

Die abc-Vermutung

Autor(en): **Lang, Serge**

Objektyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **48 (1993)**

PDF erstellt am: **19.03.2021**

Persistenter Link: <http://doi.org/10.5169/seals-44627>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Die *abc*-Vermutung

Serge Lang

Serge Lang wurde 1927 in Paris geboren, wo er auch seine ersten Schuljahre absolvierte. Die weitere Ausbildung erhielt er dann allerdings in den Vereinigten Staaten, wo er das California Institute of Technology (Caltech) und die University of Princeton besuchte. Hier erhielt er das Doktorat in Mathematik im Jahre 1951. Nach Aufenthalt am Institute for Advanced Study in Princeton und an der University of Chicago war er von 1955 bis 1970 Professor an der Columbia University in New York. Gastprofessuren in Princeton und Harvard folgten, und 1972 wurde er Professor an der Yale University. Seine Interessen sind weitgespannt, aber sein Hauptinteresse gehörte immer der Mathematik, besonders der Zahlentheorie. Bis anhin hat er 34 Bücher und über 70 Forschungsartikel veröffentlicht.

Wir wollen mit einem Satz über Polynome beginnen. Wahrscheinlich glauben alle von Ihnen, alles über Polynome zu wissen; sicherlich meinten bis vor kurzem die meisten Mathematiker, ich selbst nicht ausgeschlossen, dass man alles über Polynome wisse. Es war deshalb eine grosse Überraschung, als R.C. Mason 1983 einen neuen und sehr

Das berühmte Fermatsche Problem, die Frage also, ob die Gleichung $x^n + y^n = z^n$ für $n \geq 3$ im Ring der ganzen Zahlen eine Lösung besitzt, kennen wohl alle an Mathematik Interessierte. Aber wer hat schon über das analoge Problem für andere Ringe nachgedacht? Zum Beispiel: Gibt es komplexe Polynome $x(t)$, $y(t)$, $z(t)$, welche die Gleichung $x(t)^n + y(t)^n = z(t)^n$ erfüllen? Dies ist eine der Fragen, mit denen sich Serge Lang im vorliegenden Beitrag beschäftigt. Eine Reihe von neueren Entwicklungen, Vermutungen und Fragen, die sich um das Fermatsche Problem ranken, werden hier dargestellt. Im Zentrum steht dabei die seit einigen Jahren intensiv diskutierte *abc*-Vermutung.

Der Beitrag basiert auf einem Vortrag, der am 27. Mai 1992 vor einem allgemeineren Publikum an der ETH Zürich gehalten wurde. Wir haben ihn auf Band aufgenommen und ins Deutsche übertragen, und der Text wurde anschliessend von Serge Lang überarbeitet. Wo immer möglich haben wir versucht, die direkte, informelle Sprache des Vortrags beizubehalten. Aber Geschriebenes kann den Enthusiasmus von Serge Lang, seinen mitreissenden Vortragsstil und die lebhaft, mehrsprachige Interaktion mit dem Publikum nur unvollkommen wiedergeben. Wir hoffen, dass in diesem Beitrag trotzdem etwas davon durchschimmert. *ust*

interessanten Satz über Polynome entdeckte. Wir wollen zuerst diesen Satz formulieren und ihn beweisen, bevor wir uns den ganzen Zahlen und der *abc*-Vermutung zuwenden. Der Satz handelt von komplexen Polynomen. Wir schreiben die Elemente von $\mathbb{C}[t]$ in der Form

$$f(t) = c_1 \cdot \prod_{i=1}^r (t - \alpha_i)^{m_i} ,$$

wobei $\alpha_1, \alpha_2, \dots, \alpha_r$ die (paarweise verschiedenen) Nullstellen des Polynoms $f(t)$ bezeichnen. Der Grad von $f(t)$ ist dann gegeben durch $\text{grad } f = m_1 + m_2 + \dots + m_r$. Die Anzahl der (verschiedenen) Nullstellen des Polynoms f bezeichnen wir mit $n_0(f)$, also

