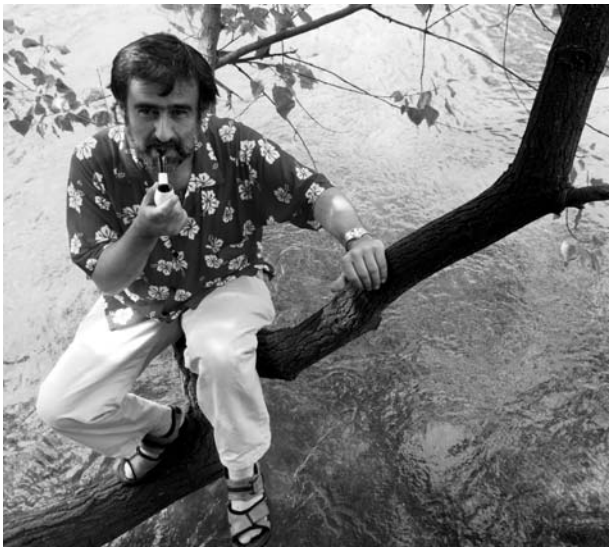

Photo: Stockmeyer

Der Satz von Preda Mihăilescu
Die Vermutung von Catalan ist richtig!

von Gerhard Frey

Satz (Preda Mihăilescu 2002)**.** *Seien x und y ganze Zahlen ungleich* 0*, und seien m und n natürliche Zahlen größer als* 1*, so dass*

$$x^n - y^m = 1$$

ist. Dann ist $n = 2$, $m = 3, |x| = 3$ und $y = 2$.

Dieser Satz bestätigt eine 1842 von E. Catalan aufgestellte Vermutung, deren Beweis Preda Mihăilescu im April 2002 gelungen ist. Dies ist ein weiterer Höhepunkt in der Reihe hervorragender Ergebnisse über Lösungen von diophantischen Gleichungen, die in den letzten zwanzig Jahren erhalten wurden.

Wahrscheinlich werden sich viele Leser beim Lesen von Satz 1 an den Satz von Wiles erinnern, der 1994 die Behauptung von Fermat bewies. Es mag interessant sein, die trotz der formalen Ähnlichkeit bestehenden Unterschiede zu diskutieren.

Fermats Gleichung involviert drei Unbestimmte X, Y, Z, die durch

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

verknüpft sind. Als Ausgleich ist die Beziehung aber homogen: Durch Division mit Z erhält man eine Gleichung vom Catalan-Typ

$$\bar{X}^n + \bar{Y}^n = 1.$$

Allerdings muss man jetzt die Lösungen im Bereich der rationalen Zahlen suchen. Geometrisch bedeutet das: Man muss die Punkte mit rationalen Koordinaten auf einer affinen oder, und das ist kein großer Unterschied, projektiven Kurve finden. Übersetzt man die Catalansche Gleichung in diese Sprache, so muss man die Punkte mit ganzzahligen Koordinaten auf einer affinen Kurve bestimmen. Es ist einleuchtend, dass für diese Fragestellung Methoden der Algebraischen Zahlentheorie viel erfolgversprechender sind als im rationalen Fall.

Betrachtet man nur eine Kurve, so ist die Endlichkeit der Menge der ganzzahligen Punkte schon durch einen fundamentalen Satz von Siegel (1929) gelöst. Für rationale Punkte wurde die entsprechende Aussage erst von Faltings 1983 bewiesen.

Wesentlich komplizierter wird die Fragestellung, wenn man ganze Scharen von Kurven gleichzeitig betrachtet, z. B. auch die Exponenten als Variable auffasst. Im Fall von rationalen Punkten sind hier selbst Endlichkeitsaussagen nur in wenigen Sonderfällen bewiesen. Für ganzzahlige Punkte sieht die Situation etwas besser aus, da Bakers Methoden mit vielen Verfeinerungen oft anwendbar sind.

