Mathematik–Online:
Beiträge zu berühmten, gelösten und ungelösten Problemen

Nummer 3 - September 2008

Die *abc*-Vermutung

von Rainer Dietmann

Eines der faszinierendsten und weitreichendsten ungelösten mathematischen Probleme stammt aus der Zahlentheorie, ist wie viele zahlentheoretische Fragen sehr einfach zu formulieren, im Gegensatz zu großen Klassikern wie beispielsweise der Frage nach unendlich vielen Primzahlzwillingen aber erst in der jüngeren Vergangenheit aufgekommen: In der heutigen Form stammt die *abc*-Vermutung von David Masser (1985) und nimmt folgende elementare, zunächst unscheinbar anmutende Form an.

abc-Vermutung Sei $\varepsilon > 0$. Dann gibt es ein $C(\varepsilon)$ mit folgender Eigenschaft: Sind a, b, c drei teilerfremde ganze Zahlen und ist $c = a + b$, dann gilt

$$\max\{|a|, |b|, |c|\} \leq C(\varepsilon) \left(\prod_{p \,|\, abc} p \right)^{1+\varepsilon},$$

wobei das Produkt über alle Primteiler p von a, b, c erstreckt ist. Es handelt sich also um eine Abschätzung der Terme in der linearen Diophantischen Gleichung $c = a + b$ gegen den *quadratfreien Kern* $P = \prod_{p \,|\, abc}$ mit einem Exponenten, der etwas größer als 1 ist. Der quadratfreie Kern erfaßt jeden Primfaktor nur einmal, und da mit (a, b, c) auch (ka, kb, kc) eine Lösung der linearen Gleichung ist, muß die Teilerfremdheit von a, b, c gefordert werden. Dies stellt eine Form von Normierung dar, in der Sprache der Geometrie wird die Gleichung also projektiv betrachtet. In der Tat stammt die *abc*- Vermutung auch aus dem Umfeld der sogenannten Arithmetischen Geometrie und ist in obiger Form das Kondensat früherer, speziellerer Vermutungen. Sind nun a, b, c Primzahlen, verifiziert man sofort, daß die Vermutung richtig ist. Aber was, wenn a, b, c aus vielen sehr kleinen Primfaktoren bestehen? Auf diesem Weg läßt sich zwar durch Konstruktion geeigneter a, b, c zeigen, daß die geforderte Abschätzung schneller wachsen muß als P, die damit vermutlich fast optimale obere Schranke $C(\varepsilon)P^{1+\varepsilon}$ zu beweisen scheint aber hoffnungslos schwierig zu sein. Zur Zeit ist noch nicht einmal bekannt, daß eine polynomiale Schranke in P existiert! Warum nun ist diese Vermutung von so großer Bedeutung geworden? Was spricht überhaupt für die Richtigkeit der *abc*-Vermutung? Ein einfaches Beispiel soll die enorme Kraft der *abc*-Vermutung demonstrieren: Wie von Wiles (1995) in seinem Beweis der Fermatschen Vermutung gezeigt wurde, hat die Diophantische Gleichung

$$X^n + Y^n = Z^n$$

für ganzzahliges $n \geq 3$ keine nichttriviale ganzzahlige Lösung (x, y, z), wobei die trivialen Lösungen diejenigen mit $xyz = 0$ sind. Nehmen wir an, die *abc*-Vermutung sei richtig, und sei (x, y, z) eine nichttriviale Lösung dieser Gleichung. Wir setzen $a = x^n$, $b = y^n$

und $c = z^n$. Dann gilt $c = a + b$, und da die Fermatgleichung homogen ist, dürfen wir annehmen, daß x, y, z und damit a, b, c teilerfremd sind. In obiger Notation gilt also

$$\max\{|x|^n, |y|^n, |z|^n\} \leq C(\varepsilon) P^{1+\varepsilon}.$$

Eine obere Abschätzung für P ist nicht schwer:

$$P = \prod_{p \mid abc} p = \prod_{p \mid x^n y^n z^n} p = \prod_{p \mid xyz} p \leq |xyz|.$$