$$n_0(f) = r .$$

Es ist offensichtlich, dass $\text{grad } f$ gross sein kann und gleichzeitig $n_0(f)$ klein. Zum Beispiel besitzt $f(t) = (t - \alpha)^{1000}$ den Grad 1000, aber es ist $n_0(f) = 1$. Für Polynome f, g gilt allgemein $n_0(f) + n_0(g) \geq n_0(f \cdot g)$, und wenn sie teilerfremd sind, gilt sogar Gleichheit:

$$n_0(f) + n_0(g) = n_0(f \cdot g) .$$

Der Satz von Mason [Ma 83, Ma 84] lautet wie folgt:

Satz. *Es seien $f, g, h \in \mathbb{C}[t]$ nichtkonstante, teilerfremde Polynome mit $f + g = h$. Dann gilt*

$$\max(\text{grad } f, \text{grad } g, \text{grad } h) \leq n_0(f \cdot g \cdot h) - 1 .$$

Der Satz besagt, dass die Relation $f + g = h$ den Grad der Polynome f, g, h beschränkt und zwar durch die Anzahl der verschiedenen Nullstellen der drei Polynome f, g, h .

Bevor wir den Beweis des Satzes angeben, wollen wir eine Anwendung besprechen. Sie vermittelt einen Eindruck davon, wie stark der Satz von Mason ist. Sie kennen wohl alle die Fermatsche Vermutung:

Für $n \geq 3$ gibt es keine von Null verschiedenen ganzen Zahlen x, y, z mit

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

Die analoge Aussage für komplexe Polynome wurde um die Jahrhundertwende mit Hilfe von Argumenten aus der algebraischen Geometrie bewiesen. Hier wollen wir dafür einen elementaren Beweis angeben, der vom Satz von Mason ausgeht.

Satz. *Für $n \geq 3$ gibt es keine nichtkonstanten, teilerfremden Polynome $x, y, z \in \mathbb{C}[t]$ mit*

$$x(t)^n + y(t)^n = z(t)^n .$$

Beweis: Wir setzen $f(t) = x(t)^n$, $g(t) = y(t)^n$, $h(t) = z(t)^n$. Dann liefert der Satz von Mason

$$\text{grad } x(t)^n \leq n_0(x(t)^n \cdot y(t)^n \cdot z(t)^n) - 1 .$$

Aber $\text{grad } x(t)^n = n \cdot \text{grad } x(t)$, und $n_0(x(t)^n) = n_0(x(t)) \leq \text{grad } x(t)$, so dass folgt

$$n \cdot \text{grad } x(t) \leq \text{grad } x(t) + \text{grad } y(t) + \text{grad } z(t) - 1 .$$

Auf analoge Weise erhalten wir für $y(t)$ und $z(t)$ die Ungleichungen

$$n \cdot \text{grad } y(t) \leq \text{grad } x(t) + \text{grad } y(t) + \text{grad } z(t) - 1 ,$$

$$n \cdot \text{grad } z(t) \leq \text{grad } x(t) + \text{grad } y(t) + \text{grad } z(t) - 1 .$$

Die Addition dieser drei Ungleichungen liefert

$$n \cdot (\text{grad } x(t) + \text{grad } y(t) + \text{grad } z(t)) \leq 3 \cdot (\text{grad } x(t) + \text{grad } y(t) + \text{grad } z(t)) - 3 .$$

Es folgt

$$(n - 3) \cdot (\text{grad } x(t) + \text{grad } y(t) + \text{grad } z(t)) \leq -3 ,$$

was für $n \geq 3$ offensichtlich ein Widerspruch ist. Damit ist der "Satz von Fermat für Polynome" bewiesen.

Der Beweis des Satzes von Fermat für Polynome ist ohne Kenntnis des Satzes von Mason recht schwierig. Es ist von vornherein nicht klar, wie man eine derartige Aufgabe überhaupt angehen würde. Sie können Ihren Freunden diese Frage als Herausforderung stellen und zusehen, wie lange diese für einen Beweis benötigen. Unser Beweis mit Hilfe des Satzes von Mason ist ganz kurz und einfach. Es existieren übrigens Verallgemeinerungen, auf die wir später zurückkommen werden.

