed the Nobel Flop. This is only of interest because it may have contributed to the myth that Nobel had planned to institute a prize in mathematics but had refrained because of his antipathy to Mittag-Leffler or - in another version of the same story - because of their rivalry for the affections of a woman ....

Schwester Mary Thomas a Kempis entdeckte allerdings einen Brief von R. C. Archibald in den Archiven der Brown University und diskutierte dessen Inhalt im The Mathematics Teacher (1966, pp.667-668). Archibald hatte Mittag-Leffler besucht und, seinem Bericht folgend, scheint es, dass Mittag-Leffler *glaubte*, dass das Fehlen eines Nobelpreises für Mathematik auf einer Entfremdung der beiden Männern basierte. (Dies ist jedenfalls die natürliche Lesweise, aber nicht die einzig mögliche.)

- Nun noch eine letzte Spekulation bezüglich des psychologischen Elements. Hätte Nobel, als er sein Testament schrieb, wahrscheinlich in der Stimmung, der Menschheit eine große Wohltat zu machen, einem persönlichen Groll erlaubt, seine idealistischen Pläne für dieses Monument, das er hinterlassen wollte, zu beeinträchtigen?

Nobel, ein Erfinder und Industrieller, schuf ganz einfach deshalb keinen Preis für Mathematik, weil er sich nicht für Mathematik oder theoretische Wissenschaften interessierte. In seinem Testament schreibt er von Preisen für „Erfindungen oder Entdeckungen“ von größtem praktischen Nutzen für die Menschheit. (Vielleicht begründet sich darin auch, dass der Preis für Physik wesentlich öfter für praktische Arbeiten als für theoretische verliehen wurde).

Aber die Geschichte über die Rivalität um eine Frau ist natürlich viel amüsanter und wird darum wohl auch weiterhin erzählt werden.

Referenzen

Mathematical Intelligencer, vol. 7 (3), 1985, p. 74. The Beginnings of the Nobel Institution. *Elisabeth Crawford.* Cambridge Univ. Press, 1984.

5.5 Die Internationale Mathematik-Olympiade und andere Wettbewerbe

Von der Homepage der IMO (**I**nternationale **M**athematik-**O**lympiade):

Die internationale Mathematik-Olympiade ist ein jährlicher mathematischer Wettbewerb für Highschool-Schüler. Sie ist eine der internationalen Wissenschaftsolympiaden. Die erste IMO wurde 1959 in Rumänien veranstaltet. Die übliche Größe einer offiziellen Deligation der IMO ist maximal 6 Schüler und maximal zwei Begleiter. Es gibt kein offizielles „Team". Die Schüler schreiben zwei Tests an aufeinanderfolgenden Tagen, wobei jeder Test aus drei Aufgaben besteht. Jede Aufgabe zählt sieben Punkte.

Weitere Informationen und die Resultate sind unter

`http://www.win.tue.nl/win/ioi/imo/`

erhältlich.

5.6 Wer ist N. Bourbaki?

Eine Gruppe von zumeist französischen Mathematikern, die ihre Treffen in den 30er Jahren aufnahmen und zum Ziel hatten, eine vereinheitlichte Darstellung aller Bereiche der Mathematik zu schreiben. Sie hatten einen richtungsweisenden Einfluss auf die Art, wie seitdem Mathematik betrieben wird. Für einen gut zugänglichen Einblick in diese Arbeit sei auf Dieudonne Mathematics: The Music Of Reason (Orig. Pour Lhonneur De Lesprit Humain) verwiesen.

Die Gründung ist in Andre Weil's Autobiographie beschrieben, betitelt als 'memoir of an apprenticeship' (orig. Souvenirs Dapprentissage). Es gibt ein interessantes Buch „Bourbaki" von J. Fang. In Kürze erscheint ein Buch von Liliane Beaulieu, das auszugsweise in A Parisian Cafe and Ten Proto-Bourbaki Meetings 1934-1935 im Mathematical Intelligencer 15 no.1 (1993) 27-35 erschienen ist.

Die Geschichte rund um Bourbaki ist zudem auch in Scientific American, Mai 1957 beschrieben.

Kapitel 6

Mathematische Trivia

6.1 Namen für große Zahlen

Namen für 10^k:

k	Amerikanische	Europaeische	SI--Prefix
-33			revo
-30			tredo
-27			syto
-24			fito
-21			ento
-18	quintillionth		atto
-15	Quadrillionth		femto
-12	trillionth		pico
-9	Billionth		nano
-6	Millionth		micro
-3	Thousandth		milli
-2	Hundredth		centi
-1	Tenth		deci
1	Ten		deca
2	Hundred		hecto
3	Thousand		kilo
4	Myriad		
6	Million	Million	mega
9	Billion	Milliard	giga
12	Trillion	Billion	tera
15	Quadrillion	Billiard	peta
18	Quintillion	Trillion	exa

```
21     Sextillion        Trilliard        hepa
24     Septillion        Quadrillion      otta
27     Octillion         Quadrilliard     nea
30     Nonillion         Quintillion      dea
33     Decillion         Quintilliard     una
36     Undecillion       Sextillion
39     Duodecillion      Sextilliard
42     tredecillion      Septillion
45     quattuordecillion Septilliard
48     quindecillion     Octillion
51     sexdecillion      Octilliard
54     septendecillion   Nonillion
                           (Noventillion)
57     octodecillion     Nonilliard
                           (Noventilliard)
60     novemdecillion    Decillion
63     VIGINTILLION      Decilliard

6*n    (2n-1)-illion     n-illion
6*n+3  (2n)-illion       n-illiard

100    Googol            Googol
303    CENTILLION
600                      CENTILLION

10^100 Googolplex        Googolplex


%From: balden@wimsey.com (Bruce Balden)
%Date: Fri, 11 Oct 1996 12:46:39 GMT
%uebersetzte Version

Chinesisches System

1           yi4
10          shi2
100         bai3
1000        qian2
10000       wan4
10^6        yi bai3 wan (d.h. 100 wan)
10^8        yi1
```

```
10^12      ???

Das amerikanische System wird benutzt in:
          USA,
          ...

Das europaeische System wird benutzt in:
          Oesterreich
          Belgien
          Chile
          Deutschland
          Niederlanden
          Italien
          Skandinavien


%Date: Mon, 25 Aug 1997 22:47:48 -0700
%From: Torbjorn Larsson <ekatla@eka.ericsson.se>
%Subject: Sci.math FAQ
%uebersetzte Version

Es sei angemerkt, dass alle Praefixe mit einem kleinen Buchstaben beginnen
muessen (ebenso wie alle SI-Einheiten, einschliesslich solcher, die nach
Personen benannt sind).

- Alle Praefixe mit k<0 sollten eine Abkuerzung mit kleinem Buchstaben haben.
  Z.B. 1 picoampere = 1 pA (Erklaerung zur SI-Einheit: Einheiten mit Personennamen
  werden mit einem grossen Buchstaben abgekuerzt).

- Alle Praefixe mit k>0 sollten mit einem grossen Buchstaben abgekuerzt werden,
  so z.B. 1 gigameter = 1Gm (Erklaerung zur SI-Einheit: Nichtnamenseinheiten
  werden mit kleinen Buchstaben abgekuerzt. Ausgenommen sind Masseinheiten: 1
  Kilogramm ist 1 kg (im Ggs. zu Km fuer Kilometer).


hv@cix.compulink.co.uk (Hugo van der Sanden):
  Soweit ich weiss, hat das House of Commons vor einer ganzen
  Weile -- um 1970 ? -- beschlossen, die US--Definition einer
  Billion zu uebernehmen; seitdem ist sie offizielle Regierungspolitik.
```

```
dik@cwi.nl (Dik T. Winter):
  Das Interessante an dieser Sache ist, dass urspruenglich
  die Franzosen 10^9 als Abkuerzung fuer eine Billion benutzten,
  waehrend die meisten anderen Europaer es fuer 10^12 benutzten.
  Ich glaube die Amerikaner haben ihre Abkuerzung von den
  Franzosen. Und die Franzosen wechselten 1948 zur ueblichen
  europaeischen Bezeichnung.


gonzo@ing.puc.cl (Gonzalo Diethelm):
  Andere Laender (wie Chile, mein eigenes, und ich denke auch
  der Grossteil von Lateinamerika) meinen mit Billion 10^12, mit
  Trillion 10^18, ... Wie sind die Bezeichnungsweisen wohl ueber
  die Weltbevoelkerung verteilt?
```

Kapitel 7

Berühmte Probleme in der Mathematik

7.1 Das Vierfarben-Theorem

Theorem 2 (Vierfarben-Theorem)
Jede planare Karte mit Ländern einfacher Grenzen kann mit maximal vier Farben derart eingefärbt werden, dass keine zwei Länder, die eine Grenze positiver Länge teilen, die gleiche Farbe haben.

Eine äquivalente kombinatorische Interpretation ist

Theorem 3 (Vierfarben-Theorem)
Jeder zyklenfreie, planare Graph besitzt eine Knoteneinfärbung mit maximal vier verschiedenen Farben.

Dieses Theorem wurde 1976 mit Hilfe von Computern bewiesen. Der Beweis zeigt, dass wenn ungefähr 1.936 Grundformen von Karten mit vier Farben eingefärbt werden können, es dann möglich ist, eine beliebige Karte mit nur vier Farben einzufärben. Bislang war noch niemand in der Lage, dies ohne Computer zu beweisen. Im Prinzip ist es natürlich möglich, die vom Computer durchgeführten Berechnungen auch per Hand durchzuführen ...