Im Allgemeinen beginnt aber erst jetzt die schwerste Aufgabe: Die Lösungen sind genau zu bestimmen. Typischerweise sind die Abschätzungen so grob, dass eine Computeruntersuchung hoffnungslos ist. Genauso war auch die Situation im Fall der Catalanschen Vermutung – bis zu den bahnbrechenden Arbeiten

von Mihăilescu. Durch wunderschöne Anwendung der tiefsten Ergebnisse, die wir über die Arithmetik von Kreisteilungskörpern haben, gelingt es ihm, mit einem Schlag *alle* möglichen Lösungen zu bestimmen, und die vorhandenen Endlichkeitssätze und die umfangreichen zur Verfügung stehenden numerischen Resultate werden nur in bescheidenem Umfang benötigt (was deren Bedeutung nicht schmälert).

Abschließend möchte ich erwähnen, dass mir bei der Abfassung dieses Berichtes der „endgültige Beweis" Preda Mihăilescus noch nicht vorlag. Nach mündlichen Mitteilungen von Mihăilescu kann er an einigen Stellen noch elementarer (wenn auch vielleicht nicht durchsichtiger) gemacht werden. Ich werde an den entsprechenden Stellen dies erwähnen, folge aber hier eng der Darstellung, die von Y. Bilu [5] gegeben wurde.

Vorarbeiten

Ich gebe hier nur die für den Beweis des Theorems relevanten Ergebnisse an. Deutlich mehr Informationen findet man in P. Ribenboim [2].

Ein erster Meilenstein war das schon 1850 von Lebesgue erzielte Ergebnis, das die Gleichungen

$$Y^n - X^2 = 1$$

für $n > 1$ nur die trivialen Lösungen mit $x = 0$ besitzt. Interesanterweise hat es danach mehr als 100 Jahre gedauert, bis Chao Ko (1965) bewiesen hat, dass

$$X^2 - Y^n = 1$$

nur Lösungen mit $y = 0$ *und* $x = 3, y = 2, n = 3$ besitzt. Man sieht leicht, dass $X^n - Y^n = 1$ ebenfalls nur triviale Lösungen besitzt.

Es bleibt also zu zeigen: Für verschiedene ungerade Primzahlen p, q und von 0 verschiedene ganze Zahlen x, y ist

$$x^p - y^q \neq 1.$$

Falls notwendig, kann man (x, y, p, q) durch $(-y, -x, q, p)$ ersetzen und deshalb ohne Einschränkung annehmen, dass $2 < p < q$ ist.

Wir gehen im Folgenden immer von einer angenommenen Lösung (x, y, p, q) aus. Durch die Relation zwischen diesen Zahlen ergeben sich zahlentheoretische Bedingungen:

Eugène Charles Catalan

Henri Lèon Lebesgue

Satz (Cassels 1960)**.** *Es gibt $a, v \in \mathbb{Z}$, so dass*

$$x - 1 = a^q \cdot p^{q-1}, \quad y = pav$$

und

$$\frac{x^p - 1}{x - 1} = p \cdot v^q.$$

Für y gelten entsprechende Gleichungen.

Aus diesen Relationen erhält man sofort untere Abschätzungen für x und y durch Ausdrücke in p und q. Zum Beispiel:

$$|x| \geq p^{q-1} - 1; \quad |y| \geq q^{p-1} - 1,$$

oder etwas tiefliegender, aber auch noch elementar herleitbar:

$$|x| \geq q(2p + 1)(2q^{p-1} + 1).$$

Dies ist ein Resultat von Hyyrö (1964).

Mihăilescu selbst bewies:

$$|x| \geq (q^{2p-2}/2)^4.$$

Ein Durchbruch gelang Tijdeman 1976 [6]. Er benutzte Bakers Methode der logarithmischen Linearformen. Der wesentliche Punkt ist, dass Formen

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$$

wobei $b_i \in \mathbb{Z}$ und α_i ganze algebraische Zahlen sind, nicht 0 werden, und dass man für $\log |\Lambda|$ untere Schranken in Abhängigkeit von $\max\{b_i\}$ und der Höhen $h(\alpha_i)$ der algebraischen Zahlen α_i hat. (Zur Definition und Bedeutung von Höhen vgl. [4]. Für teilerfremde natürliche Zahlen m, n ist $h(m/n) = \max\{\log(m), \log(n)\}$.)