Beweis des Satzes von Mason: In der Aussage des Satzes haben wir links den Grad und rechts n_0 , also die Anzahl der verschiedenen Wurzeln eines Polynoms. Wir müssen deshalb einen Weg finden, um die Vielfachheiten der Wurzeln in den Griff zu bekommen. Aus diesem Grunde dividieren wir die Gleichung $f + g = h$ durch h und erhalten

$$\frac{f}{h} + \frac{g}{h} = 1 .$$

Setzen wir $R = f/h$, $S = g/h$, so folgt $R + S = 1$, und die Ableitung nach t liefert $R' + S' = 0$. Diese Beziehung schreiben wir in der Form

$$\frac{R'}{R} + \frac{S'}{S} = 0 . \quad (1)$$

Wir betrachten nun den Quotienten g/f . Mit unseren Bezeichnungen und mit der Beziehung (1) lässt sich dieser durch

$$\frac{g}{f} = \frac{S}{R} = -\frac{R'/R}{S'/S} \quad (2)$$

ausdrücken. Wir haben also g/f als Quotient von logarithmischen Ableitungen $F \rightsquigarrow F'/F$ schreiben können. Es stellt sich heraus, dass wir das mehrfache Auftreten der Wurzeln damit unter Kontrolle gebracht haben. In der Tat hat – wie Sie wissen

– die logarithmische Ableitung die angenehme Eigenschaft, Produkte in Summen überzuführen:

$$\frac{(F \cdot G)'}{F \cdot G} = \frac{F'}{F} + \frac{G'}{G} .$$

Dies folgt direkt aus der Produktformel für die Ableitung. Dann gilt bekanntlich auch

$$\frac{(F/G)'}{F/G} = \frac{F'}{F} - \frac{G'}{G} .$$

Wenn wir unsere Polynome in der am Anfang angegebenen Form schreiben, also

$$f(t) = c_1 \cdot \prod (t - \alpha_i)^{m_i} ,$$

$$g(t) = c_2 \cdot \prod (t - \beta_j)^{n_j} ,$$

$$h(t) = c_3 \cdot \prod (t - \gamma_k)^{l_k} ,$$

so erhalten wir für die logarithmischen Ableitungen die folgenden einfachen Ausdrücke

$$\frac{f'}{f} = \sum \frac{m_i}{t - \alpha_i} , \quad \frac{g'}{g} = \sum \frac{n_j}{t - \beta_j} , \quad \frac{h'}{h} = \sum \frac{l_k}{t - \gamma_k} .$$

Mit $R = f/h$ und $S = g/h$ und indem wir die Regeln der logarithmischen Ableitung verwenden, erhalten wir aus (2)

$$\frac{g}{f} = -\frac{f'/f - h'/h}{g'/g - h'/h} = -\frac{\sum \frac{m_i}{t - \alpha_i} - \sum \frac{l_k}{t - \gamma_k}}{\sum \frac{n_j}{t - \beta_j} - \sum \frac{l_k}{t - \gamma_k}} . \quad (3)$$

Es sei nun $D(t)$ das Polynom

$$D(t) = \prod (t - \alpha_i) \cdot \prod (t - \beta_j) \cdot \prod (t - \gamma_k) .$$

Offensichtlich gilt $\text{grad } D(t) = n_0(f \cdot g \cdot h)$. Daraus folgt

$$\text{grad} \left(\frac{D(t)}{t - \alpha_i} \right) = n_0(f \cdot g \cdot h) - 1 = \text{grad} \left(\frac{D(t)}{t - \beta_j} \right) = \text{grad} \left(\frac{D(t)}{t - \gamma_k} \right) .$$