Die bekannten Beweise arbeiten per Widerspruch. Der Grundgedanke alle Beweise ist anzunehmen, dass es Gegenbeispiele gäbe. Dann müßte es auch ein minimales Gegenbeispiel geben, in dem Sinn, dass jede Teilmenge des Graphen auch mit vier Farben einfärbbar ist. Dann wird gezeigt, dass alle solchen Gegenbeispiele als Teilgraphen eine bestimmte Basiskonfiguration enthalten müssten.

Aber es stellt sich heraus, dass jede dieser Basiskonfigurationen durch etwas kleineres ersetzt werden kann, während weiterhin fünf Farben benötigt werden – im Widerspruch zur Minimalität.

Die Zahl dieser Basiskonfigurationen konnte auf 633 reduziert werden.

Eine neue Vereinfachung des Beweises des Vierfarben–Theorems von Robertson, Sanders, Seymour und Thomas beseitigte alle Zweifel, die dem komplexen Originalbeweis von Appel und Haken anhafteten.

Die zugehörigen Programme können nun per FTP erhalten und auf Korrektheit überprüft werden. Ebenso ist der nicht-programmierte Teil des Beweises nun wesentlich einfacher zu überprüfen. Dieser neue Beweis, sofern korrekt, sollte alle vernünftige Kritik am Beweis dieses Satzes ausräumen.

Referenzen

K. Appel and W. Haken. **Every planar map is four colorable**. Bulletin of the American Mathematical Society, vol. 82, 1976 pp.711-712.

K. Appel and W. Haken. **Every planar map is four colorable**. Illinois Journal of Mathematics, vol. 21, 1977, pp. 429-567.

N. Robertson, D. Sanders, P. Seymour, R. Thomas. **The Four Colour Theorem Preprint**. February 1994. Available by anonymous ftp from ftp.math.gatech.edu, in directory /pub/users/thomas/fcdir/npfc.

The Four Color Theorem: Assault and Conquest. *T. Saaty and Paul Kainen.* McGraw-Hill, 1977. Reprinted by Dover Publications 1986.

7.2 Die Dreiteilung eines Winkels

Theorem 4

Die Dreiteilung eines Winkels mit Zirkel und Lineal ist im allgemeinen nicht möglich.

Dieses Problem, zusammen mit Problemen wie der *Verdopplung des Würfels*, der *Konstruktion des regulären Heptagons* und der *Quadratur des Kreises*, wurde von den Griechen in der Antike aufgestellt und war bis in die Moderne ungelöst.

Die Lösung dieser Probleme ist von einem geometrischen Standpunkt aus eher unelegant. Bislang wurde kein geometrischer Beweis veröffentlicht [nachprüfen?], aber eine sehr clevere Lösung wurde unter Verwendung recht elementarer Ergebnisse aus der Theorie der Erweiterungskörper und modernen Algebra gefunden.

Es stellt sich heraus, dass die Dreiteilung eines Winkels äquivalent zur Lösung einer kubischen Gleichung ist. Konstruktionen mit Zirkel und Lineal können nur eine kleine Zahl solcher Gleichungen lösen, selbst dann, wenn wir uns auf ganzzahlige Koeffizienten beschränken. Insbesondere kann die

Gleichung für $\theta = 60^\circ$ nicht mit Zirkel und Lineal gelöst werden. Damit ist auch die Dreiteilung dieses Winkels nicht möglich.

Allerdings ist eine Dreiteilung möglich mit einem Zirkel und einem Lineal, auf dem zwei Punkte markiert sind:

Sei X ein Punkt auf dem Einheitskreis, so dass $\angle XOE$ der zu teilende Winkel ist. Zeichne nun eine Gerade AX durch einen Punkt A auf der x-Achse, so dass $|AB| = 1$ (was das gleiche wie der Radius des Einheitskreises ist), wobei B der Schnittpunkt von AX mit dem Kreis ist.

Sei $\theta = \angle BAO$. Dann ist $\angle BOA = \theta$ und $\angle XBO = \angle BXO = 2\theta$.

Da nun die Summe der Innenwinkel eines Dreiecks gleich π bzw. 180° ist, haben wir

$$\angle XBO + \angle BXO + \angle BOX = \pi.$$

Dies impliziert, dass $4\theta + \angle BOX = \pi$ ist. Nun ist ebenfalls

$$\angle AOB + \angle XOE + \angle BOX = \pi$$

und damit $\theta + \angle BOX + \angle XOE = \pi$. Da nun beide Gleichungen gleich π sind, erhalten wir

$$\theta + \angle BOX = \theta + \angle BOX + \angle XOE$$

und somit folgt letztendlich

$$3\theta = \angle XOE.$$

7.3 Was sind Hilberts 23 Probleme?

Sie wurden ursprünglich an verschiedenen Orten in Deutsch veröffentlicht. Eine Übersetzung wurde 1902 von der AMS publiziert. Dieser Artikel wurde 1976 von der AMS erneut veröffentlicht (s. Referenzen).

Das am Ende erwähnte AMS–Symposium enthält eine Serie von Artikeln über den damals aktuellen Stand der meisten Probleme (sowie die Probleme selbst).

Unter

`http://www.astro.virginia.edu/eww6n/math/Hilbert'sProblems.html`

kann eine Liste der Probleme und deren aktueller Stand eingesehen werden.

Referenzen

Mathematical Developments Arising from Hilbert Problems, volume 28 of Proceedings of Symposia in Pure Mathematics, pages 134, Providence, Rhode Island. American Mathematical Society, 1976.

D. Hilbert. Mathematical problems. Lecture delivered before the International Congress of Mathematicians at Paris in 1900. Bulletin of the American Mathematical Society, 8:437479, 1902.

7.4 Ungelöste Probleme

7.4.1 Gibt es eine Zahl, die perfekt und ungerade ist?

Eine Zahl heißt perfekt, wenn sie gleich der Summe ihrer echten Teiler ist. Die ursprüngliche Frage wurde das erste Mal von Euklid im alten Griechenland gestellt. Die Frage ist immer noch ungelöst. Euler zeigte, dass wenn N eine ungerade perfekte Zahl ist, in der Primfaktorzerlegung von N genau ein Exponent kongruent 1 modulo 4 ist, und alle anderen Exponenten sind gerade. Mehr noch: Die Primzahl mit ungeradem Exponenten muss selber kongruent 1 modulo 4 sein. Eine Kurzfassung des Beweises findet sich in Aufgabe 87 auf Seite 203 von Underwood Dudley's „Elementary Number Theory“. Bislang hat man gezeigt, dass es keine ungeraden perfekten Zahlen $< 10^{300}$ gibt.

7.4.2 Das Collatz-Problem

Sei $m \in \mathbb{Z}^+$.

```
n := m
wiederhole {
 wenn (n ungerade)
  dann
    n:=3*n+1;
  sonst
    n:=n/2;
} bis n==1
```

Vermutung Das Programm terminiert für alle positiven ganzen Zahlen m.

Die Vermutung wurde für alle Zahlen bis $5,6 \cdot 10^{13}$ nachgewiesen.

Referenzen

Unsolved Problems in Number Theory. Richard K Guy. Springer, Problem E16.
Elementary Number Theory. Underwood Dudley. 2nd ed.
G.T. Leavens and M. Vermeulen 3x+1 search programs] Comput. Math. Appl. vol. 24 n. 11 (1992), 79-99.

7.4.3 Die Goldbachsche Vermutung

Diese Vermutung besagt, dass jede gerade Zahle grösser oder gleich 4 als Summe von zwei Primzahlen darstellbar ist. Sie wurde von Sinisalo für Werte bis $4 \cdot 10^{10}$ getestet.

7.4.4 Die Primzahlzwillingsvermutung

Es gibt unendlich viele positive ganze Zahlen p, so dass p und $p + 2$ beides Primzahlen sind. Vgl. hierzu Abschnitt 3.2.3. Es gibt einige Ergebnisse über die geschätzte Dichte von Primzahlzwillingen.

Kapitel 8

Mathematische Spiele

8.1 Das Monty Hall-Problem

Dieses Problem ist inzwischen Teil der mathematischen Folklore geworden.

Der American Mathematical Monthly berichtete und erklärte das Problem (samt seiner Lösung) ausführlich in seiner Ausgabe im Januar 1992. Das Folgende stammt aus diesem Artikel:

Das Problem:

Sie sind Gast eine TV-Gewinnshow. Der Moderator zeigt Ihnen drei nummerierte Tore[1]. Hinter einer verbirgt sich ein Auto und hinter zweien jeweils eine Ziege. Aus diesen drei Toren wählt man nun eines aus und gewinnt, was sich dahinter verbirgt.

Allerdings läßt der Moderator, der weiß hinter welchem Tor sich das Auto verbirgt, nach der Wahl ein Tor mit einer Ziege dahinter öffnen und fragt Sie dann, ob Sie Ihre Wahl revidieren wollen oder nicht. Vergrößert eine Änderung der Wahl die Chance das Auto zu gewinnen?

Wenn der Moderator immer eine der beiden andere Türen öffnet, so sollten Sie wechseln. Denn in 1/3 aller Fälle haben Sie das richtige Tor (d.h. das mit dem Auto) gewählt und Wechseln ist schlecht, während Sie in 2/3 aller Fälle ein falsches Tor (d.h. eines mit einer Ziege) gewählt haben und Wechseln das Auto gewinnt.

Darum ist der Erwartungswert 2/3 bei Änderung der Wahl, also größer als der ursprüngliche Erwartungswert von 1/3 wenn man nicht wechselt.