Das berühmte Resultat von Tijdeman ist

Theorem 1 (Tijdeman)**.** *Die Exponenten p und q sind durch eine effektiv berechenbare Zahl nach oben beschränkt.*

Also gibt es nur endlich viele Lösungen der Catalanschen Gleichung, und „im Prinzip“ kann man sie alle bestimmen.

Dies ist ein großartiges Ergebnis, das die ganze Kraft der Methode von Baker zeigt. Leider ist die Schranke, die man erhält, so groß, dass eine direkte rechnerische Verifikation außer der Reichweite der Computer liegt. Natürlich versucht man daher, bessere Abschätzungen zu bekommen. Die schärfsten Abschätzungen nach oben, die man für mögliche Exponenten (p, q) erhielt, waren (vgl. [3])

$$\max\{p, q\} \leq 7.78 \cdot 10^{16}.$$

Gleichzeitig werden durch stärkere arithmetische Bedingungen an potentielle Lösungen immer weniger Kandidaten zugelassen.

Hier gelang Inkeri (1964/1992) ein wesentlicher Fortschritt. Er benutzt die Arithmetik von Kreisteilungskörpern, und so ist es nicht verwunderlich, dass Klassenzahlen dieser Körper und „Regularitätsbedingungen“, wie man sie aus zahlentheoretischen Beweisansätzen für den Fermatschen Satz kennt, auftauchen. Sehr bemerkenswert ist es, dass es Mihăilescu in [8] gelang, diese Klassenzahlbedingungen zu eliminieren.

Er erhält

Proposition 1. *Für jede Lösung (x, y, p, q) der Catalangleichung gilt:*

$$p^{q-1} \equiv 1 \mod q^2$$

und

$$q^2 \mid x.$$

Die zweite Aussage von Proposition 1 erleichtert auch numerisches Rechnen beträchtlich. Mignotte und Roy haben mit Rechnern bewiesen, dass $\min\{p, q\} > 10^7$ sein muss (siehe [3]).

Der Fall $p \not\equiv 1 \pmod q$

Die im letzten Abschnitt gesammelten Informationen genügen, um einen Sonderfall auszuschließen.

Proposition 2. *Falls (x, y, p, q) eine Lösung der Catalangleichung ist, dann ist $p \not\equiv 1 \pmod q$.*

Beweisskizze: Wir nehmen an, dass $p \equiv 1 \pmod q$ ist. Aus Proposition 1 folgt, dass $p - 1$ sogar durch q^2 teilbar ist.

Also ist $p = k \cdot q^2 + 1$ mit einer natürlichen Zahl k. Da p ungerade ist, muss k gerade sein. Da $2q^2 + 1$ durch 3 teilbar ist, muss $k \geq 4$ sein, also gilt:

$$p > 4q^2.$$

Wir haben Abschätzungen für q im letzten Abschnitt gesehen. Alles was wir aber hier brauchen, ist, dass $q > 28000$ ist. Denn dann greifen die Methoden von Tijdeman (sogar in vereinfachter Form). Man erhält, dass

$$p \leq 24.34q(\max\{\log \frac{p+1}{\log(q)} + 0,14, 21\})^2 \log(q)$$

ist. Nachrechnen ergibt: Falls $q \geq 28000$, dann ist $p \leq 4q^2$. Das ist aber ein Widerspruch zu dem oben erhaltenen Resultat.

Bemerkung: Nach einer mündlichen Mitteilung hat Preda Mihăilescu eine Beweisvariante gefunden, die sowohl die Bakersche Methode wie auch jegliche Vorberechnung zum Beweis der Proposition 2 überflüssig macht.

Der Beweis

Wir können jetzt annehmen, dass $p > q \geq 7$ und das q prim zu $p-1$ ist. Wir nehmen (x, y, p, q) als Lösung der Catalangleichung an und erinnern uns an die Ergebnisse von Cassels: Es ist $x - 1$ durch p teilbar und $\frac{x^p-1}{x-1} = p \cdot v^q$.