Erweitern wir den Bruch (3) mit $D(t)$, so erhalten wir

$$\frac{g}{f} = -\frac{\sum \frac{m_i}{t - \alpha_i} - \sum \frac{l_k}{t - \gamma_k}}{\sum \frac{n_j}{t - \beta_j} - \sum \frac{l_k}{t - \gamma_k}} \cdot \frac{D(t)}{D(t)} = \frac{\text{Polynom vom Grad} \leq n_0(f \cdot g \cdot h) - 1}{\text{Polynom vom Grad} \leq n_0(f \cdot g \cdot h) - 1} .$$

Damit ist g/f als Quotient von zwei Polynomen geschrieben, deren Grad höchstens $n_0(f \cdot g \cdot h) - 1$ ist. Da f und g teilerfremd sind, folgt daraus, dass auch die Grade der Polynome f und g höchstens $n_0(f \cdot g \cdot h) - 1$ sein können. Und schliesslich hat das Polynom h , als Summe $h = f + g$, ebenfalls höchstens diesen Grad. Damit ist der Satz von Mason bewiesen.

Es ist zweifellos eine ganz merkwürdige Tatsache, dass ein solch einfacher und doch starker Satz über Polynome erst im Jahre 1983 entdeckt worden ist.

Wir wollen nun diesen Satz in die ganzen Zahlen "übersetzen". Sie wissen natürlich, dass es eine tiefe Analogie zwischen ganzen Zahlen und Polynomen mit Körperkoeffizienten gibt; zum Beispiel besitzen beide Ringe einen Euklidischen Algorithmus, und damit gilt in beiden Ringen die eindeutige Primfaktorzerlegung. Wir suchen nun für die ganzen Zahlen etwas Entsprechendes zum Grad eines Polynoms und zur Grösse n_0 . Bei der Multiplikation von zwei Polynomen addieren sich die Grade dieser Polynome; dem Grad eines Polynoms entspricht also bei ganzen Zahlen der Logarithmus des Betrages. Bei der "Übersetzung" von n_0 hilft uns die folgende Bemerkung weiter. Für

$$f(t) = \prod (t - \alpha_i)^{m_i}$$

definieren wir $N_0(f(t)) = \prod (t - \alpha_i)$. Dann gilt

$$n_0(f) = \text{grad } N_0(f(t)) .$$

Was wird also für eine ganze Zahl m die "richtige" Definition für $n_0(m)$ sein? Nehmen wir an, m habe die Primfaktorzerlegung

$$m = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} . \quad (4)$$

Ein Student: Ich schlage vor, für $n_0(m)$ die Anzahl verschiedener Primfaktoren von m zu nehmen, also $n_0(m) = r$.

Serge Lang: Das ist keine schlechte Antwort, aber sie ist nicht ganz gut genug. Wenn wir komplexe Polynome betrachten, dann haben alle irreduziblen Faktoren den Grad eins. Aber über anderen Körpern können irreduzible Faktoren durchaus höheren Grad besitzen. Dem Grad bei Polynomen entsprechend muss deshalb im Ring der ganzen Zahlen die Primzahl p mit einem Gewicht versehen werden, nämlich $\log p$. Für die Zahl m mit Primfaktorzerlegung (4) ist also

$$n_0(m) = \sum_{i=1}^r \log p_i$$

zu setzen, was wir auch in der Form

$$n_0(m) = \sum_{p|m} \log p$$

schreiben können. Konsequenterweise definieren wir

$$N_0(m) = \prod_{p|m} p = \prod_{i=1}^r p_i .$$

Was ist also für ganze Zahlen die Aussage, die dem Satz von Mason entspricht? Es ist einfach, die Voraussetzungen zu übersetzen:

Es seien a, b, c von Null verschiedene teilerfremde ganze Zahlen mit $a + b = c$.

Dann wollen wir eine Ungleichung der Form

$$\max(|a|, |b|, |c|) \leq ? .$$

Was soll auf der rechten Seite der Ungleichung stehen?

Ein Student: Vielleicht $N_0(abc) - 1$?