Selbst wenn der Moderator nur manchmal anbietet zu wechseln, lohnt sich ein Wechsel. Nur wenn wir einen bösartigen Moderator annehmen (d.h. einen Moderator, der einen Wechsel auf Grundlage des Wissens anbietet, dass man das richtige Tor gewählt hat), lohnt sich wechseln nicht.

[1] Anmk. des Übersetzers: „Zonk“ ist solch eine Show

Es gibt viele Möglichkeiten sich davon zu überzeugen, dass ein Wechsel die richtige Entscheidung ist. Hier ist einer: Sie wählen ein Tor. Jetzt fragt der Moderator Sie, ob Sie wechseln möchten, **bevor** er ein Tor öffnet. Die Wahrscheinlichkeit einer falschen Wahl sind hoch (2/3), also gibt es keinen Grund sich umzuentscheiden, weil man eben nicht weiß zu welchem Tor man wechseln soll. Das bedeutet, dass die Wahrscheinlichkeit 2/3 gleichverteilt ist. Ein Wechsel ist genauso gut wie die aktuelle Situation. Aber sobald Monty (der Moderator) eines der beiden anderen Tore öffnet, sind die Chancen, das richtige Tor gewählt zu haben, weiterhin 1/3, und falls man wechselt, muss man nur noch ein Tor wählen. Also zahlt es sich aus zu wechseln.

Referenzen

L. Gillman **The Car and the Goats** American Mathematical Monthly, January 1992, pp. 3-7.

8.2 Master Mind

Es konnte gezeigt werden, dass für das Spiel Master Mind auch im ungünstigsten Fall nicht mehr als fünf Züge nötig sind.

Ein entsprechender Algorithmus wurde 1970 oder 1971 (denke ich) im Journal of Recreational Mathematics veröffentlicht; er löste das das 4-Steine-Problem stets in maximal fünf Zügen. Knuth veröffentlichte später einen Algorithmus, der durschnittlich weniger, in manchen Fällen aber sechs Züge benötigt.

1994 fanden Kenji Koyama und Tony W. Lai durch erschöpfende Suche heraus, dass $5625/1296 = 4.340$ die im Durchschnitt optimale Strategie ist. Diese Strategie benötigt im ungünstigsten Fall sechs Züge. Eine Strategie, die stets maximal fünf Züge benötigt, wurde ebenfalls präsentiert. Sie braucht durchschnittlich $5626/1296 = 4.341$ Versuche.

Referenzen

Donald E. Knuth. The Computer as Master Mind. J. Recreational Mathematics, 9 (1976-77), 1-6.
Kenji Koyama, Tony W. Lai. An optimal Mastermind Strategy. J. Recreational Mathematics, 1994.

Kapitel 9

Das Auswahlaxiom und die Kontinuumshypothese

9.1 Das Auswahlaxiom

Es gibt einige äquivalente Formulierungen des Auswahlaxioms:

- Das kartesische Produkt einer nichtleeren Menge ist nichtleer, auch wenn es ein Produkt einer unendlichen Familie von Mengen ist.
- Gegeben sei eine Menge S von paarweise disjunkten nichtleeren Mengen, dann gibt es eine Menge C, die genau ein Element von jedem Element von S enthält. (Man kann sich C als das Resultat einer „Auswahl“ eines Repräsentanten von jeder Menge in S vorstellen. Daher der Name des Axioms.)

9.1.1 Relevanz des Auswahlaxioms

Das Auswahlaxiom

Es gibt viele verschiedene Versionen des Auswahlaxioms; die folgende gab dem Axiom seinen Namen:

> Für jede Menge X gibt es eine Funktion f, mit Definitionsbereich $X \setminus \emptyset$, so dass $f(x)$ Element von x für alle nichtleeren $x \in X$ ist.

Solch ein f wird „Auswahlfunktion“ auf X genannt (es sei daran erinnert, dass in der Zermelo-Fraenkel-Mengenlehre alle mathematischen Objekte Mengen sind und somit auch jedes Element von X wieder eine Menge ist).

Das Auswahlaxiom (abgekürzt AC nach „Axiom of Choice“) ist eines der am meisten diskutierten Axiome der Mathematik, übertroffen vielleicht nur von Euklids Parallelenaxiom.

Die Axiome der Mengentheorie gaben der modernen Mathematik eine Grundlage wie Euklids fünf Postulate der euklidischen Geometrie eine Grundlage gaben; die Fragen um das AC sind die gleichen wie beim Parallelenaxiom:

1. Kann es von den anderen Axiomen abgeleitet werden?

2. Ist es konsistent mit den anderen Axiomen?

3. Sollten wir es als Axiom akzeptieren?

Für viele Mengen, einschließlich aller endlichen Mengen, reichen die ersten sechs Axiome der Mengenlehre (abgekürzt ZF nach „Zermelo-Fraenkel“) aus, um die Existenz solch einer Auswahlfunktion zu garantieren, aber es gibt Mengen, für die das AC *benötigt* wird, um die Existenz nachzuweisen. Die Existenz solcher Mengen wurde 1963 von Paul Cohen bewiesen. Das bedeutet, dass AC tatsächlich nicht aus den anderen sechs Axiomen abgeleitet werden kann; das heißt „AC ist unabhängig von ZF“. Dies beantwortet Frage 1.

Die Frage, ob AC mit den anderen Axiomen konsistent ist, wurde 1938 von Goedel beantwortet. Goedel zeigt, dass, wenn die anderen Axiome konsistent sind, auch das AC mit diesen konsistent ist. Dies ist ein Beweis „relativer Konsistenz“; mehr dürfen wir auf Grund des zweiten Goedelschen Unvollständigkeitssatzes auch nicht erwarten .

Die dritte Frage, „Sollten wir es als Axiom akzeptieren?“, führt uns in den Bereich der Philosophie. Heutzutage gibt es hinsichtlich der Verwendung des Auswahlaxioms drei große Schulen in der Mathematik:

1. Akzeptiere es als ein Axiom und benutze es ohne Zögern.

2. Akzeptiere es als ein Axiom aber benutze es nur, wenn es nicht anders geht.

3. AC ist nicht akzeptierbar.

Die meisten Mathematiker heutzutage zählen zur ersten Gruppe. Die Angehörigen der zweiten Gruppe sind meist auf Grund eines Glaubens an Occam’s Razor (benutze so wenig Annahmen wie möglich um etwas zu erklären) oder eines Interesses in Metamathematik in ihr. Es gibt eine steigende Zahl von Menschen, die zur dritten Gruppe wechseln, insbesondere Computerwissenschaftler, die an automatisiertem Beweisen mit Hilfe konstruktiver Typtheorien arbeiten.

Den verschiedenen Schulen des Umgangs mit AC liegen unterschiedliche Ansichten über Wahrheit und Natur mathematischer Objekte zu Grunde. Die drei wichtigsten sind Platonismus, Konstruktivismus und Formalismus.

Platonismus Ein Platonist glaubt, dass mathematische Objekte unabhängig vom menschlichen Denken existieren und eine mathematische Aussage wie AC objektiv entweder falsch oder wahr ist. Ein Platonist akzeptiert AC nur dann, wenn es objektiv wahr ist. Damit fallen Platonisten in die erste oder dritte Schule, je nach persönlichem Glauben. Wenn ein Platonist sich über den Wahrheitsgehalt von AC nicht sicher ist, mag er zur zweite Schule gehören, so dass er, sobald er den Wahrheitsgehalt bestimmen kann, auch weiß welche Sätze wahr sind.

Konstruktivismus Ein Konstruktivist, glaubt, dass die einzigen akzepierbaren mathematischen Objekte solche sind, die vom menschlichen Verstand konstruiert werden können und dass die einzig wahren Beweise konstruktive Beweise sind. Da nun AC keine Methode für die Konstruktion einer solchen Auswahlfunktion gibt, gehören Konstruktivisten zur dritten Schule.

Formalismus Ein Formalist glaubt, dass Mathematik strikte Symbolmanipulation ist und dass jede vernünftige Theorie studiert werden sollte. Für einen Formalisten ist der Begriff Wahrheit vom Kontext des mathematische Modells abhängig. So würde ein Formalist z.B. nicht sagen, dass das Parallelenaxiom falsch ist, sondern dass es in der Riemannschen Geometrie falsch ist. Ein Formalist würde sich selbst vermutlich zu keiner der drei Schulen zuordnen. Er würde je nach seinen derzeitigen Interessen zwischen allen drei Schulen wechseln.

Was nun? Sollte man das AC akzeptieren? Einige Pro- und Contra-Argumente dazu:

Contra

- Es ist kein simples, ästhetisches und intuitiv klares Axiom wie die anderen.
- Es ist äquivalent zu anderen Aussagen, die ebenfalls nicht intuitiv klar sind, wie „Jede Menge kann wohlgeordnet werden“. Wie würden Sie z.B. die reellen Zahlen wohlordnen?
- Mit dem Axiom kann man nicht-intuitive Resultate erzielen, wie die Existenz einer unstetigen additiven Funktion, die Existenz einer nicht-messbaren Menge von reellen Zahlen und das Banach-Tarski-Paradoxon (vgl. .

- Es ist nicht konstruktiv – es beschwört eine Menge herauf ohne eine tatsächliche Methode anzugeben, wie man diese Menge konstruieren kann.