Natürlich erinnert die linke Seite der Gleichung sofort an die Fermatgleichung, rechts steht allerdings eine zu p prime Potenz. Ausserdem kommen nur zwei Variable vor. Beide Unterschiede erleichtern das Leben sehr: Man studiert q-te Potenzen in $\mathbb{Q}(\zeta)$, wobei ζ eine p-te Einheitswurzel ist, und betrachtet darin die Identität

$$\prod_{k=1,\ldots,p-1} \frac{x - \zeta^k}{1 - \zeta^k} = v^q.$$

Es ist leicht zu zeigen, dass die Faktoren auf der linken Seite ganz-algebraisch, zu p prim und teilerfremd sind. Will man dies ausnutzen, stößt man auf die übliche Schwierigkeit:

Es ist das *Ideal*

$$\left(\frac{x - \zeta^k}{1 - \zeta^k}\right)$$

eine q-te Potenz, nicht aber notwendigerweise das Element. Man kann aber Ideale zum „Kapitulieren“ bringen (d. h. zum Hauptideal machen), indem man geeignete ganzzahlige Kombinationen Θ (s. u.) von Elementen aus der Galoisgruppe des Kreisteilungskörpers anwendet. Man ist damit aber immer noch nicht am Ziel: Es treten Einheiten auf, die verhindern könnten, dass $(\frac{x-\zeta^k}{1-\zeta^k})^\Theta$ eine p-te Potenz ist.

Hier beginnt nun die subtile Analyse, die Mihăilescu zum Erfolg führt. Zunächst brauchen wir mehr Definitionen und Notationen.

Es empfiehlt sich, die konjugiert komplexen Paare

$$\left(\frac{x-\zeta^k}{1-\zeta^k}\right)\left(\frac{x-\bar{\zeta}^k}{1-\bar{\zeta}^k}\right)$$

zusammenzufassen und in dem *reellen* Teilkörper $K := \mathbb{Q}(\zeta+\bar{\zeta})$, der den Grad $(p-1)/2$ über $\mathbb{Q}$ hat, zu arbeiten.

Sei G^+ seine Galoisgruppe über $\mathbb{Q}$. Der ganzzahlige Gruppenring von G^+ ist

$$\mathbb{Z}[G^+] := \Big\{ \sum_{g\in G^+, n_g\in\mathbb{Z}} n_g \cdot g \Big\},$$

entsprechend ist der Gruppenring über dem Körper mit q Elementen, $\mathbb{F}_q$, definiert durch

$$\mathbb{F}_q[G^+] := \Big\{ \sum_{g\in G^+, n_g\in\mathbb{F}_q} n_g \cdot g \Big\}.$$

Da G^+ zu q prime Ordnung hat, ist dieser Gruppenring von besonders einfacher Gestalt: Er ist das Produkt von Körpern.

Die Gruppe G^+ und damit $\mathbb{Z}[G^+]$ operieren auf den K zugeordneten arithmetischen Objekten wie der Idealklassengruppe H und der Gruppe der Einheiten $\mathcal{E}$ in natürlicher Weise. Geht man von diesen Gruppen zu Quotienten über, deren Ordnung q teilt, so ist die Operation von $\mathbb{F}_q[G^+]$ wohldefiniert.

So ist $\mathcal{E}/\mathcal{E}^q$ ein zyklischer $\mathbb{F}_q[G^+]$-Modul, dessen Annulator von dem Normelement $\mathcal{N} := \sum_{g\in G^+} g$ erzeugt wird.

Einer der wichtigsten Gründe für die arithmetische Zugänglichkeit der Kreisteilungskörper ist die relativ einfache Struktur ihrer Einheiten.

Die Elemente $\frac{\zeta^k-1}{\zeta-1}$ sind Einheiten in $\mathbb{Q}(\zeta)$, die durch Multiplikation mit geeigneten Potenzen von ζ zu Einheiten in K werden. Sie erzeugen die Gruppe der reellen zyklotomischen Einheiten $\mathcal{C}$. Der Index von $\mathcal{C}$ in $\mathcal{E}$ ist eng mit der Klassenzahl von K verknüpft.