Serge Lang: Es ist nicht ganz so einfach. Zuerst zu -1 : dies war im Falle der Polynome ein Geschenk der Götter, und wir wollen hier, bei den ganzen Zahlen davon absehen. Wir wollen einfach die etwas schwächere Ungleichung

$$\max(|a|, |b|, |c|) \leq N_0(abc)$$

betrachten. Leider ist aber die Aussage in dieser Form falsch. Sie bleibt sogar auch dann falsch, wenn auf der rechten Seite zusätzlich irgendeine noch so grosse multiplikative Konstante K zugelassen wird: es gibt keine Konstante K , so dass die Ungleichung

$$\max(|a|, |b|, |c|) \leq K \cdot N_0(abc)$$

für alle von Null verschiedenen, teilerfremden ganzen Zahlen a, b, c mit $a + b = c$ erfüllt ist! Dies zeigt das folgende Beispiel, das von zwei Studenten der Yale University stammt, Wojtek Jastrzebowski und Dan Spielman.

Wir betrachten die Gleichung $a_n + b_n = c_n$ mit $a_n = 3^{2^n}$, $b_n = -1$ und

$$c_n = 3^{2^n} - 1 .$$

Indem man $3 = 1 + 2$ schreibt, beweist man leicht mit Induktion nach n , dass 2^n die Zahl $3^{2^n} - 1$ teilt. Damit folgt

$$N_0(a_n b_n c_n) \leq 3 \cdot 2 \cdot \frac{c_n}{2^n} .$$

Die Ungleichung

$$3^{2^n} \leq K \cdot 3 \cdot 2 \cdot \frac{3^{2^n}}{2^n}$$

kann aber nicht für alle n erfüllt sein, gleichgültig, wie gross die Konstante K gewählt wird.

Wird die obige, als falsch erkannte Aussage etwas modifiziert, so spricht man von der *abc*-Vermutung. Sie ist eine der interessantesten zahlentheoretischen Vermutungen der neueren Zeit.

Die *abc*-Vermutung. (Masser, Oesterlé, 1986) *Zu $\epsilon > 0$ existiert eine Konstante $K(\epsilon)$, so dass für alle von Null verschiedenen, teilerfremden ganzen Zahlen a, b, c mit $a + b = c$ die Ungleichung*

$$\max(|a|, |b|, |c|) \leq K(\epsilon) \cdot (N_0(abc))^{1+\epsilon}$$

erfüllt ist.

Mit im wesentlichen dem selben Beweis wie oben für Polynome kann man zeigen, dass aus dieser Vermutung die (ganzzahlige) Fermatsche Vermutung für grosse Exponenten n folgt. Dazu können wir ohne Beschränkung der Allgemeinheit annehmen, dass a, b, c positive ganze Zahlen sind, so dass wir die Absolutbeträge nicht schreiben müssen. Wir nehmen dann an, dass wir positive, paarweise teilerfremde ganze Zahlen x, y, z haben, welche der Gleichung

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

genügen. Wir setzen $a = x^n$, $b = y^n$ und $c = z^n$. Dann gilt

$$N_0(x^n y^n z^n) = N_0(xyz) \leq xyz.$$

Aus der *abc*-Vermutung folgt

$$x^n << (xyz)^{1+\epsilon}, \quad y^n << (xyz)^{1+\epsilon}, \quad z^n << (xyz)^{1+\epsilon}, \quad (5)$$

wobei wir der Kürze halber das Zeichen $<<$ verwendet haben, um auszudrücken, dass es eine von ϵ abhängige Konstante $K(\epsilon)$ gibt, so dass die linke Seite kleiner oder gleich dem Produkt der rechten Seite mit $K(\epsilon)$ ist. Das Produkt der Ungleichungen (5) ergibt

$$(xyz)^n << (xyz)^{3+\epsilon},$$

weil wir in unserer Notation natürlich 3ϵ wieder durch ϵ ersetzen können. Logarithmieren wir, so folgt

$$(n - 3 - \epsilon) \cdot \log(xyz) \leq \log K$$

für eine gewisse Konstante $K = K(\epsilon)$. Wegen $xyz \geq 2$ liefert aber diese Ungleichung eine Schranke für n , so dass die Fermatsche Vermutung für alle genügend grossen ganzen Zahlen n bewiesen wäre.