Pro Die Akzeptanz des AC basiert auf dem Glauben, dass unsere Vorstellung von endlichen Mengen auf unendliche ausgedehnt werden kann. Der Hauptgrund es zu akzeptieren ist seine Nützlichkeit. Viele wichtige plausible Sätze sind zum AC äquivalent oder basieren darauf. Folgende Aussagen beispielsweise sind äquivalent zu AC:

- Jeder Vektorraum hat eine Basis.
- Die Trichotomie für Kardinalzahlen. Für alle Kardinalzahlen k und l gilt entweder $k < l$, oder $k = l$ oder $k > l$.
- Tychonoff's Theorem: Das Produkt von kompakten Räumen ist kompakt in der Produkttopolgie.
- Zorn's Lemma: Jede nicht-leere partiell geordnete Menge P, in der jede Kette eine obere Schranke besitzt, besitzt ein maximales Element.

Sätze, die von AC abhängen (d.h. sie können nicht aus ZF allein bewiesen werden):

- Die Vereinigung von abzählbar vielen abzählbaren Mengen ist abzählbar.
- Jede unendliche Menge hat eine abzählbare Teilmenge.
- Das Loewenheim-Skolem-Theorem: Jede Theorie erster Ordnung, die ein Modell besitzt, besitzt auch ein abzählbares Modell.
- Der Bairesche Kategoriensatz: Die reellen Zahlen sind nicht Vereinigung von abzählbar vielen nirgendwo dichten Mengen.
- Das Ultrafilter-Theorem: Zu jeder boolschen Algebra gibt es einen Ultrafilter auf dieser Algebra.

Alternativen zu AC

- Akzeptieren einer schwächeren Form von AC wie z.B. das Abzählbare AC (jede abzählbare Menge besitzt eine Auswahlfunktion) oder das Abhängige AC.
- Akzeptieren eines Axioms, das AC impliziert, wie z.B. das Axiom der Konstruierbarkeit ($V = L$) oder die Verallgemeinerte Kontinuumshypothese (GCH).

- Akzeptieren von AC als ein Axiom der Logik (Hilbert schlug dies für sein epsilon-Axiom vor). Wenn man Mengenlehre in einem solchen logischen System untersucht, wird das Auswahlaxiom zum Satz.
- Akzeptieren eines Axioms, das AC widerspricht, wie dem Axiom der Determinierung.
- Verwenden einer komplett anderen Grundlage für Mathematik, wie Kategorientheorie. Mit Kategorientheorie kann z.B. Tychonoff's Axiom ohne AC bewiesen werden (Johnstone, 1981).

Testen Sie sich, wann ist AC notwendig?

Wenn man in der ZF-Mengenlehre ohne AC arbeitet, kann man dann ein Element auswählen aus...

1. einer endlichen Menge?
2. einer unendlichen Menge?
3. jedem Element einer unendlichen Menge von einelementigen Mengen?
4. jedem Element einer unendlichen Menge von Schuhpaaren?
5. jedem Element einer unendlichen Menge von Sockenpaaren?
6. jedem Element einer endlichen Menge von Mengen, wenn jedes Element eine unendliche Menge ist?
7. jedem Element einer unendlichen Menge von Mengen, wenn jedes Element eine unendliche Menge ist?
8. jedem Element einer abzählbaren Menge von Mengen, wenn jedes Element eine unendliche Menge ist?
9. jedem Element einer unendlichen Menge von Mengen rationaler Zahlen?
10. jedem Element einer abzählbaren Menge von abzählbaren Mengen?
11. jedem Element einer unendlichen Menge von endlichen Mengen?
12. jedem Element einer unendlichen Menge von endlichen Mengen reeller Zahlen?
13. jedem Element einer unendlichen Menge von Mengen reeller Zahlen?

14. jedem Element einer unendlichen Menge von zweielementigen Mengen, deren Elemente Mengen reeller Zahlen sind?

Die Antworten können unter http://www.jazzie.com/ii/math/index.html eingesehen werden.

Referenzen

Benacerraf, Paul and Putnam, Hilary. Philosophy of Mathematics: Selected Readings, 2nd edition. Cambridge University Press, 1983.

Dauben, Joseph Warren. Georg Cantor: His Mathematics and Philosophy of the Infinite. Princeton University Press, 1979.

A. Fraenkel, Y. Bar-Hillel, and A. Levy with van Dalen, Dirk. Foundations of Set Theory, Second Revised Edition. North-Holland, 1973.

Johnstone, Peter T. Tychonoffs Theorem without the Axiom of Choice. Fundamenta Mathematica 113: 21-35, 1981.

Leisenring, Albert C. Mathematical Logic and Hilberts Epsilon-Symbol. Gordon and Breach, 1969.

Maddy, Believing the Axioms, I, J. Symb. Logic, v. 53, no. 2, June 1988, pp. 490-500, and Believing the Axioms II in v.53, no. 3.

Moore, Gregory H. Zermelos Axiom of Choice: Its Origins, Development, and In uence. Springer-Verlag, 1982.

Rubin, Herman and Rubin, Jean E. Equivalents of the Axiom of Choice II. North-Holland, 1985.

9.2 Zerteilung einer Sphäre in Teile größeren Volumens

Ist es möglich eine Sphäre so in eine endliche Anzahl von Stücken zu zerteilen, dass man die Stücke zu einem Körper doppelten Volumens zusammensetzen kann?

Diese Frage besitzt viele Varianten und wird am besten ausführlich beantwortet.

Gegeben seien zwei Polygonen gleichen Flächeninhalts. Ist es immer möglich, eines derart in eine endliche Anzahl von Stücken zu unterteilen, dass es nach Zusammensetzung identisch mit dem zweiten Polygon ist?

Die Zerteilungstheorie ist umfangreich. In solchen Fragen muss man einiges genau spezifizieren:

- Was bedeutet hier Stück? (Ein Polygon? Eine topologische Kugel? Eine Borelmenge? Eine Lebesgue-messbare Menge? Eine beliebige Menge?)
- Wieviele Stücke sind erlaubt? (Endlich viele? Abzählbar viele? Überabzählbar viele?)
- Welche Bewegungen sind beim Zusammensetzen erlaubt? (Tranlationen? Rotationen? Orientierungsumkehrende Abbildungen? Isometrien? Affine Abbildungen? Beliebige stetige Abbildungen?)
- Was ist beim „Zusammenkleben“ der Stücke erlaubt? Die einfachste Restriktion ist, dass sie disjunkt sein müssen. Sind die Stücke Polygone (oder Stücke mit glattem Rand), so kann man ein Zusammenkleben entlang der Ränder erlauben, d.h. das Innere der Stücke ist disjunkt und ihre Vereinigung die gewünschte Figur.

Einige Resultate

- Wenn wir in endlich viele Polygone zerteilen, verschieben, rotieren und entlang der Ränder zusammenkleben dürfen, dann sind zwei Polygone gleicher Fläche auch gleichzerlegbar.

  Dies wurde von Bolyai und Gerwien unabhängig voneinander bewiesen und auch unzweifelhaft schon viele Male zuvor unabhängig entdeckt. Es wäre nicht überraschend, wenn bereits die Griechen dies gewußt haben.

  Das Hadwiger-Glur-Theorem impliziert, dass zwei Polygone gleicher Fläche schon gleichzerlegbar sind, wenn man lediglich Translationen und Rotationen von 180° erlaubt.

  Theorem 5 (Hadwiger-Glur, 1951)
- Zwei gleichflächige Polygone P und Q sind gleichzerlegbar mit Translationen genau dann, wenn $\phi_P() = \phi_Q()$ ist.

  Dabei sei, für jede Richtung v (d.h. jedem Vektor auf dem Einheitskreis in der Ebene), $\phi_P(v)$ die Summe der Längen der Kanten von P, die senkrecht auf v stehen, wobei für eine Kante die Länge positiv ist, wenn v äußerlich normal auf der Kante ist und negativ, wenn v innerlich normal auf der Kante ist.

- In der dritten Dimension haben wir Hilbert's berühmtes „Drittes Problem“:

> Sind zwei Polyeder gleichen Volumens stets gleichzerlegbar, wenn man Translationen und Rotationen, endlich viele Teilpolyeder und Zusammenkleben entlang der Ränder erlaubt?

Die Antwort ist **Nein**, wie von Dehn 1900 nur wenige Monate nach Veröffentlichung des Problems gezeigt wurde. (Über raumgleiche Polyeder, Göttinger Nachrichten 1900, 345-354). Es war das erste von Hilbert's Problemen, das gelöst wurde. Zwar ist der Beweis nicht trivial; er benötigt aber nicht das Auswahlaxiom (AC).

Referenzen

Hilberts Third Problem. V.G. Boltianskii. Wiley 1978.

- Mittels Anwendung von AC auf eine nicht-abzählbare Menge kann man beweisen, dass eine feste Sphäre in endlich viele Stücke unterteilt werden kann, die so zu zwei festen Sphären zusammengesetzt werden können, dass beide das gleiche Volumen, wie das Original haben. Nicht mehr als 9 Stücke werden dazu benötigt.

  Die kleinstmöglichste Zahl hierzu ist fünf (es ist recht einfach nachzuweisen, dass vier nicht reichen). Es gibt bestimmte Unterteilungen, in denen eines der fünf Stücke das Zentrum der Originalsphäre ist und die anderen vier Stücke A, A', B und B' derart sind, dass A kongruent zu A' ist und B kongruent zu B' (vgl. Wagon's Buch).

