Alte und neue ungelöste Probleme aus der Zahlentheorie

Vortrag im didaktischen Seminar, Januar 2004

Dieter Wolke

1 Einleitung

Man kann die Attraktivität eines Forschungsgebietes daran messen, über wieviele ungelöste Probleme es verfügt. Ein Wissensbereich, in dem alle Fragen beantwortet sind, mag vom ästhetischen Standpunkt her ansprechend sein. Für einen jungen Forscher, der seine Kräfte an offenen Fragen erproben möchte, bietet es wenig an Herausforderung. So wie ein Mensch, der keine Pläne, keine unerfüllten Wünsche mehr hat, bedauert werden kann, ist auch ein Wissenschaftszweig ohne ungelöste Probleme ein Stück weit gestorben.

In der Mathematik wird man vor allem die ältesten Teile, Geometrie und Zahlentheorie, auf einen solchen Prüfstand stellen. Der heutige Vortrag gilt der Zahlentheorie und der Frage: Lebt sie noch oder sind ihre grossen Probleme überwiegend gelöst? **Gauß** pflegte zu sagen: Ein Narr kann mehr Fragen über Zahlen stellen als tausend weise Männer beantworten. Hat die zahlentheoretische Weisheit inzwischen so stark zugenommen, dass der Narr nichts mehr findet? **David Hilbert** hielt 1900 auf dem Welt–Mathematikerkongress in Paris seinen berühmten Vortrag über die nach seiner Einschätzung 23 wichtigsten Probleme der Mathematik. Darunter waren sechs, die zur Zahlentheorie gehören, drei davon mehr zum algebraischen Teil. Auf die drei weitgehend elementar formulierbaren werde ich hier unter anderem eingehen.

Die Lösung des großen **Fermat–Problems** durch **Andrew Wiles** kurz vor der Jahrtausendwende ging durch die Tagespresse, das letzte Wort zur **Catalan–Vermutung** durch **Preda Mihailescu** bald darauf ebenfalls.

Kann man daraus folgern, dass die Zahlentheorie weitgehend abgeschlossen und damit uninteressant geworden ist? Die Frage muss eindeutig mit Nein beantwortet werden. Es gibt noch viele ungelöste Fragen, zum Teil uralte, zum Teil erst in jüngster Zeit aufgestellte. Im Folgenden werde ich zuerst auf drei der Hilbertschen Problemkreise eingehen, und danach einige in die Jahre gekommene, sowie einige neue Fragen ansprechen.

2 Drei der Hilbertschen Probleme

2.1 Diophantische Gleichungen

Sei F ein Polynom in k Variablen mit ganzzahligen Koeffizienten. Als „**Diophantische Gleichung**“ oder Diophantisches Problem bezeichnet man die Frage nach den ganzzahligen Lösungen der Gleichung

$$F(x_1, \ldots, x_k) = 0.$$

Gibt es überhaupt Lösungen? Endlich oder unendlich viele? Wenn es welche gibt, wie kann man sie finden? Gehorchen sie eventuell einer einfachen Gesetzmäßigkeit? So konnte man schon in der Antike die „**pythagoräischen Tripel**“, d.h. die Lösungen der Gleichung

$$x^2 + y^2 = z^2$$

im Prinzip vollständig auflisten. Wesentlich schwieriger die **Fermat–Vermutung**: Für kein $n \in \mathbb{N},\ n \geq 3$ hat die Gleichung