In $\mathcal{C}$ liegen die von Mihăilescu betrachteten q-primären zyklotomischen Einheiten $\mathcal{C}_q$, die nach Definition modulo q^2 kongruent zu einer q-ten Potenz

„Ja, das ist ein ausgezeichneter Beweis. Aber ihm fehlt eine gewisse Wärme.“

im Ring der ganzen Zahlen von K sind.

Der $\mathbb{F}_q[G^+]$-Modul $\mathcal{E}/\mathcal{E}^q$ wird nun in drei Zwischenschritten aufgebaut:

Man betrachtet die $\mathbb{F}_q[G^+]$-Moduln $\mathcal{E}/\mathcal{C}\mathcal{E}^q$, $\mathcal{C}/\mathcal{C}_q$ und $\mathcal{C}_q/(\mathcal{C}_q \cap \mathcal{E}^q)$ mit den paarweise primen Annulatoridealen $\mathfrak{a}_1$, $\mathfrak{a}_1$ und $\mathfrak{a}_3$, mit der Idealidentität

$$\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3 = (\mathcal{N}).$$

Nun zeigt Mihăilescu, dass ganz allgemein in Kreisteilungskörpern wegen $p > q$ das Ideal $\mathfrak{a}_2 \neq (1)$ ist.

Andererseits leitet er aus der Existenz einer Lösung (x, y, p, q) der Catalangleichung her, dass $\mathfrak{a}_1 \cdot \mathfrak{a}_3 = (\mathcal{N})$ ist. Daraus folgt nach einfachen Schlüssen der kommutativen Algebra, dass $\mathfrak{a}_2 = (1)$ ist, und wir haben einen Widerspruch! Also ist Catalans Vermutung bewiesen.

Um zu diesem Ergebnis zu kommen, untersucht Mihăilescu genau die Operation von *„ausgewogenen" Elementen* $\Theta = \sum n_g \cdot g$ mit $\sum n_g = 0$ aus dem Gruppenring $\mathbb{F}_q[G^+]$ auf den Elementen $(x-\zeta)(x-\bar{\zeta})$ modulo q-ten Potenzen. Er zeigt, dass

- $((x-\zeta)(x-\bar{\zeta}))^\Theta \equiv 1 \mod K^{*q}$ für ausgewogene Elemente in $\mathfrak{a}_1\mathfrak{a}_3$ ist, und dass andererseits
- für ausgewogene Elemente Θ, die nicht gleich 0 sind, $((x-\zeta)(x-\bar{\zeta}))^\Theta \not\equiv 1 \mod K^{*q}$ ist.

Daraus folgt recht schnell, dass $\mathfrak{a}_2 = (1)$ sein müsste.

Die erste Aussage basiert auf einem tiefen Theorem von Thaine [7][1], das besagt, dass ein Element aus dem Gruppenring $\mathbb{Z}[G^+]$, das den q-Anteil von $\mathcal{E}/\mathcal{C}$ annulliert, auch den q-Anteil der Klassengruppe von K annulliert.

Der Beweis der zweiten Aussage enthält die schönste Idee von Mihăilescu: Er verbindet reell-analytische Funktionentheorie mit algebraischer Zahlentheorie und mit der Geometrie der Zahlen.

Es ist wohlbekannt, dass für ungerade natürliche Zahlen n die Potenzierung mit n einen Homeomorphismus der reellen Zahlen $\mathbb{R}$ ergibt. Die Umkehrfunktion wird innerhalb des Einheitskreises durch die Binomialreihe

$$\sum_{k=0,\ldots,\infty} \binom{1/n}{k} T^k$$

gegegeben.

Diese Reihe kann sowohl arithmetisch (Nennerauf-nahme) wie auch analytisch gut behandelt werden; explizite Restgliedabschätzungen sind möglich. Koordinatenweise kann man dies auf den reellen affinen Raum der Dimension $(p-1)/2$ ausdehnen, in den man K und also auch $(x-\zeta)(x-\bar{\zeta})$ durch Anwendung der verrschiedenen Einbettungen von K in die reellen Zahlen abbildet.