  Diese Konstruktion ist als BANACH-TARSKI-PARADOXON bekannt oder auch als BANACH-TARSKI-HAUSDORFF-PARADOXON (Hausdorff entwickelte eine frühe Version dieses Paradoxons). Die Stücke hier sind nicht-messbare Mengen, und sie werden disjunkt zusammengesetzt (sie werden nicht entlang ihrer Rändern zusammengeklebt, anders als in Bolyai's Theorem). Ein ausgezeichnetes Buch über Banach-Tarski ist

  The Banach-Tarski Paradox. Stan Wagon. Cambridge University Press, 985

  Robert M. French. The Banach-Tarski theorem. The Mathematical Intelligencer, 10 (1988) 21-28.

  Die einzelnen Stücke sind nicht messbar, da Maße unabhängig von Bewegungen sind. Da die Stücke nicht messbar sind, haben sie auch keine venünftigen Ränder. So kann es passieren, dass der topolgische Rand jedes Stückes die ganze Einheitskugel ist.

  Das vollständige Banach-Tarski-Paradoxon ist stärker als die bloße Verdoppelung der Kugel. Es besagt:

- Zwei beliebige beschränkte Teilmengen (des dreidimensionalen Raumes) mit nichtleerem Inneren sind durch Translationen und Rotationen gleichzerlegbar.

  Dies wird normalerweise dadurch illustriert, dass eine Erbse in endlich viele Stücke aufgeteilt und zu einem Objekt von der Größe der Erde wieder zusammengesetzt werden kann.

  Das einfachste Zerteilungsparadoxon wurde zuerst von Hausdorff entdeckt:

- Das Einheitsintervall kann in abzählbar viele Stücke zerteilt werden, die durch Translation zu einem Intervall der Länge 2 zusammengesetzt werden können.

  Dieses Resultat ist heutzutage trivial und ist das Standardbeispiel einer nicht-messbaren Menge, wie es in einführenden Vorlesungen in die Maßtheorie gelehrt wird.

  Theorem 6 (Foreman und Dougherty)

- Es gibt eine endliche Familie von disjunkten offenen Mengen im Einheitswürfel des $\mathbb{R}^3$, welche durch Isometrien in eine Familie von disjunkten offenen Mengen überführt werden können, die dicht in einem Würfel der Größe 2 (in $\mathbb{R}^3$) sind.

- Ein Quadrat kann **nicht** in einen Kreis umgewandelt werden. wenn man lediglich endlich viele Stücke mit glatten Rändern zuläßt.

- Hingegen kann ein Quadrat allein mit Translationen in einen Kreis umgeformt werden, wenn es erlaubt ist, endlich viele Stücke beliebiger Form (nicht notwendigerweise zusammenhängend) und disjunktes Zusammensetzen zu benutzen.

Referenzen

Boltyanskii. Equivalent and equidecomposable figures. in Topics in Mathematics published by D.C. HEATH AND CO., Boston.

Dubins, Hirsch and ? Scissor Congruence American Mathematical Monthly.

„Banach and Tarski had hoped that the physical absurdity of this theorem would encourage mathematicians to discard AC. They were dismayed when the response of the math community was 'Isn't AC great? How else could we get such counterintuitive results?' “

9.3 Die Kontinuumshypothese

Eine Standardreferenz hierzu ist Gödel's „What is Cantors Continuum Problem?“ von 1947 mit einer Ergänzung von 1963, neu erschienen in Benacerraf's und Putnams Sammlung „Philosophy of Mathematics“. Hierin umreißt Gödel seine allgemein ablehnende Haltung zur Kontinuumshypothese (CH), indem er einige nicht plausible Konsequenzen von CH aufzeigt.

‘I believe that adding up all that has been said one has good reason to suspect that the role of the continuum problem in set theory will be to lead to the discovery of new axioms which will make it possible to disprove Cantors conjecture.’

In einem Stadium glaubte er einen Beweis gefunden zu haben, dass $\mathbb{C} = \aleph_2$ aus einigen neuen Axiomen folgt, dies stellte sich aber als falsch heraus (vgl. Ellentuck, Godels Square Axioms for the Continuum, Mathematische Annalen 1975).

Maddys Believing the Axioms, Journal of Symbolic Logic 1988 (in 2 Teilen) ist ein sehr interessanter, amüsant zu lesender Artikel. Als Bonus gibt er allen Nicht-Mengentheoretikern, die die Grundlagen kennen, einen guten Einblick in viele Felder der gegenwärtigen Mengenlehre.

Der erste Teil ist überwiegend „plausiblen Argumenten“ für oder gegen CH gewidmet: wie sich die Kontinuumshypothese einerseits zu anderen möglichen Axiomen, andererseits zu einigen „Faustregeln“ der Mengenlehre verhält. Man bekommt dabei den Eindruck, dass das Gewicht der Argumente gegen die CH größer ist, obwohl Maddy schreibt, dass viele „jüngere“ Mengentheoretiker stärker mit CH sympathisieren als die Älteren. Allerdings wollen wir an dieser Stelle nicht zu sehr ins Detail gehen.

Einige Highlights aus Maddy's Diskussion sowie einiges, was andere mir geschickt haben:

1. Cantors Gründe an CH zu glauben sind heute nicht mehr besonders überzeugend.

2. Gödels Beweis der Konsistenz von CH zeigt, dass CH aus ZFC zusammen mit dem Axiom der Konstruierbarkeit ($V = L$, d.h. grob, dass das mengentheoretische Universum gleich dem konstruierbaren Universum ist) folgt. Jedoch halten viele Mengentheoretiker Konstruierbarkeit für nicht plausibel und viel zu einschränkend. Konstruierbarkeit ist ein Beispiel eines Minimierungsprinzips, welches dazu neigt, die Zahl der Mengen, die zu einem Universum gehören, zu verkleinern. Scheinbar werden Maximierungsprinzipien von Mengentheoretikern mit größerer Sympathie bedacht. Solche Prinzipien sind allerdings eher mit $\neg$CH als mit CH verträglich.

3. Wenn die Verallgemeinerte Kontinuumshypothese (GCH) wahr ist, dann impliziert das, dass $\aleph_0$ einige einzigartige Eigenschaften besitzt: z.B. dass es die Kardinalzahl ist, vor der GCH falsch ist und nach der GCH wahr ist. Einige würden gerne glauben, dass das mengentheoretische Universum gleichförmiger (homogener) ist, ohne diese Art singulärer Besonderheiten. Solche „Gleichförmigkeitsprinzipien" tendieren dazu, $\neg$GCH zu implizieren.

4. Die meisten derjenigen, die CH für falsch halten, glauben, dass das Kontinuum eine sehr große Kardinalität besitzt, viel mehr als $\aleph_2$ (wie Gödel scheinbar vorgeschlagen hat). Selbst Cohen, ein Formalist, argumentiert, dass die Potenzmengenoperation eine derart starke Operation ist, dass sie zu Mengen führen sollte, die weit größer sind als diejenigen, die rasch durch Fortschreiten in den Ordinalzahlen erreicht werden können:

   > This point of view regards C as an incredibly rich set given to us by a bold new axiom, which can never be approached by any piecemeal process of construction.

5. Es gibt auch ein paar Argumente für CH, z.B. dass $\neg$CH restriktiv (im Sinne von (2) oben) ist. Außerdem ist CH viel einfacher zu erzwingen (Cohen's Methode) als $\neg$CH. Und CH erlaubt viele herausragende Resultate zu erhalten, während $\neg$CH sich diesen Resultaten gegenüber eher neutral verhält.

6. Die meisten Axiome über große Kardinalzahlen (diese sichern die Existenz von Kardinalzahlen mit verschiedenen Eigenschaften von „Größe" zu; abgeleitet entweder von der Größe von $\aleph_0$ im Vergleich zu endlichen Kardinalzahlen unter Anwendung des Uniformitätsprinzips, oder von der Größe von V (des mengentheoretischen Universums) in Relation zu allen Mengen und Anwendung von „Reflektion") scheinen das Thema CH nicht zu entscheiden.

7. Verschiedene andere Axiome haben gewisse Bedeutung. Axiome zum Determinismus beschränken die Klasse von reellen Mengen, die Gegenbeispiele zu CH sein könnten. Axiome (z.B. Martin's Axiom), die Maximalitätsprinzipien (im Sinne von (2) oben) sind, implizieren $\neg$CH. Das stärkste (Martin's Maximum) impliziert, dass $\mathbb{C} = \aleph_2$ ist. Selbstverständlich gibt es auch Kontroversen über all diese Axiome.

8. Freiling's Prinzip, „Dartpfeile auf die reelle Achse zu werfen", scheint ein sehr plausibles Prinzip zu sein, das große Kardinalzahlen überhaupt

nicht bemüht. Aus ihm folgt sofort $\neg$CH. Freiling's Artikel (JSL 1986) ist eine gute Lektüre. Mehr dazu weiter unten.

Selbstverständlich haben wir es auffallend vermieden darüber zu sprechen, ob es ünerhaupt vernünftig wäre anzunehmen, dass CH einen bestimmten Wahrheitswert hat. Formalisten würden argumentieren, dass wir uns den Wahrheitswert aussuchen können, abhängig vom System, in dem wir arbeiten. Andererseits sollte uns die bloße Tatsache der Unabhängigkeit von ZFC nicht zu dieser Schlussfolgerung verleiten. Dies würde ZFC nämlich einen priviligierten Status verleihen, den es nicht notwendigerweise besitzt. In der Tat weist Maddy darauf hin, dass verschiedene Axiome (wie AC oder das Ersetzungsaxiom) ZFC aus äußerlichen Gründen (z.B. „Nützlichkeit“) ebenso hinzugefügt wurden wie aus immanenten Gründen (z.B. „Intuitivität“). Es ist gut möglich, dass aus den gleichen Gründen weitere Axiome, die vielleicht auch das Thema CH entscheiden könnten, hinzugefügt werden.