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

Lösungen $x, y, z \in \mathbb{N}$. Man sieht leicht, dass es reicht, $n = 4$ und $n =$ ungerader Primzahl p zu untersuchen. Für $n = 4$ gab **Fermat** eine elementare Methode an. Für $p \geq 3$ ist es nützlich, algebraische Hilfsmittel bereitzustellen, insbesondere die von den p–ten Einheitswurzeln $\xi_p = \exp(2\pi i/p)$ erzeugten „Kreisteilungskörper“ $\mathbb{Q}_p = \mathbb{Q}(\xi_p)$ zu studieren. So war das Fermatsche Problem einer der Haupt–Anreger für die Entwicklung der algebraischen Zahlentheorie. Hilbert erwähnt die Fermat–Vermutung in der Vorrede zu seiner Problem–Sammlung, schildert seine Rolle als Motor der Entwicklung der algebraischen Zahlentheorie, vor allem durch **Dedekind, Kronecker** und **Kummer**, nimmt es aber nicht ausdrücklich in seine Liste auf. Seine Frage, die Nummer 10, ist wesentlich umfassender, und lautet

> *Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

Dass es ein solches Verfahren, etwa im Sinn einer Turing–Maschine, nicht geben kann, wurde um 1970 von **Martin Davis, Julia Robinson** und **Yuri Matiasewich** bewiesen. Zwar gibt es für spezielle Teilklassen, zumindest prinzipiell, solche Algorithmen, jedoch ist die gesamte Diophantische Theoric zu komplex, um mit einem einzigen Verfahren erledigt zu werden.

Insbesondere war das Fermat–Problem weiterhin eine gewaltige Herausforderung. Nachdem man mit den klassischen Methoden des neunzehnten Jahrhunderts, kombiniert mit schnellen Rechnern, die Exponenten bis 150 000 abhaken konnte, war zur vollen Lösung

ein großer methodischer Sprung nötig. **Andrew Wiles** hat sich damit einen Ehrenplatz im Olymp der Mathematik gesichert.

Ein weiteres namhaftes Problem konnte unlängst, überraschenderweise mit klassischen Methoden, gelöst werden. **Eugène Charles Catalan** (1814–1894) vermutete 1844, wie schon zahlreiche Mathematiker vorher, dass $8 = 2^3$ und $9 = 3^2 = 2^3 + 1$ die einzigen aufeinanderfolgenden echten Potenzen sind.

Mit Hilfe der Bakerschen Ergebnisse über Linearformen in Logarithmen algebraischer Zahlen konnte **Tijdeman** 1976 zeigen: Gilt $x^m - y^n = 1$ mit $x, y \in \mathbb{N}$; $m, n \geq 2$, dann ist $\max(x, y, m, n) < C$ mit einem numerisch angebbaren C. Ein möglicher Wert war $C = \exp\exp\exp\exp 730$ (Langevin, 1996). Etwas zu groß für das Durchrechnen der nur endlich vielen Lösungskandidaten. Nach **Mihailescu** ist das überflüssig.

Gibt es noch interessante, nicht restlos analysierte diophantische Gleichungen? Sehr wohl. Nur ein Beispiel. Für alle $n \leq 10^7$ weiß man, dass $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ in $x, y, z \in \mathbb{N}$ lösbar ist. $4/n$ als sehr kurzer ägytischer Bruch. Vermutlich gilt es immer. Falls es Ausnahmen gibt, sind diese sehr selten. Ein Beweis für alle n scheint weit entfernt zu sein.

2.2 Riemannsche Vermutung und Primzahlprobleme

Bernhard Riemann erkannte als erster die Bedeutung der Funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad (\text{Realteil von } s > 1)$$

für die Untersuchung der Verteilung der Primzahlen. Diese Funktion, **Riemannsche Zeta–Funktion** genannt, nimmt man ihr den einzigen Pol $1/(s-1)$, ist in die ganze Ebene holomorph fortsetzbar. Sie hat für $\operatorname{Re} s > 1$ keine Nullstelle. Riemann vermutete, dass sie sogar in der Halbebene $\operatorname{Re} s > 1/2$ nicht verschwindet. 1896 konnten **Jaques Hadamard** und **Charles de la Vallée–Poussin** zeigen, dass $\zeta(s)$ auf der Geraden $\operatorname{Re} s = 1$ und ein Stückchen links davon nicht verschwindet, und damit den lange vermuteten **Primzahlsatz**

$$\#\{p \leq x,\ p \text{ prim}\} \cdot (x/\ln x)^{-1} \to 1 \quad \text{für} \quad x \to \infty$$

beweisen. Angesichts dieser Erfolge sowie der sich stürmisch entwickelnden komplexen Funktionentheorie war es natürlich, dass Hilbert hoffnungsvoll auf diesen Problemkreis schaute.
In seiner Frage Nr. 8 sagt er unter anderem