Delikat ist allerdings die Operation von $\mathbb{Z}[G^+]$ auf diesem Raum, da G^+ nicht stetig operiert. Beschränkt man sich aber auf Elemente von K, bei denen *alle Konjugierten* den Betrag kleiner 1 haben, und setzt dies in die Binomialreihe ein, so ist die Galoisoperation auf dem Ergebnis durch die Operation auf den Teilsummen der Binomialreihen beschreibbar, und die Restgliedabschätzungen können verwendet werden. Dies wendet Mihăilescu auf die Zahlen $(1-\zeta/x)(1-\bar{\zeta}/x)$ an.

Er betrachtet $\Theta \in \mathbb{Z}[G^+]$ mit nicht-negativen Koeffizienten n_g, deren Summe gleich qm ist. (Dies entspricht der „gelifteten" Ausgewogenheitsbedingung.) Die Abschätzungen ergeben, dass die ganzalgebraische Zahl

$$q^{m+ord_q(m!)}x^m(1-\zeta/x)^{\Theta/q}$$

gleich

$$P(T)(x)$$

ist, wobei $P(T)$ ein Polynom ist, das modulo $q\mathbb{Z}[\zeta][T]$ gleich $q^{m+ord_q(m!)}\alpha_m(\Theta)$ ist und $\alpha_m(\Theta)$ der m-te Koeffizient von

$$\left(\sum_{k=0,\ldots,\infty} \binom{1/q}{k} (\zeta T)^k\right)^\Theta$$

ist.

Dies ist das Schlüsselergebnis. Daraus kann Mihăilescu folgern, dass *jeder* Koeffizient von Θ durch q teilbar ist. Also ist Θ modulo q gleich 0, und daraus folgt die zweite Behauptung von oben.

Die ABC-Vermutung

Wie es sich für Mathematiker gehört, lassen wir einem bewiesenen Resultat gleich weitere Fragen folgen.

Die Catalansche Vermutung reiht sich ein in eine ganze Familie von diophantischen Aufgaben des Typs:

Bestimme alle Lösungen von

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

mit $a, b \in \mathbb{Z}$ *fest,* $n, m, k \in \mathbb{N} \cup \{0\}$.

Man sucht also Zahlen x, y, die hohe Potenzen enthalten, und von denen eine (feste) Linearkombination dieselbe Eigenschaft hat.

Offensichtlich kann man diese Fragen mit arithmetischen und mit geometrischen Methoden angreifen.

1 Auch hier hat Mihăilescu mitgeteilt, dass er die Verwendung des Ergebnisses von Thaine vermeiden kann.

Es gibt „triviale“ Lösungen (z. B. für kleine Exponenten), in ganz wenigen Fällen helfen schon Kongruenzbedingungen, manchmal sind algebraische Manipulationen wenigstens in gut verstandenen Erweiterungskörpern wie Kreisteilungskörpern möglich (s. o.), und unter gewissen Homogenitätsbedingungen kann man Galoisdarstellungen ins Spiel bringen.

Im Allgemeinen wird dies aber nicht zum Ziel führen. Daher ist man schon froh, *asymptotische* Aussagen machen zu können.

Das wesentliche Hilfsmittel, das dazu gegenwärtig zur Verfügung steht, ist die oben schon angesprochene Methode von Baker mit vielen Verfeinerungen, die in manchen Fällen zu effektiven oberen Schranken für die Größe von Lösungen führen. Allerdings sind diese Abschätzungen exponentiell, und sie führen auch nicht immer zum Ziel.

Beispiel: Die asymptotische Fermat-Vermutung. *Gegeben seien $a, b, c \in \mathbb{Z}\setminus\{0\}$ und teilerfremd. Dann ist die Menge*

$$\mathcal{L}_{a,b,c} = \{(x,y,z) \in \mathbb{Z}^3 \text{ und teilerfremd};\\ \exists n \in \mathbb{N}_{\geq 4} \quad \text{mit} \quad ax^n + by^n = cz^n\}$$

endlich.