Ein korrespondierender Mengentheoretiker sagte, dass Mengentheoretiker selber sehr abgeneigt seien, über Wahrheit oder Falschheit solcher Behauptungen zu reden. (Sie sind bereit zu folgern, dass 2+2=4 wahr ist, aber sobald man nicht mehr über ganze Zahlen redet, wird es problematisch. Z.B. zögern die meisten sogar, zu behaupten, dass die Riemannsche Vermutung notwendigerweise einen bestimmten Wahrheitswert besitzt). Allerdings schienen die Zeitgenossen Maddy's, die in ihrem Paper diskutiert werden, durchaus gerne über Wahrheit oder Falschheit von CH zu spekulieren.

Die ganzen Zahlen sind nicht nur eine Grundlage, auch jede endliche Zahl von Potenzmengen scheint intuitiv natürlich zu sein. Dies würde darauf hinweisen, dass CH auf die eine oder andere Weise bestimmt wäre ... Wie ein Korrespondent vorschlug, ist die Frage nach der Bestimmtheit von CH der wohl beste Weg, Platonisten und Formalisten zu unterscheiden.

Und ist sie nun wahr oder falsch? Nun gut, CH ist einigermaßen intuitiv plausibel. Aber nach dem Lesen all dieser Fakten scheint es so, als würde das Gewicht der Beweise eher gegen CH tendierren.

Das Folgende ist von Bill Allen über Freilings Symmetrieaxiom. Es ist ein guter Startpunkt zum Testen der eigenen Intuition ...

> Let A be the set of functions mapping Real Numbers into countable sets of Real Numbers. Given a function f in A, and some arbitrary real numbers x and y, we see that x is in $f(y)$ with probability 0, i.e. x is not in $f(y)$ with probability 1. Similarly, y is not in $f(x)$ with probability 1. Let AX be the axiom which states
>
> 'for every f in A, there exist x and y such that x is not in $f(y)$ and y is not in $f(x)$'

The intuitive justification for AX is that we can find the x and y by choosing them at random.

In ZFC, AX = not CH. proof: If CH holds, then well-order R as $r_0, r_1, ..., r_x, ...$ with $x < \aleph_1$. Define $f(r_x)$ as $\{r_y : y \geq x\}$. Then f is a function which witnesses the falsity of AX.

If CH fails, then let f be some member of A. Let Y be a subset of $\mathbb{R}$ of cardinality $\aleph_1$. Then Y is a proper subset. Let X be the union of all the sets $f(y)$ with y in Y , together with Y . Then, as X is an $\aleph_1$ union of countable sets, together with a single $\aleph_1$ size set Y , the cardinality of X is also $\aleph_1$, so X is not all of $\mathbb{R}$. Let a be in $\mathbb{R}$ X, so that a is not in $f(y)$ for any y in Y . Since $f(a)$ is countable, there has to be some b in Y such that b is not in $f(a)$. Thus we have shown that there must exist a and b such that a is not in $f(b)$ and b is not in $f(a)$. So AX holds.

Freilings Beweis benutzt keine großen Kardinalzahlen oder schwierige Kombinatorik im Unendlichen um herauszuarbeiten, dass die CH unintuitive Ergebnisse impliziert. Freiling hat auch darauf hingewiesen, dass die natürliche Erweiterung von AX das Axiom AXL (meine Notation) ist, wobei in AXL das Auftreten der Abzählbarkeit durch Lebesguemaß 0 ersetzt wird. Unter Verwendung von AXL hat Freiling einige interessante, Fubini-ähnliche Sätze gezeigt.

Vgl. „Axioms of Symmetry: Throwing Darts at the Real Line“ von Freiling, Journal of Symbolic Logic, 51, Seiten 190-200. Eine Erweiterung dieses Artikels erschien in „Some properties of large filters“ von Freiling und Payne im JSL, LIII, Seiten 1027-1035.

Dieser Abschnitt basiert auf einem Posting von David Chalmers von der Indiana University.

Vgl. auch Nancy McGoughs *Continuum Hypothesis article* oder die *Kopie*:

`http://www.jazzie.com/ii/math/ch/`
`http://www.best.com/~ii/math/ch/`

Kapitel 10

Formeln von allgemeinen Interesse

10.1 Wie kann man den Wochentag zu einem Datum ermitteln?

Zunächst eine kurze Einführung: Im Gregorianischen Kalender gibt es über eine Periode von 400 Jahren 97 Schaltjahre und 303 normale Jahre. In jedem normalen Jahr verschiebt sich der 1. Januar um einen Wochentag, in jedem Schaltjahr um 2.

$$303 + 2 \cdot 97 = 497 = 7 * 71$$

Also folgt, dass der 1. Januar im Jahr N der gleiche Wochentag ist wie der 1. Januar im Jahr $N + 400$. Wegen der Schaltjahre wiederholt sich das Muster im 400-Jahre-Zyklus. Eine einfache Tabelle mit 400 Einträgen und eine einfach modulo-Operation ermöglichen es, den Wochentag (im Gregorianischen Kalender) zu bestimmen, und dies wesentlich schneller als andere Algorithmen. Außerdem benötigt jeder Eintrag nur 3 Bit, damit braucht die ganze Tabelle nur 1.200 Bit; auf vielen Computern wird dies weniger sein als die Anweisung, die zur Berechnung all der anderen komplizierteren Algorithmen benötigt werden.

Ein kleiner Einschub: Weil 7 nicht 400 teilt, fällt der 1. Januar auf bestimmte Wochentage häufiger als auf andere. Verblüffen Sie ihre Freunde! In einem Zyklus von 400 Jahren treten folgende Verteilungen für den 1. Januar und den 1. März auf:

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Jan 1:	58	56	58	57	57	58	56
Mar 1:	58	56	58	56	58	57	57

Zudem ist von Interesse, dass (entgegen den meisten ersten Schätzungen) das Auftreten nicht maximal gleichverteilt ist. In der Mathematical Gazette, vol. 53, pp.127-129, wurde gezeigt, dass der 13. eines Monats häufiger auf einen Freitag als auf jeden anderen Wochentag fällt. Der Autor war der damals 13jährige S. R. Baxter.

Der Gregorianische Kalender wurde 1582 in Europa eingeführt und 1752 in Großbritanien und seinen Kolonien übernommen, und zu anderen Zeitpunkten verschiedenen Ländern der Welt. Er ersetzte den Julianischen Kalender, der einen vierjährigen Schaltjahreszyklus hat; nach vier Jahren liegt der 1. Januar fünf Tage früher. Da 5 und 7 teilerfremd sind, ist eine Tabelle von 4*7=28 Elementen für den Julianischen Kalendar notwendig.

Trotzdem gibt es einen Fehler von 3 Tagen in 10.000 Jahren, den der Gregorianische Kalender nicht berücksichtigt. Irgendwann wird eine geeignete Korrektur durchgeführt werden müssen, aber Ihre Software wird dann sehr wahrscheinlich nicht mehr benutzt werden.

Hier ist eine Standardmethode für Berechnungen im Kopf:

1. Nehme die letzten beiden Ziffern.
2. Teile durch 4, ignoriere einen etwaigen Rest.
3. Addiere den Tag des Monats.
4. Addiere den Schlüsselwert des Monats: JFM AMJ JAS OND 144 025 036 146.
5. Ziehe 1 für den Januar oder Februar eines Schaltjahres ab.
6. Für Gregorianische Daten addiere 0 für 1900's, 6 für 2000's, 4 für 1700's, 2 für 1800's; für andere Jahrhunderte addiere oder subtrahiere Vielfache von 400.
7. Für Julianische Daten addiere 1 für 1700's und 1 für jedes zusätzliche Jahrhundet, das man zurückgeht.
8. Addiere die letzten beiden Ziffern.
9. Teile durch 7 und nimm den Rest.

1 ist nun Sonntag, 2 Montag, usw.

Die folgende, nur für den Gregorianischen Kalender geeignete Formel mag bequemer zu programmieren sein. Man beachte, dass in einigen Programmiersprachen die Restoperation mit negativem Operanden ein negatives Ergebnis liefern kann, also ist mod 7 nicht unbedingt der richtige Rest.

$$W = (k + \lfloor 2.6m - 0.2 \rfloor - 2C + Y + \lfloor Y/4 \rfloor + \lfloor C/4 \rfloor) \mod 7$$

wobei $\lfloor\cdot\rfloor$ die ganzzahlige floor-Funktion bezeichnet,
k ist der Tag (1 bis 31),
m ist der Monat (1 = März, ..., 10 = Dezember, 11 = Jan, 12 = Feb), Januar & Februar gelten dabei als Monate des vorangegangenen Jahres
C ist die Jahrhundertzahl[1] (zu 1987 wäre $C = 19$)
Y ist die Jahreszahl (zu 1987 wäre $Y = 87$, wobei $Y = 86$ für Jan & Feb)
W ist der Wochentag (0 = Sonntag, ..., 6 = Samstag)

Hier sind die 100- und 400-Jahr-Korrekturen schon in die Formel integriert. Der Term $2.6m - 0.2$ steht in Zusammenhang mit dem Muster, dass die Monate mit 30 Tagen aufweisen, wenn man den März als ersten Monat nimmt.