> *Nach einer erschöpfenden Disskussion der Riemannschen Primzahlformel wird man vielleicht dereinst in die Lage kommen, an die strenge Beantwortung des Problems von Goldbach zu gehen, ob jede gerade Zahl als Summe zweier Primzahlen darstellbar ist, ferner an die bekannte Frage, ob es unendlich viele Primzahlpaare mit*

der Differenz 2 oder gar an das allgemeinere Problem, ob die lineare diophantische Gleichung

$$a\,x + b\,y + c = 0$$

mit gegebenen ganzzahligen paarweise teilerfremden Koeffizienten a, b, c stets in Primzahlen x, y lösbar ist.

Der grosse Erfolg ist bislang ausgeblieben. Man kennt zwar einige Milliarden „nichttriviale“ Nullstellen der Zeta–Funktion (die „trivialen“ liegen bei $-2, -4, \ldots$ und waren schon Riemann bekannt). Alle haben den Realteil $1/2$. Aber dies schließt Ausnahmen zur Riemannschen Vermutung weit draußen nicht aus. Man weiß seit 1937 dank **I.M. Vinogradow**, dass jede hinreichend große ungerade Zahl Summe dreier Primzahlen ist. Das binäre **Goldbach–Problem** – $2N = p_1 + p_2$ – ist offen. Auch unter Annahme der Riemannschen Vermutung oder einer ihrer Verallgemeinerungen ist es bislang nicht möglich, die Goldbach–Frage und ebenso wenig das **Primzahl–Zwillingsproblem** zu entscheiden.

Aus der Richtigkeit der Riemannschen Vermutung folgt eine sehr präzise Form des Primzahlsatzes

$$\big|\#\{p \le x,\ p\,\text{prim}\ \} - \operatorname{Li} x\big| \le C x^{1/2} \ln x \quad \big(C > 0,\ \operatorname{Li} x = \int_2^x dt (\ln t)^{-1}\big).$$

Für andere Primzahlprobleme wie etwa das Studium der Abstände zwischen den Primzahlen müßten darüber hinaus Aussagen über die Verteilung der Imaginärteile der Nullstellen zur Verfügung stehen.

Die Riemannsche Vermutung wird übereinstimmend als eine der ganz großen Herausforderungen an die Mathematiker(innen) angesehen. Ein Durchbruch ist nicht in Sicht. Hilbert, der bekanntlich nach 1910 intensiv im Bereich der Integralgleichungen und –Operatoren arbeitete, äußerte die Idee, die Frage nach den Nullstellen der Zeta–Funktion als Eigenwertproblem für einen noch zu findenden Operator umzuformulieren. **Hugh L. Montgomery** studierte um 1970 die Verteilung der Differenzen aufeinanderfolgender Zeta–Nullstellen und erfuhr von einem Physiker, dass diese an das Energiespektrum großer Atomkerne in der Quantentheorie erinnern. Zeta–Funktionen und Hamilton–Operator? Eventuell ein gemeinsamer Hintergrund? Man darf gespannt sein.

Neben den genannten Primzahlproblemen gibt es eine Fülle ungelöster Fragen zu den Primzahlen, zum Beispiel die von **Legendre**: Liegt zwischen n^2 und $(n+1)^2$ stets eine Primzahl? Man konnte kürzlich in der Presse lesen, dass dies jetzt gesichert sei. Der amerikanische Mathematiker Don Goldston hatte im Frühjahr in Oberwolfach, allerdings unter Vorbehalten, ein wesentlich stärkeres Ergebnis angekündigt. Die Fachwelt wartet noch auf die genaue Ausführung.