Die Schranke für n hängt offensichtlich von der Konstanten $K(\epsilon)$ ab. Über deren Grösse bestehen bis heute keinerlei Vermutungen. Anzumerken bleibt auch, dass wir in der obigen Überlegung $\epsilon = 1$ hätten setzen können. Auf diese Weise hätten wir eine absolute, von ϵ unabhängige Schranke erhalten.

Ein Student: Hat man schon versucht, auf rechnerische Art Gegenbeispiele zur *abc*-Vermutung zu finden?

Serge Lang: Dies funktioniert nicht. Tabellen über die Primzahlzerlegung von Zahlen scheinen die Vermutung allerdings zu bestätigen. Beachten Sie, dass der in der Ungleichung vorkommende Exponent $1+\epsilon$ die Aussage sehr stark macht. Unter anderem besagt die *abc*-Vermutung folgendes: Wenn in den Primzahlfactorisierungen von a, b, c Primzahlen mit hohen Exponenten vorkommen, dann müssen diese Primzahlen durch viele kleine Primzahlen oder durch grosse Primzahlen, die nur mit Exponent eins vorkommen, kompensiert werden. Zum Beispiel hat man Tabellen für die Primzahlfactorisierung von $2^n \pm 1$ (und von ähnlichen Zahlen) berechnet [BLSTW]. Diese Tabellen zeigen klar, dass fast alle Primfaktoren nur mit Exponent eins vorkommen; treten kleine Primfaktoren mit grösseren Exponenten auf, so kommen regelmässig auch grosse Primfaktoren vor, deren Exponent eins ist.

Ein Student: Impliziert der “Grosse Satz von Fermat” die *abc*-Vermutung?

Serge Lang: Nein. Der Satz von Fermat ist einfach ein Spezialfall. Die *abc*-Vermutung ist viel stärker und gibt viel mehr Informationen über die Art und Weise, wie die Exponenten der Primzahlen beschränkt werden, die in der Factorisierung von *abc* auftreten. Um dies noch etwas klarer zu machen: Wir hätten, um den Satz von Fermat für grosse n zu beweisen, ohne weiteres den Exponenten $1+\epsilon$ durch einen *festen* Exponenten ersetzen können.

Ein Student: Wie wird man dazu geführt, eine solche Vermutung auszusprechen?

Serge Lang: Masser und Oesterlé haben die Vermutung nicht als plötzliche Eingebung gefunden, und auch nicht mit elementaren Überlegungen, wie wir sie hier durchgeführt haben. Das Leben ist viel komplizierter. Die Vermutung entstand aus sehr tiefliegenden Überlegungen in der algebraischen Geometrie und der Theorie der Modulfunktionen, und nicht nur im Zusammenhang mit Masons Theorem. Diese Überlegungen sind zu kompliziert, als dass ich sie hier darstellen könnte. Aber ich will trotzdem noch einige Bemerkungen zu diesem Themenkreis machen.

Wir betrachten eine Gleichung der Form

$$u^3 - v^2 = k$$

für teilerfremde ganze Zahlen u, v und k . Diese Gleichung wurde zuerst von M. Hall [Ha] betrachtet; er hat darüber die folgende Vermutung ausgesprochen:

Vermutung von M. Hall. Für ganze Zahlen u, v und k mit $u^3 - v^2 = k \neq 0$ gilt

$$|u|^3 \ll |k|^{6+\epsilon} \quad \text{und} \quad |v|^2 \ll |k|^{6+\epsilon}.$$

Hall hat allerdings die Vermutung ohne ϵ hingeschrieben, da er damals die Notwendigkeit dafür nicht erkannt hat. Aus dem gleichen Grund wie bei der *abc*-Vermutung ist die ursprüngliche Form der Vermutung von Hall falsch. Die “Vermutung von Hall für Polynome” war bereits 1965 von Davenport bewiesen worden [Da], und zwar sogar in einer schärferen Form, nämlich ohne konstanten Faktor auf der rechten Seite.