Es folgt

$$|xyz|^n \leq \max\{|x|^n, |y|^n, |z|^n\}^3 \leq C(\varepsilon)^3 P^{3(1+\varepsilon)} \leq C(\varepsilon)^3 |xyz|^{3(1+\varepsilon)}.$$

Ist nun $n \geq 4$, so können wir $\varepsilon < \frac{1}{3}$ wählen. Dann ist die letzte Ungleichungskette nur noch für *endlich viele* n, x, y, z möglich, die Fermatgleichung hat für gegebenen Exponenten $n \geq 4$ also nur endlich viele nichttriviale Lösungen und für hinreichend großes n gar keine nichttrivialen Lösungen. Das ist zwar schwächer als Wiles Resultat, folgt aber ohne Mühe aus der *abc*-Vermutung, während Wiles Beweis extrem kompliziert ist und in vielen Teilen auf die spezielle Form der Gleichung zugeschnitten. Obige Methode hingegen ist sehr flexibel und sofort auf allgemeinere Gleichungen zum Beispiel der Form

$$aX^k + bY^l = cZ^m$$

anwendbar. Die erhaltenen Endlichkeitsaussagen erinnern an den berühmten Satz von Faltings (1983): Eine rationale Kurve vom Geschlecht größer als Eins hat nur endlich viele rationale Punkte. Damit war bereits vor Wiles klar, daß die Fermatgleichungen für festes $n \geq 3$ nur endlich viele Lösungen haben. Elkies (1991) hat nun gezeigt, daß aus der *abc*-Vermutung auch der Satz von Faltings folgt! (Das ist formallogisch trivial, gemeint ist: Unter Annahme der *abc*-Vermutung bekommt man einen relativ einfachen, schnellen Beweis des Satzes von Faltings). Die *abc*- Vermutung hat also im Bereich der Diophantischen Gleichungen eine zentrale Stellung, ähnlich wie die Riemannsche Vermutung bei Problemen mit Primzahlen. Dies hat auch dazu geführt, daß inzwischen viele Resultate "unter Annahme der *abc*-Vermutung" bekannt sind, so wie es viele Resultate "unter Annahme der Riemannschen Vermutung" gibt. Die *abc*-Vermutung hat inzwischen auch zu hochinteressanten Folgerungen außerhalb des engeren Kreises der Diophantischen Gleichungen geführt, etwa im Bereich der L-Reihen, die bei Primzahlfragen eine große Rolle spielen. Für diese L-Reihen, die man als Verallgemeinerung der Riemannschen Zetafunktion betrachten kann, gibt es eine verallgemeinerte Riemannsche Vermutung, derzufolge es im kritischen Streifen (Realteil zwischen 0 und 1) nur Nullstellen auf der kritischen Geraden Realteil $\frac{1}{2}$ gibt. Eine schwächere Vermutung besagt, daß es für reelle L-Reihen keine Nullstellen dicht bei der 1 gibt, sogenannte Siegelsche Nullstellen. Granville und Stark (2000) konnten nun zeigen, daß aus einer Verallgemeinerung der *abc*-Vermutung für eine große Klasse von reellen L-Reihen folgt, daß es keine Siegelschen Nullstellen gibt. Da die *abc*-Vermutung inzwischen zu derart weitreichenden Folgerungen geführt hat, stellt sich die Frage nach Argumenten für ihre Plausibilität, da ein Beweis im Moment in weiter Ferne scheint. Wie so oft in der Zahlentheorie läßt sich ein über den ganzen Zahlen extrem schweres Problem in ein analoges Problem in Funktionenkörpern übersetzen, das dann wesentlich einfacher ist. Im Falle der *abc*-Vermutung geht das so: Wir betrachten den Ring $\mathbf{C}[X]$ komplexer Polynome, der viele Eigenschaften wie die Existenz eines Euklidschen Algorithmus und damit eindeutige Primfaktorzerlegung mit den ganzen Zahlen teilt. Das Analogon zum Betrag ist der Grad, und das Analogon zur *abc*-Vermutung ist folgender Satz, der trotz seiner elementaren Natur überraschenderweise erst 1984 von Mason entdeckt wurde:

Seien $a, b, c \in \mathbf{C}[X]$ teilerfremd mit $c = a + b$. Dann gilt

$$\max\{\deg a, \deg b, \deg c\} \leq n(abc) - 1,$$

wobei $n(f)$ die Anzahl *verschiedener* Nullstellen eines Polynoms f bezeiche.