2.3 Algebraische und transzendente Zahlen

1882 war **Ferdinand Lindemann** in Freiburg mit dem Beweis der **Transzendenz der Zahl** π ein ganz großer Wurf gelungen. π also nicht Nullstelle eines Polynoms $f(x) = a_n x^n + \cdots + a_0$ mit ganzen Koeffizienten. Im Gegensatz beispielsweise zur Irrationalzahl $\sqrt[3]{2}$, die das Polynom $f(x) = x^3 - 2$ verschwinden lässt. Mit dem Beweis der Transzendenz von π war das antike Problem der Quadratur des Kreises gelöst: Es gibt keine Konstruktion mit Zirkel und Lineal, die in endlich vielen Schritten einen Kreis in ein flächengleiches Quadrat umwandelt. **Hilbert** selbst hat 1893 eine sehr eleganten Beweis zur Transzendenz von e und π veröffentlicht. Insofern ist es nicht überraschend, dass er in seinem 7. Problem unter anderem den Wunsch äussert:

> *Man weise nach, dass die Potenz α^β für eine algebraische Basis α und einen algebraisch irrationalen Exponenten, z.B. die Zahl $2^{\sqrt{2}}$ oder $e^\pi = i^{-2i}$, stets eine transzendente oder auch nur eine irrationale Zahl darstellt.*

Hilbert, ein ausgezeichneter Kenner der Materie, hielt dies Problem für außerordentlich schwierig. 1917 äußerte er in einer Vorlesung die Vermutung, dass

a) die Riemannsche Vermutung in absehbarer Zeit entschieden werde,

b) die Lösung des Fermatschen Problem einige der Anwesenden vielleicht gerade noch erleben könnten, während

c) die Transzendenz von $2^{\sqrt{2}}$ in unabsehbar weiter Ferne liege.

Mit b) hat er im Prinzip recht gehabt, während die Entwicklung zu a) und c) genau umgekehrt verlaufen ist.

Nach Vorarbeiten von **Carl Ludwig Siegel** konnten **Theodor Schneider** und **Alexander Osipovich Gelfond** 1934 unabhängig voneinander die Hilbertsche Frage vollständig lösen. Seien α und β algebraische komplexe Zahlen, $\alpha \notin \{0, 1\}$, $\beta \notin \mathbb{Q}$. Dann ist $\alpha^\beta = \exp(\beta \log \alpha)$ transzendent. Zum Beispiel $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$, e^π, $e^{\pi\sqrt{163}}$. Die ersten zehn Nachkomma–Stellen der letzten Zahl sind gleich Neun.

Das Gebiet der transzendenten Zahlen hat seitdem weitere große Erfolge erlebt, es enthält aber auch noch viele offene Fragen. 1978 konnte **Roger Apéry** zeigen, dass $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ irrational ist. Über den Charakter der Zahlen $\zeta(5), \zeta(7), \ldots$ ist bis heute nur wenig bekannt. Ebenso weiß man kaum etwas über die **Eulersche Konstante**

$$\gamma = \lim_{N\to\infty} \Big(\sum_{n\le N} \frac{1}{n} - \ln N \Big) = 0,5772\ldots$$

Oder: Wie steht es mit dem arithmetischen Charakter der Zahlen $e + \pi$, $e\pi$?

3 Einige ältere Probleme

3.1 Vollkommene Zahlen, Mersenne– und Fermatsche Primzahlen

Die alten Griechen nannten eine natürliche Zahl n **vollkommen**, wenn sie gleich der Summe ihrer echten natürlichen Teiler ist $n = \sum_{d|n, d<n} d$, **Euklid** zeigte, dass falls $2^m - 1$ eine Primzahl ist, $n = 2^{m-1}(2^m - 1)$ eine gerade vollkommene Zahl darstellt. **Euler** bewies, dass alle geraden vollkommenen Zahlen so aussehen. Nach **Mersenne** (1588–1648) kann nur für prime $m = p$ $M_p = 2^p - 1$ Primzahl sein. Die ersten geraden vollkommenen Zahlen sind somit $2^1(2^2 - 1) = 6$, $2^2(2^3 - 1) = 28$, $2^4(2^5 - 1) = 496, \ldots$. Bei der Primzahl $p = 11$ stößt man erstmals auf eine zusammengesetzte Mersenne–Zahl. Gibt es unendlich viele Mersennesche Primzahlen und damit vollkommene Zahlen? Ein zur Zeit völlig unangreifbares Problem. Was erscheint plausibel?