Satz von Davenport. Es seien f, g zwei nichtkonstante Polynome mit $f^3 - g^2 \neq 0$. Dann gilt

$$\text{grad}(f^3 - g^2) \geq \frac{1}{2} \cdot \text{grad } f - 1$$

und

$$\text{grad}(f^3 - g^2) \geq \frac{1}{3} \cdot \text{grad } g - 1 .$$

Sie können diese Ungleichungen ohne weiteres mit Hilfe des Satzes von Mason beweisen, falls die Polynome f und g teilerfremd sind. Es ist eine gute Übungsaufgabe in Algebra, diese Ungleichungen auch für den Fall *nicht* teilerfremder Polynome f und g zu beweisen. Dann haben Sie wiederholt einen gemeinsamen Faktor auszuklammern, bis Sie beim Fall teilerfremder Polynome angelangt sind, und Sie müssen dann eine Abschätzung für eine allgemeinere Gleichung der Form

$$Af^3 + Bg^2 = h$$

betrachten. Die Schranken, die in den entsprechenden Ungleichungen für die Grade vorkommen, werden natürlich von A und B abhängig sein.

Kehren wir zu den ganzen Zahlen zurück und betrachten wiederum die Gleichung

$$u^3 - v^2 = k$$

für teilerfremde ganze Zahlen u, v, k . Wendet man die abc -Vermutung darauf an, so findet man Abschätzungen

$$|u|^3 \ll (N_0(k))^{6+\epsilon} \text{ und } |v|^2 \ll (N_0(k))^{6+\epsilon} . \quad (6)$$

Dies nachzurechnen ist eine nicht allzu schwierige Übungsaufgabe. Die Vermutung von M. Hall folgt also (wenigstens für teilerfremde Zahlen) aus der abc -Vermutung, denn es gilt $N_0(k) \leq k$. Betrachten wir Gleichungen

$$Au^3 + Bv^2 = k$$

mit von Null verschiedenen, ganzzahligen Koeffizienten A, B , so ergeben sich aus der abc -Vermutung die gleichen Abschätzungen wie in (6); natürlich sind dann die in den Ungleichungen implizit vorkommenden Konstanten von den Koeffizienten A und B abhängig. Noch allgemeiner können wir eine Gleichung von höherem Grad betrachten,

$$Au^n + Bv^m = k ;$$

dabei setzen wir für die (ganzzahligen, positiven) Exponenten n, m nur $mn \neq m + n$ voraus. Es ist dann nicht schwierig, die Abschätzung

$$|u|^n \ll (N_0(k))^{\frac{mn(1+\epsilon)}{mn - (m+n)}}$$

nachzuweisen, und eine entsprechende für $|v|^m$. Wie oben sind dabei natürlich die in den Ungleichungen implizit vorkommenden Konstanten von A und B abhängig. Kehren wir zu $m = 3$, $n = 2$ zurück. Hier gibt es spezielle Werte für A und B , die besonderes Interesse verdienen, zum Beispiel $A = -4$ und $B = -27$. Dann ist

$$-4u^3 - 27v^2 = \Delta$$

bekanntlich die Diskriminante des Polynoms

$$X^3 + uX + v.$$

Für diese speziellen Werte von A und B bilden die vermuteten Ungleichungen die **verallgemeinerte Vermutung** von Szpiro. Szpiro hat allerdings ursprünglich nicht mit N_0 sondern mit einer komplizierteren Invariante N gearbeitet, die aus der Theorie der elliptischen Kurven und der Gleichung