Die Größe n entspricht also dem quadratfreien Kern, und so wie der quadratfreie Kern einer großen Zahl durchaus klein sein kann, kann $n(f)$ klein sein, obwohl f großen Grad hat. Der Beweis von Masons Satz ist überraschend einfach: Ist eines der Polynome konstant, so ist die Behauptung leicht einzusehen, so daß wir voraussetzen können, daß a, b, c alle mindestens Grad 1 haben. Aus $c = a+b$ folgt nun $f+g = 1$ mit $f = a/c$ und $g = b/c$. Wir nutzen nun ein strukturelles Hilfsmittel aus, das für Polynome, aber nicht für ganze Zahlen zur Verfügung steht, nämlich die Ableitung (Derivation). Diese liefert $f' + g' = 0$, also

$$\frac{f'}{f} f + \frac{g'}{g} g = 0.$$

Es folgt

$$\frac{b}{a} = -\frac{f'/f}{g'/g}.$$

Seien

$$a(X) = \alpha \prod (X - \alpha_i)^{r_i}, b(X) = \beta \prod (X - \beta_j)^{s_j}, c(X) = \gamma \prod (X - \gamma_k)^{t_k}.$$

Die logarithmische Ableitung liefert dann

$$\frac{f'/f}{g'/g} = \frac{\sum \frac{r_i}{X-\alpha_i} - \sum \frac{t_k}{X-\gamma_k}}{\sum \frac{s_j}{X-\beta_j} - \sum \frac{t_k}{X-\gamma_k}}.$$

Nun ist

$$N = \prod (X - \alpha_i)^{r_i} \prod (X - \beta_j)^{s_j} \prod (X - \gamma_k)^{t_k}$$

ein gemeinsamer Nenner von f'/f und g'/g mit $n(N) = n(abc)$. Sowohl Nf'/f als auch Ng'/g sind damit Polynome vom Grad kleiner gleich $n(abc) - 1$. Wegen

$$\frac{b}{a} = -\frac{Nf'/f}{Ng'/g}$$

und Teilerfremdheit von a und b folgt damit $\deg a, \deg b \leq n(abc) - 1$ und wegen $c = a+b$ auch $\deg c \leq n(abc) - 1$, womit alles gezeigt ist.

Mit diesem Resultat läßt sich nun sofort ein elementarer Beweis der Fermatschen Vermutung für komplexe Polynome geben: Gelte

$$f^n + g^n = h^n$$

mit $f, g, h \in \mathbf{C}[X]$ und $n \geq 3$. Falls f, g, h alle konstant sein dürfen, gibt es sicherlich Lösungen, habe also mindestens eines der drei Polynome Grad mindestens 1. Wir nehmen zusätzlich an, daß alle drei Polynome Grad mindestens 1 haben (die anderen Fälle laufen analog). Dann folgt aus dem Satz von Mason

$$n \deg f = \deg f^n \leq \deg f + \deg g + \deg h - 1,$$

also durch analoge Betrachtung für g und h und Aufaddieren

$$n(\deg f + \deg g + \deg h) \leq 3(\deg f + \deg g + \deg h) - 3,$$

was für $n \geq 3$ ein Widerspruch ist. Dieser polynomiale Satz von Fermat war zwar schon seit langer Zeit bekannt, die früheren Beweise nutzten aber Methoden aus der Algebraischen Geometrie, während dieser Beweis völlig elementar ist. Die *abc*-Vermutung hingegen ist nach wie vor völlig offen und könnte wegen ihrer weitreichenden Konsequenzen eines der zentralen mathematischen Probleme für die kommenden Generationen darstellen.

Autor:
PD Dr. Rainer Dietmann
Institut für Algebra und Zahlentheorie
Universität Stuttgart, Pfaffenwaldring 57
D-70550 Stuttgart
E-Mail: Rainer.Dietmann@mathematik.uni-stuttgart.de