Schon Euler stellte fest: Ist p prim, $\equiv 3 \bmod 4$ (d.h. lässt bei Division durch 4 den Rest 3) und ist $2p + 1$ selbst Primzahl, dann ist M_p zusammengesetzt. Also vermutlich unendlich viele nicht prime M_p.

Was spricht für unendlich viele prime M_p? Nach dem Primzahlsatz gibt es für großes x etwa $\frac{\ln x}{\ln 2 \cdot \ln \ln x}$ Primzahlen p mit $M_p \leq x$. Andererseits braucht man im Mittel etwa $\ln x$ Lose mit Nummer $\leq x$, um einen Gewinn „Primzahl“ zu ziehen. Das sieht nicht gut aus. Zum Glück erfüllen die M_p einige zusätzliche Bedingungen, so dass viele „Nieten“ überhaupt nicht in Betracht kommen. Es spricht, verfolgt man dies genauer, einiges dafür, dass es unterhalb x etwa $\frac{e^\gamma}{\ln 2} \ln \ln x$ Mersennesche Primzahlen gibt. Einige Mersenne–Zahlen, von denen man weiß, dass sie prim sind, gehören zu den größten heute numerisch bekannten Primzahlen, zum Beispiel $M_{859\,433}$, eine 258 716–stellige Zahl.

Noch mühsamer ist der Umgang mit den **Fermatschen Zahlen** $F_n = 2^{2^n} + 1$. Fermat vermutete, dass sie für alle $n \in \mathbb{N}_0$ Primzahlen sind. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$. In Ordnung! **Euler** stellte fest, dass F_5 zusammengesetzt ist: $F_5 = 641 \cdot 6700417$. **Landry** zeigte 1880, man sagt nach etwa 9 Monaten harter Arbeit, dass

$$F_6 = 274\,177 \cdot 67\,280\,421\,310\,721$$

gilt. Bis heute kennt man keine weitere prime Fermat–Zahl. Alle F_n mit $5 \leq n \leq 22$ sind zusammengesetzt. Von vielen weiteren weiß man es ebenfalls, zum Beispiel von $F_{23\,471}$. Es spricht wegen des doppelt exponentiellen Wachstums der Fermat–Folge vieles dagegen, dass es unendlich viele Primzahlen von dieser Gestalt gibt. **Paul Erdös**, der große, 1996 gestorbene Zahlentheoretiker, hielt das Problem für extrem schwierig, und erwartete für die nächsten tausend Jahre keine abschließende Antwort. Von Interesse wäre es. Denn nach **Gauß** ist das regelmäßige n–Eck mit Zirkel und Lineal genau dann konstruierbar, wenn

a) $n = 2^k$ oder

b) $n = 2^k\ p_1 \dots p_s$,

wobei $p_1, \dots, p_s$ verschiedene Fermatsche Primzahlen sind.

Das dritte ungelöste Problem in diesem Bereich ist die Frage nach ungeraden **vollkommenen Zahlen**. Man kennt bislang keine und vermutet auch, dass es keine gibt. Wenn ja, dann müssen sie ziemlich groß sein. Mindestens 10^{50} und mindestens acht verschiedene Primfaktoren.