Das folgende kurze `C`-Programm liefert für einen eingeschränkten Bereich die richtigen Ergebnisse; es gibt 0 für Montag, 1 für Dienstag usw. zurück.

```
dow(m,d,y){y-=m<3;return(y+y/4-y/100+y/400+"-bed=pen+mad."[m]+d)%7;}
```

Das Programm wurde ursprünglich von `sakamoto@sm.sony.co.jp (Tomohiko Sakamoto)` am 10. März 1993 in `comp.lang.c` gepostet.

Eine leicht zu merkende Regel um den Wochentag zu berechnen ist folgende. In jedem Jahr fallen die folgenden Tage auf den gleichen Wochentag:

4.4.
6.6.
8.8.
10.10.
12.12.

Um sich nun die nächsten vier zu merken, erinnere man sich daran, dass ich von 9-5 an einer 7-11 arbeite, also

9.5.
5.9.
7.11.
11.7.

und der letzte Tag im Februar.

„1995 fielen sie auf einen Dienstag. Dies schreitet jedes Jahr um einen Wochentag fort, in Schaltjahren sogar um zwei Wochentage. Darum wird 1996 der Wochentag Donnerstag sein, 1997 Freitag. Daher schreitet normalerweise

[1] Hier befindet sich im Original ein Fehler, da das zugehörige Jahrhundert hierbei jeweils $C + 1$ wäre.

alle vier Jahre der Wochentag um 5 vor. Es gibt eine kleine Korrektur für Jahrhunderte, da Jahrhunderte genau dann Schaltjahre sind, wenn sie durch 4 teilbar sind. Damit ist 2000 ein Schaltjahr, 1900, 1800 und 1700 aber nicht“.

Auch wenn man die Form für eine Periode von Jahren ignoriert, ist dies dennoch nützlich, da man im allgemeinen den Wochentag zu einem gegebenen Datum schneller herausfinden kann, als wenn jemand dies in einem Kalender nachschlägt, der nicht gerade zur Hand ist. (Eine nützliche Fähigkeit.)

Referenzen

Winning Ways for your mathematical plays. Elwyn R. Berlekamp, John H. Conway, and Richard K. Guy London ; Toronto : Academic Press, 1982.
Mathematical Carnival. Martin Gardner. New York : Knopf, c1975.
Elementary Number Theory and its applications. Kenneth Rosen. Reading, Mass. ; Don Mills, Ont. : Addison-Wesley Pub. Co., c1993. p. 156.
Michael Keith and Tom Craver. The Ultimate Perpetual Calendar? Journal of Recreational Mathematics, 22:4, pp. 280-282, 19

10.2 Symbolische Programmpakete

Dies ist sicherlich keine vollständige Liste. Es gibt andere Computeralgebrapakete, die Ihren Ansprüchen besser genügen mögen. Eine Liste erhältlicher Pakete wird von der UC Berkeley betreut. (Diese Liste kann unter math.berkeley.edu via anonymous ftp abgerufen werden).

Das Symbolic Computation Network unter `http://symbolicnet.mcs.kent.edu` enthält viele weitere nützliche Informationen.

```
A: MaplePurpose: Symbolic and numeric computation, mathematical
          programming, and mathematical visualization.
        Contact: Waterloo Maple Software,
        450 Phillip Street
        Waterloo, Ontario
        N2L 5J2
        Phone (519)747-2373
        FAX    (519)747-5284
        email: info@maplesoft.on.ca


A: DOE-Macsyma
        Purpose: Symbolic and mathematical manipulations.
```

Contact: National Energy Software Center
Argonne National Laboratory 9700 South Cass Avenue
Argonne, Illinois 60439
Phone: (708) 972-7250

A: Pari Purpose: Number-theoretic computations and simple numerical analysis.
Available for most 32-bit machines, including 386+387 and 486.
This is a copyrighted but free package, available by ftp from math.ucla.edu (128.97.4.254) and ftp.inria.fr (128.93.1.26).
Contact: questions about pari can be sent to pari@math.u-bordeaux.fr and for the Macintosh versions to bernardi@mathp7.jussieu.fr

A: Mathematica
Purpose: Mathematical computation and visualization, symbolic programming.
Contact: Wolfram Research, Inc.
100 Trade Center Drive Champaign,
IL 61820-7237
Phone: 1-800-441-MATH

A: Macsyma
Purpose: Symbolic numerical and graphical mathematics.
Contact: Macsyma Inc.
20 Academy Street
Arlington, MA 02174
tel: 617-646-4550
fax: 617-646-3161
email: info-macsyma@macsyma.com

A: Matlab
Purpose: 'matrix laboratory' for tasks involving matrices, graphics and general numerical computation.
Contact: The MathWorks, Inc.
21 Prime Park Way
Natick, MA 01760
508-653-1415
info@mathworks.com

```
A: Cayley/Magma
        A: Cayley/Magma
        Cayley is no longer being licenced or supported.
        It has been superseded by a new and more powerful system
        called Magma.
        Purpose: Computation in algebraic, geometric and
        combinatorial structures such as groups, rings, fields,
        algebras, modules, graphs and codes.
        Available for: SUN 3, SUN 4, SUN 10 (SUNOS 4.x and Solaris 2)
        DECstation (Ultrix), DEC Alpha (OSF/1), IBM RS6000 (AIX),
        HP9000/700 (HP-UX), Apollo M680x0, SGI, 486/Pentium (MS-DOS).
        Contact: Computational Algebra Group
        School of Mathematics and Statistics
        University of Sydney
        NSW 2006
        Australia
        Phone: +61 2 351 3338
        Fax: +61 2 351 4534
        URL: http://www.maths.usyd.edu.au:8000/comp/magma/Overview.html
        magma@maths.su.oz.au

A: Axiom
        Purpose: Symbolic programming, symbolic and numeric computation,
                 mathematical visualisation.
        Contact: The Numerical Algorithms Group Ltd
        Wilkinson House
        Jordan Hill Road
        Oxford
        OX2 8DR
        UK
        email: infodesk@nag.co.uk
        Phone: +44 1865 311744
        Fax:   +44 1865 311755
```

10.3 Formel für den Flächeninhalt der Oberfläche einer Sphäre im N-dimensionalen euklidischen Raum

Dieser Flächeninhalt ist gleich dem Volumen einer $N-1$-dimensionalen Sphäre, die der Rand der N-dimensionalen Sphäre ist.

Das Volumen einer Kugel ist die am einfachsten zu merkende Formel:

$$V = r^N \frac{\pi^{N/2}}{(N/2)!}$$

Das einzig schwierige dabei ist die Berechnung von $(N/2)!$. Die eigentliche Definition der Fakultät ist gegeben durch $x! = \Gamma(x+1)$, aber wenn Sie eine Formel wollen:

$$(1/2+n)! = \sqrt{\pi}\frac{(2n+2)!}{(n+1)!4^{n+1}}$$

Zur Berechnung der Oberfläche differenzieren wir einfach und erhalten

$$N \cdot \frac{\pi^{N/2}}{(N/2)!} \cdot r^{N-1}.$$

Es gibt auch einen raffinierten Weg diese Formel durch Gaußsche Integrale zu erhalten. Zunächst bemerken wir, dass das Integral über die reelle Achse von e^{-x^2} gleich $\sqrt{\pi}$ ist. Darum ist das Integral über den N-dimensionalen Raum von $e^{-x_1^2-x_2^2-\ldots-x_N^2}$ gleich $\sqrt{\pi}^N$. Wir gehen nun zu Polarkoordinaten über und erhalten das Integral von 0 bis unendlich von $Vr^{N-1}e^{-r^2}$, wobei V das Öberflächenvolumen der Sphäre ist. Wiederholte schrittweise Integration ergibt die gesuchte Formel.

Es ist möglich das Volumen einer Sphäre von den „first principles“ abzuleiten.

10.4 Formel zur Berechnung von Zinseszinsen

Hier ist eine Formel, die in Lotus 123, Excel, Wings und Dynaplan genutzt werden kann:

```
------- Input this data -------------------------------
principal amount = E9                            ( in dollars )
Amortization Period = d10                        ( in years ie 6 mon = .5 )
```

```
Payments / year = D11                              ( 12 = monthly, 52 = weekl
Published Interest rate = D12                      ( ie 9 % = 0.09 )
Times per year Int calculated = d13                ( CDN mortgage use 2
                                                 US mortgage use 12
                                                 all other loans use 12 )
----- Calculate the proper rate of interest -----------

e14 = Effective annual rate = EXP(D13*LN(1+(D12/D13)))-1
e15 = Interest rate per payment = (EXP(LN(E14+1)/(D10*D11))-1)*D10*D11

e17 = Payments = APMT(E9,E15/D11,D10*D11) ( both these functions are
                 = PMT (E9,E15/D11,D10*D11) ( identical,diff spreadsheet)
       APMT( principal amount,interest rate per period,# periods )
       ( this is a standard function on any true commercial spreadsheet)

       OR use the following if done using a calculator
    = Payments = P*I/[1-(I+1)^-T]
                 = E9*(E15/D11)/(1-((E15/D11) +1)**(-1*D10*D11))

Total interest cost = E17*D10*D11-E9

 -- Use these formulas if you wish to generate an amortization table --
 always add up to 'Payments (e17)'
 Interest per payment = current balance * ( E15 / D11 )
 Principal per payment = current balance - Interest per payment
 new current balance     = current balance - Principal per payment -
                             (extra payment)
  keep repeating until 'new current balance' = 0
```

Herleitung der Zinzeszinsformel

Angenommen Sie überweisen eine festgelegte Summe in regelmäßigen Abständen auf ein verzinstes Konto, sagen wir monatlich am Ende eines jeden Monats. Wieviel Geld wird dann am Ende des n-ten Monats auf dem Konto sein (nachdem Sie n Einzahlungen getätigt haben)?