Es gibt nun eine faszinierende Vermutung, die von Masser und Oesterlé 1986 aufgestellt wurde:

ABC-Vermutung: *Zu jeder reellen Zahl $\epsilon > 0$ gibt es eine Zahl $c_\varepsilon \in \mathbb{R}$, so dass für alle teilerfremden $A, B, C \in \mathbb{Z}$ gilt:*

$$|A| \leq c_\varepsilon\Big(\prod_{l \,|\, ABC} \ell\Big)^{(1+\epsilon)}.$$

Dabei steht l für Primzahlen.

Man sieht sofort, welch starke Wirkung diese Vermutung auf Gleichungen vom „Catalan-Typ“ hat.

Sei etwa

$$ax^n + by^m = cz^k$$

mit relativ primen x, y, z.

Dann folgt aus der ABC-Vermutung, dass

$$|(x^{(n-3-\epsilon)}y^{(m-3-\epsilon)}z^{(k-3-\epsilon)}| \leq c_1^3|(abc)^2|$$

mit einer „Weltkonstanten“ c_1, und aus dieser Abschätzung bekommt man sofort Endlichkeitssätze. Diese sind effektiv, wenn c_1 effektiv zu berechnen ist (was üblicherweise Teil der ABC-Vermutung ist).

Leider scheint gegenwärtig der Beweis der ABC-Vermutung außerhalb unserer Reichweite zu sein. Mit Methoden der diophantischen Approximation (s. o.) gelingt es Steward und Tijdeman, eine exponentielle Version der Vermutung zu beweisen.

Es sollte hier bemerkt werden, dass sowohl die Endlichkeitsvermutungen für Lösungen von $aX^n+bY^m = cZ^k$ als auch die ABC-Vermutung natürliche Verallgemeinerungen haben, wenn $\mathbb{Q}$ durch Zahlkörper oder Funktionenkörper einer Variablen ersetzt wird. Es stellt sich heraus, dass der *Beweis* der ABC-Vermutung im Funktionenkörperfall recht einfach ist. Man kann sie beispielsweise aus einer Aussage über Flächen (Ungleichung von Bogomolov–Miyaoka–Yau) herleiten. Interessanterweise hat diese Ungleichung eine Interpretation in der Theorie der arithmetischen Flächen, die zu Kurven über Zahlkörpern gehören. Da diese Theorie schon zu dem Beweis der Mordellschen Vermutung durch G. Faltings geführt hat, könnte sich hieraus durchaus ein hoffnungsvoller Ansatz ergeben. Mehr Einzelheiten finden sich in [1].

Literatur

[1] G. Frey: Galois Representations Attached to Elliptic Curves and Diophantine Problems. Number Theory, Proc. of the Turku Symp. on Number Theory in Memory of Kustaa Inkeri, eds. M. Jutila und T. Metsänkylä. de Gruyter 2001.

[2] P. Ribenboim: *Catalan's Conjecture. Are 8 and 9 the only consecutive powers?* Academic Press 1994.

[3] M. Mignotte: Catalan's equation just before 2000. Number Theory, Proc. of the Turku Symp. on Number Theory in Memory of Kustaa Inkeri, eds. M. Jutila und T. Metsänkylä. de Gruyter 2001.

[4] S. Lang: Survey of Diophantine Geometry. Springer 1997.

[5] Y. Bilu: `http://www.ufr-mi.u-bordeaux.fr/~yuri/`

[6] R. Tijdeman: On the equation of Catalan. Acta Arithm. **29** (1976), no. 2, 197–209

[7] F. Thaine: On the ideal class groups of real abelian number fields. Ann. Math. (2) **128**, no. 1, 1–18 (1988).

[8] P. Mihăilescu: A class number free criterion for Catalan's conjecture. Journ. of Number Th. Im Druck.

Adresse des Autors
Prof. Dr. Gerhard Frey
Institut für Experimentelle Mathematik
Universität Essen
Ellernstraße 29
45326 Essen
`frey@exp-math.uni-essen.de`