3.2 Primzahltests und Faktorisierungsverfahren

Der wohl wichtigste praktische Anwendungsbereich der Zahlentheorie ist die **Kryptografie**, das Ver– und Entschlüsseln von Nachrichten. Die Suche nach mit geringem Aufwand ausführbaren Verfahren, die eine Nachricht so entstellen, dass nur ein Eingeweihter, mit „Schlüsseln“ versehener Empfänger in der Lage ist, den Inhalt zu „entschlüsseln“ und damit zu verstehen. Die bekannteste Methode ist das **RSA–Verfahren**. Seine vermutliche und bislang durch die Praxis und Theorie nicht widerlegte Sicherheit beruht darauf, dass es relativ einfach ist einer vorgegebenen Zahl anzusehen, ob sie Primzahl ist, **Primzahltest**. Dass es andererseits ungleich aufwändiger ist, eine Zahl, von der man weiß, dass sie zusammengesetzt ist, in ihre Primfaktoren zu zerlegen, **Faktorisierung**. Wenn etwa eine 200–stellige Zahl Produkt zweier Primzahlen mit ungefähr gleich vielen Stellen ist, braucht man nach dem heutigen Wissenstand Jahrhunderte, um diese zwei Faktoren zu bestimmen.

Wann kann man einen Algorithmus als schnell bezeichnen? In der Komplexitätstheorie nennt man ihn **polynomial**, und das gilt übereinstimmend als gut, wenn er bei einer n–stelligen Zahl N in $\leq C_1 n^{C_2} \approx (\ln N)^{C_2}$ Schritten zum Ziel führt. Bei unseren Beispielen: Verlässlich über prim oder nicht prim Auskunft gibt bzw. einen nichttrivialen Teiler von N liefert.

Die Suche nach einem solchen Primzahltest konnte im letzten Jahr überraschend abgeschlossen werden. 1983 hatten **Adleman, Rumley** und **Pomerance** einen Test mit anspruchsvollem theoretischem Hintergrund und mit einer Laufzeit $\leq C_1 \ln N^{C_2 \ln\ln\ln N}$ konstruiert, der also das Ziel nur knapp verfehlte. Im letzten Jahr gaben die in diesem Forschungsbereich bislang kaum hervorgetretenen indischen Mathematiker **Agraval, Kayal** und **Saxena** einen überraschend einfach fundierten Test an, der eine Laufzeit $\leq C_1(\ln N)^{10,5}$ aufweist. Das Verfahren beruht auf folgendem, leicht einzusehenden Kriterium: Sei $N \geq 2$, $(a, N) = 1$. Man reduziere in den Polynomen $f_1(x) = (x + a)^N$ und $f_2(x) = x^N + a$ alle Koeffizienten modulo N. N ist Primzahl genau dann, wenn die so veränderten f_1 und f_2 übereinstimmen.

Für die Praxis taugt dies noch nicht, da ja etwa N Reduktionen nötig sind. Überraschenderweise kann der Aufwand auf $\leq C(\ln N)^{10,5}$ Schritte reduziert werden. Hiermit ist es möglich, zum Beispiel 1000–stellige Zahlen in Minutenschnelle, von Rechenfehlern abgesehen, verlässlich zu testen.

Viel weniger befriedigend ist die Situation beim Faktorisieren. Im Prinzip geht man immer noch vor wie **Fermat**. Es soll N zerlegt werden. Angenommen, man hat zwei natürliche a und b mit $N = a^2 - b^2 = (a+b)(a-b)$, dann steht dort eine Zerlegung. Eines der heute besten Verfahren, das **Number field sieve** von **Buhler, Lenstra** und **Pomerance** (1993), findet in der Regel – nicht zwingend für jedes N – nach $\leq C_1 \exp\big(C_2(\ln N)^{1/3}(\ln\ln N)^{2/3}\big)$ Schritten einen Faktor.

Eine vorgelegte Zahl d darauf zu testen, of sie ein Teiler von N ist, schafft man mit schwach polynomialen Aufwand. Sollte es also gelingen, das große Problem der Komplexitätstheorie **P = NP** ? positive zu beantworten, dann wüsste man, dass es einen polynomialen Teiler– Such–Algorithmus gibt. Aber das allgemeine Problem steht eventuell in entfernteren Sternen als das Faktorisierungsproblem.