$$Y^2 = X^3 + uX + v$$

stammt. Diese Theorie ist schwierig zu erklären, und wir wollen hier nicht näher darauf eingehen. Jedenfalls wurde Szpiro durch tiefliegende Überlegungen in der algebraischen Geometrie und der Zahlentheorie zu dieser Vermutung geführt. Indem ich N_0 so definiert habe wie in diesem Vortrag und indem ich die *abc*-Vermutung nur mit dem Satz von Mason in Zusammenhang gebracht habe, bin ich ganz und gar nicht der historischen Entwicklung gefolgt. In diesem Sinne habe ich eigentlich eine Unwahrheit erzählt, da ich die Existenz des zugrunde liegenden grossen mathematischen Gebäudes ganz verschwiegen habe. Ich habe aus der ganzen Theorie einfach das herausgenommen, was auf einfache Weise und innerhalb einer Stunde dargestellt werden kann. Aber die Mathematiker, die diese Vermutungen formuliert haben, sind nicht auf so direkte Weise darauf gestossen, sondern erst im Laufe intensiver Beschäftigung mit diesen tiefen und umfangreichen Theorien.¹⁾

Ich will zum Abschluss noch erwähnen, dass die ursprüngliche Vermutung von Szpiro nicht aus den Ungleichungen (6) sondern nur aus der etwas schwächeren Ungleichung

$$|\Delta| \ll (N_0(\Delta))^{6+\epsilon} \quad (7)$$

besteht. Die stärkeren Ungleichungen (6), welche sogar $|u|$ und $|v|$ selbst beschränken und nicht nur $|\Delta|$, wurden erst später formuliert. Dies ist der Grund, weshalb wir oben von der *verallgemeinerten* Szpiro-Vermutung gesprochen haben.

Sie sehen, es hat in der Entwicklung der *abc*-Vermutung eine lange Zeit gebraucht, bis ihre zentrale Stellung voll erkannt worden ist. Die Geschichte verlief nicht gradlinig, sondern auf seltsamen Umwegen, wobei verwandte Sätze für Polynome, wie der Satz von Davenport, eine Rolle spielten, und auch die Vermutung von Hall, deren erstmalige Formulierung sich sogar als falsch herausgestellt hat. Aber dies ist genau die Art und Weise, wie sich die Mathematik entwickelt!

1) Für Anwendungen der *abc*-Vermutung auf die Theorie der elliptischen Kurven sowie für weitere Bemerkungen vergleiche man [La]. Dort ist auch eine umfangreichere Bibliographie zu finden.

Bibliographie

- [BLSTW] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman and S.S. Wagstaff, Jr., *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11$ up to high powers*, Contemporary Mathematics Vol. 22, AMS, 1983
- [Da] H. Davenport, *On $f^3(t) - g^2(t)$* , K. Norske Vid. Selsk. Forrh. (Trondheim), **38** (1965), pp. 86–87
- [Ha] M. Hall, *The diophantine equation $x^3 - y^2 = k$* , Computers in Number Theory (A.O.L. Atkin and B.J. Birch, eds.), Academic Press, London, 1971, pp. 173–198
- [La] S. Lang, *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990) 37–75
- [Ma 83] R.C. Mason, *Equations over function fields*, in “Number Theory, Noordwijkerhout 1983”, Springer Lecture Notes **1068** (1984), 149–157.
- [Ma 84] R.C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Note Series, vol. 96, Cambridge University Press, United Kingdom, 1984

Acknowledgement: I want to express here my appreciation to Urs Stammbach for his efforts in producing the article, and for his translation.

Serge Lang
 Yale University
 New Haven
 Connecticut 06520
 USA

In der neuesten Auflage seines Buches

Serge Lang: *Undergraduate Algebra*, Second Edition, Undergraduate Texts in Mathematics, Springer Verlag 1990

hat der Autor die *abc*-Vermutung und die verschiedenen damit zusammenhängenden zahlentheoretischen Sätze und Vermutungen sowie den Satz von Mason für Polynome bereits berücksichtigt (siehe Chapter IV, §9, p. 165–170). Nur wenige Jahre nach ihrer Entdeckung haben diese Resultate also bereits Eingang in die Lehrbuchliteratur gefunden.