Sei i die monatliche Zinsrate.
Sei x der Betrag, der monatlich eingezahlt wird.
Sei n die Gesamtzahl der Monate.
Sei $p[k]$ das Guthaben nach k Monaten.

Daraus ergibt sich die folgende rekusive Formel:

$$p[n] = x + ((1+i)p[n-1]) \tag{10.1}$$

Dies führt zu der Summe

$$p[n] = \sum_{k=0}^{n} x(1+i)^k$$

Ein Weg dies zu lösen ist mit $(1+i)$ zu multiplizieren und die Originalgleichung vom Ergebnis zu subtrahieren. Damit fallen alle Terme der Summe bis auf den letzten Term der multiplizierten Gleichung und den ersten der Originalgleichung weg:

$$i \cdot p[n] = x((1+i)^n - 1)$$

oder

$$p[n] = x((1+i)^n - 1)/i$$

Nun wollen wir annehmen, dass man p zu einem festen Zins i geliehen hat. Wiederum werden monatliche Zahlungen des Betrages x vereinbart. Es stellt sich heraus, dass dieses Problem identisch dazu ist eine Gesamtanleihe von p zu nutzen (d.h. alles ist am Ende eines Zeitraums fällig) und Zahlungen von x auf ein Sparkonto zu leisten. Am Ende des Zeitraums benutzt man das Guthaben auf dem Sparkonto um die Anleihe auszugleichen. Anleihe und Sparkonto müssen selbstverständlich den gleichen Zinssatz aufweisen. Was wir also wissen wollen ist: Welche monatliche Zahlung wird benötigt, damit das Guthaben auf dem Sparkonto nach n Zahlungen gleich der Anleihe (einschließlich der zu zahlenden Zinsen) ist?

Die Formel für die Anleihe am Ende des n-ten Monats ist

$$p[n] = p[0](1+i)^n$$

Setzen wir diesen Ausdruck nun mit dem Ausdruck für das Sparkonto von oben gleich, so erhalten wir:

$$p[0](1+i)^n = x((1+i)^n - 1)/i$$

oder nach x aufgelöst

$$x = p[0](1+i)^n i/((1+i)^n - 1)$$

Wenn nun $(1+i)^n$ groß genug ist (sagen wir größer als fünf), haben wir eine Approximation um n aus den Daten von x, p und i zu errechnen:

$$n \approx -\ln(\ln(x(ip)))/\ln(1+i)$$

Diese Approximation basiert auf der Approximation

$$\ln(y-1) \approx \ln(y) - 1/y$$

die innerhalb 2 ist.

Betrachten wir ein Beispiel. Ein Darlehen von \$100.000 mit einem Zinssatz von 1% monatlich sollte in 360 Monaten mit \$1028,61 pro Monat abbezahlt sein. Die Approximation liefert 358,9 Zahlungen.

Wenn dies eine 30 Jahres-Hypothek wäre und im Monat \$1028.61 zu zahlen sind und man dann den Effekt einer monatlichen Zahlung von \$1050 sehen möchte, so liefert die obige Approximation, dass man in in 303,5 Monaten (25 Jahren und 3,5 Monaten) alles abbezahlt hätte. Setzen wir nun 304 Monate für x in die Gleichung ein, so erhalten wir \$1051.04, also ist die Rechnung sehr gut. Allerdings funktioniert die Approximation nicht für sehr kleine Zinssätze oder eine kleine Anzahl von Zahlungen. Die Regel ist, zunächst einen ersten Eindruck von $(1+i)^n$ zu bekommen. Ist dies größer als 5, so wird die Approximation recht gut sein. In den obigen Beispielen ist $(1+i)^n$ ungefähr 36.

i aus n, x und p zu berechnen ist nicht so einfach. Wenn i kleiner als 5% pro Zahlungszeitraum ist, kann die folgende Näherungsgleichung genutzt werden:

$$i = -(1/n)\ln(1 - ip/x)$$

Es gibt keine direkt Lösung hierfür, aber man kann dieses Problem mit der Newton-Raphson-Approximation angehen. Man beginnt mit einer Vermutung $i[0]$, dann wendet man an:

$$i[k+1] = i[k] - \frac{x(1 - i[k]p/x)(ni[k] + \ln(1 - i[k]p/x))}{xn(1 - i[k]p/x) - p}$$

Hierbei muss man mit einem zu großen Wert für i starten, denn die Gleichung besitzt eine Lösung bei $i = 0$, die sicherlich nicht die gesuchte Lösung ist.

Beispiel: Sei die Anleihe für p = \$10.000, x =\$50 pro Woche für 5 Jahre (n = 260). Sei $i[0]$=20% pro Jahr oder $0,3846\%$ pro Woche. Da i ein Bruch sein muss und nicht eine Prozentangabe, ist $i[0] = 0,003846$. Anwendung von 10.1 liefert:

```
i[1] = 0.003077
i[2] = 0.002479
i[3] = 0.002185
i[4] = 0.002118
i[5] = 0.002115
```

Die Reihe beginnt hier offensichtlich zu konvergieren.

Um nun $i[5]$ als jährliche Prozentrate zu erhalten, müssen wir es mit 52 Wochen und 100% multiplizieren, also $i[5] = 10,997\%$. Setzen wir nun wieder $i[5]$ in die Gleichung für x ein, so ergibt sich $x = \$50.04$, also ist die Approximation recht gut.

Referenzen

The theory of interest. Stephen G. Kellison. Homewood, Ill., R. D. Irwin, 1970.

Kapitel 11

Referenzen, Allgemeine Bibliographie und Fachbücher

Die folgenden Bücher wurden von einigen Lesern empfohlen. Die Zahl in eckigen Klammern gibt die Zahl der Empfehlenden an.

- Algebra
  Lang, Serge. Algebra. 2nd ed. Addison-Wesley Pub. Co., 1984.[2]
  Halmos, Linear Algebra. [1]
  Birkhoff, McLane, Algebra.
  van der Waerden, Algebra.
  Atiyah & MacDonald, Introduction to Commutative Algebra.

- Komplexe Analysis
  Ahlfors, Lars Valerian. Complex analysis: an introduction to the theory of analytic functions of one complex variable. 3rd ed. New York; Toronto: McGraw-Hill, 1979. [2]
  Conway, John B. Functions of one complex variable [*by*] John B. Conway. [*NewYork*] Springer-Verlag New York, 1973. [1]
  Priestley, Introduction to complex analysis.

- Reelle und komplexe Analysis
  Titchmarsh. Theory of Functions
  Boas. Primer of Real Functions
  Polya & Szego. Problems & Theorems in Analysis
  Rudin, Walter. Principles of mathematical analysis. 3d ed. New York : McGraw-Hill, 1976. [2]
  Rudin, Walter. „Functional Analysis“

Royden, H. L. Real analysis. 3rd ed. New York, Macmillan ; London : Collier Macmillan, 1988. [1]
Hewitt, Edwin, 1920. Real and abstract analysis : a modern treatment of the theory of functions of a real variable. New York : Springer-Verlag, 1969. [2]
Dieudonne'. Foundations of Analysis
Courant & Hilbert. Mathematical Methods of Physics.

- Geometrie
  David Hilbert. Foundations of Geometry 2nd English edition, tr. by Leo Unger, publ. by Open Court, 1971. Neumann, Stoy & Thompson. Groups and Geometry [1]

- Zahlentheorie
  Hardy, Littlewood.
  Samuel, „Algebraic Theory of Numbers“
  Hardy & Wright

- Geschichte der Mathematik
  Morris Kline Mathematical Thought from Ancient to Modern Times

- Topologie
  Guillemin, Victor and Alan Pollack: Differential Topology. Spivak, Michael: A Comprehensive Introduction to Differential Geometry, Vol. I
  Morgan, Frank: Riemannian Geometry: A Beginner's Guide
  Milnor, „Topology from the Differentiable Viewpoint“
  R. Engelking. General Topology.
  Kuratowski. Topology.
  Copson. Metric Spaces.
  Greenberg, Martin and (?) Harper: Algebraic Topology: An Introduction.
  Kelly, General topology

- Calculus
  Hardy, Course of Pure Mathematics.[2]
  Landau. Differential & Integral Calculus.
  Courant & John. Introduction to Calculus & Analysis, vol.1.

Spivak. Calculus on Manifolds.

- Wahrscheinlichkeitstheorie
  Feller, Introduction to probability theory

- Statistik
  Silvey, Statistical inference

- Maßtheorie
  Weir, Integration and measure

- Allgemein
  Courant & Robins [2] What is Mathematics. Oxford University Press. 1969

Kapitel 12

Das Sci.Math FAQ Team

The sci.math FAQ, which was initally edited and compiled by Alex Lopez-Ortiz is now a distributed effort of scientists in over five countries. At this time, the FAQ contains sections maintained by Alex Lopez-Ortiz (alopez-o@barrow.uwaterloo.ca), Nancy McGough (nancym@ii.com), and Hans de Vreught (J.P.M.deVreught@cs.tudelft.nl). Several others sections are in the works, on the hands of other volunteers.

If you wish to collaborate, send mail to alopez-o@barrow.uwaterloo.ca.

12.1 Copyright Notice

Questions and Answers Edited and Compiled by:
Alex Lopez-Ortiz alopez-o@barrow.UWaterloo.ca
Department of Computer Science University of Waterloo
Waterloo, Ontario Canada