4 Zwei jüngere Probleme

4.1 Das Collatz–Problem

Die Fragestellung, die in der Literatur unter zahlreichen anderen Namen (Ulam, Syracuse, Kakutani, Hasse,...) zu finden ist, wurde wahrscheinlich um 1930 erstmals durch Lothar **Collatz** (1910–1990), den namhaften Numeriker, betrachtet. Sei für $n \in \mathbb{N}$

$$T(n) = \begin{cases} n/2, & \text{falls } n \text{ gerade} \\ (3n+1)/2, & \text{falls } n \text{ ungerade.} \end{cases}$$

Wie sieht die Folge der „iterierten“ Werte $n, T(n);\ T^2(n) = T\big(T(n)\big), \ldots$ aus?
Einige Beispiele:

$$n = 3: \quad 3, 5, 8, 4, 2, 1.$$

So bald die Eins erreicht ist, bleibt man in der Zweierperiode $1, 2$.

$$n = 9: \quad 9, 14, 7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1.$$

Collatz vermutete, dass man für jedes n schließlich bei der Eins landet. Denkbar wären auch andere Perioden oder Divergenz gegen $+\infty$.

Bislang ist die Vermutung für alle $n \leq 224 \cdot 10^{50}$ bestätigt worden, wobei einige Zahlen sehr lange brauchen, bis sie schließlich bei $1, 2$ zur Ruhe kommen. So zum Beispiel 70 Schritte bei $n = 27$.

Trotz intensiven Bemühens steht eine Entscheidung noch aus. Ein paar Teil–Ergebnisse.
1. Falls es ein k gibt mit $T^k(n) < n$, wird das kleinste solche k als **Stoppzeit** $S(n)$ von n bezeichnet. Andernfalls spricht man von unendlicher Stoppzeit. Es ist leicht zu sehen, dass die Collatz–Vermutung stimmt, wenn alle $n > 1$ endliche Stoppzeit haben. **Terras** (1976) und **Everett** (1977) konnten zeigen, dass „fast alle“ n endliche Stoppzeit haben, d.h.

$$\lim_{N\to\infty} N^{-1}\#\big\{n \le N,\ S(n) = \infty\big\} = 0.$$

gilt.

2. Es ist noch nicht gelungen zu zeigen, dass „fast alle“ n die Collatz–Vermutung erfüllen. Nach **Crandall** (1978) weiß man, dass für ein $c > 0$ mindestens N^c der Zahlen $n \le N$ dies tun.

Man mag hier und bei vielen anderen elementar formulierbaren zahlentheoretischen Problemen einwenden, dass es sich nur um eine Spielerei mit einem gewissen Unterhaltungswert handelt. Möglich! Andererseits sind durch sehr spezielle Fragen immer wieder weitreichende Theorien angeregt worden. So wie in der Kriminalistik schon manchmal die Verhaftung eines kleinen Taschendiebes zur Zerschlagung einer bedeutenden Bande geführt hat, ist auch hier nicht auszuschließen, dass hinter dem Collatz–Problem ganz wesentliche Zusammenhänge auf ihre Entdeckung warten.

4.2 Die ABC–Vermutung

Zur Motivation muss etwas weiter ausgeholt werden. Es werde die Fermat–Gleichung

$$x^n + y^n = z^n \qquad (n \ge 3)$$

nicht für ganze Zahlen x, y, z, sondern für Polynome $x(t), y(t), z(t)$ über $\mathbb{C}$ betrachtet. Schon **Liouville** wusste, dass es außer dem trivialen Fall $x(t) = c_1 f(t)$, $y(t) = c_2 f(t)$, $z(t) = c_3 f(t)$, $c_1^n + c_2^n = c_3^n$ $(c_1, c_2, c_3 \in \mathbb{C})$ keine Lösung in Polynomen gibt. Dies kann mit etwas Aufwand verallgemeinert werden.

Seien $a(t)$, $b(t)$, $c(t)$ Polynome über $\mathbb{C}$, nicht alle konstant, ohne gemeinsame Nullstellen, und $a(t) + b(t) = c(t)$. Dann gilt

> Das Maximum der Grade von a, b, c ist $\le$ der Zahl der Nullstellen – jede einfach gezählt – von $a \cdot b \cdot c$.

Insbesondere: Wenn etwa a eine Nullstelle hoher Ordnung hat, dann muss $b \cdot c$ viele verschiedene Nullstellen besitzten.

Was für Polynome stimmt, gilt vielfach – richtig formuliert – auch für Zahlen. Wenn man „Linearfaktor von $a(t)$“ durch „Primteiler der Zahl a“ und „Grad von $a(t)$“ durch $|a|$

ersetzt, dann lautet die obige Aussage:

Seien $a, b, c \in \mathbb{N}$ paarweise teilerfremd mit $a + b = c$. Dann gilt

$$\max(a, b, c) \leq \prod_{p \text{ prim}, p/abc} p.$$

Wieder: Wenn zum Beispiel in a ein Primteiler in hoher Potenz auftritt, dann müssen b und c entsprechend viele Primteiler beisteuern.

In dieser Form stimmt die Aussage noch nicht, wie man mit Zahlenbeispielen belegen kann. Es spricht jedoch einiges dafür, dass eine abgeschwächte Form richtig ist. Nach **Masser** und **Oesterlé** (um 1990) kann man vermuten:

Seien $a, b, c \in \mathbb{N}$, paarweise teilerfremd, $a + b = c$. Dann gibt es zu jedem $\varepsilon > 0$ eine Konstante $K(\varepsilon)$, so dass

$$c \leq K(\varepsilon)\Big(\prod_{p|abc} p\Big)^{1+\varepsilon} \qquad \text{gilt.}$$

ABC–Vermutung

Die Richtigkeit dieser Vermutung hat zahlreiche Konsequenzen. Zum Beispiel bewirkt sie bei der verallgemeinerten Fermat–Gleichung

$$Ax^n + By^n = Cz^n, \qquad n \geq 3,$$

dass es zu jedem n – bei festgehaltenen A, B, C – nur endlich viele Lösungen geben kann. Ebenso bei anderen drei–termigen diophantischen Gleichungen. Aber auch zu den Nullstellen Zeta–ähnlicher Funktionen hat die ABC–Vermutung wichtige Konsequenzen.

Für einen Beweis der Vermutung gibt es bislang noch keinen vielversprechenden Ansatz.

5 Literaturangaben

1. Jeremy **Gray**. The Hilbert Challenge. 2000, Oxford University Press.

Benjamin H. **Yandell**. The Honors Class. Hilbert's problems and their solvers. 2003, Peters, Massachusetts.

Zwei Bücher, in denen Hilberts Probleme und ihre Entwicklung bis heute geschildert werden. Das erste bietet etwas mehr Mathematik, das zweite viel Biografisches zu den beteiligten Mathematikern(innen).

2. Richard K. **Guy**. Unsolved Problems in Number Theory. 1994, Springer Verlag.

Eine umfassende Sammlung elementar formulierter zahlentheoretischer Probleme mit Literaturangaben.

3. Paulo **Ribenboim**. The new Book of Prime Number Records. 1996, Springer Verlag.

Wladyslav **Narkievicz**. The Development of Prime Number Theory. 1991, Springer Verlag.

Zwei Standardwerke zu Problemen und Geschichte der Primzahltheorie mit umfassenden Literaturangaben. Vor allem das zweite ist mathematisch anspruchsvoll.

4. Otto **Forster**. Algorithmische Zahlentheorie. 1996, Viehweg–Verlag.

Eine Einführung in die elementare Zahlentheorie unter starker Berücksichtigung numerisch– algorithmischer Gesichtspunkte.