Der große Satz von Fermat - die Lösung eines 300 Jahre alten Problems

Jürg Kramer, Humboldt-Universität

Vortrag vom 19.04.1996 an der Urania, Berlin

1 Einführung

In diesem Vortrag soll über die neuesten, aufsehenerregenden Entwicklungen im Zusammenhang mit der Vermutung von Fermat berichtet werden. Diese Vermutung besagt, daß es keine von Null verschiedenen, ganzen Zahlen a, b, c gibt, welche der Gleichung

$$a^n + b^n = c^n \tag{1}$$

genügen, sobald der Exponent n größer als zwei ist. Fermat stellte seine Vermutung um das Jahr 1637 herum, also vor mehr als 350 Jahren, auf.

Pierre de Fermat wurde am 20. August 1601 in der südwestfranzösischen Stadt Beaumont de Lomagne geboren. Auf Drängen seines Vaters schlug er die juristische Laufbahn ein und wurde im Jahr 1631 zum *Conseiller au Parlement de Toulouse* ernannt. Außerdem war Fermat auch als Richter in Toulouse tätig. Politischen Ehrgeiz besaß er nicht; statt dessen widmete er sich in seiner Freizeit der Mathematik, insbesondere der Zahlentheorie, welche damals im wesentlichen aus den in Diophants Werk aus dem 3. Jh., der *Arithmetica*, gesammelten Beiträgen bestand. So kam es, daß Fermat die 1621 von Claude Gaspar Bachet neu herausgegebene *Arithmetica* des Diophant eingehend studierte und seinerseits eine ganze Reihe von Beobachtungen an den Rand seines persönlichen Exemplars notierte. Die meisten dieser Beobachtungen waren nur sehr skizzenhaft, sie wurden aber alle nach dem Tode von Fermat rigoros bewiesen bis auf die eine, die einleitend genannte Vermutung, welche bis 1995 unbewiesen blieb. Die Lösung dieses letzten

Rätsels verdanken wir dem britischen, in Princeton (New Jersey, USA) lehrenden Mathematiker Andrew Wiles, der während mehr als sieben Jahren seine Forschungstätigkeit auf dieses Problem konzentrierte und letztendlich gemeinsam mit Richard Taylor mit einem Beweis der Fermat-Vermutung belohnt wurde; wir werden im zweiten Teil dieses Vortrags darüber berichten. Pierre de Fermat lebte noch fast weitere dreißig Jahre nach seiner berühmten Entdeckung und entwickelte in dieser Zeit neben der Zahlentheorie auch wesentliche Beiträge zur Wahrscheinlichkeitstheorie und zur Differentialrechnung. Am Ende des Jahres 1664 erkrankte Fermat schwer und starb kurz darauf am 12. Januar 1665.

Pierre de Fermat (1601–1665)

2 Wie stieß Fermat auf seine Vermutung?

Bevor wir diese Frage beantworten, erinnern wir an den Lehrsatz des Pythagoras: Ist ein rechtwinkliges Dreieck (s. Fig. 1) mit den beiden Katheten a, b und der Hypothenuse c gegeben, so besteht nach Pythagoras die Beziehung

$$a^2 + b^2 = c^2. \tag{2}$$

Hierbei brauchen die Größen a, b, c nicht notwendigerweise ganzzahlig zu sein; sind z.B. $a = 1$ und $b = 2$, so ist die Hypothenuse c gegeben durch die irrationale Zahl $\sqrt{5} \approx 2,236....$

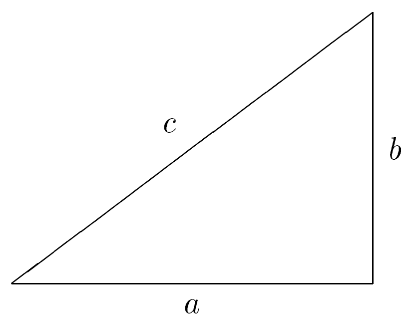

Fig. 1: Rechtwinkliges Dreieck

Bemerkenswerterweise gilt auch die Umkehrung dieses Lehrsatzes: Sind nämlich a, b, c drei positive, reelle Zahlen, die der Gleichung (2) genügen, so gehört dazu ein rechtwinkliges Dreieck mit den Seitenlängen a, b, c, wobei c der Hypothenuse entspricht.

Es stellt sich nun sogleich die Frage, ob es positive, *natürliche* Zahlen a, b, c gibt, welche die Gleichung (2) erfüllen. In der Tat ist den meisten unter uns das Beispiel $a = 3, b = 4, c = 5$ bekannt, denn es gilt ja

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2.$$

Bei den Pythagoreern wurden solche ganzzahligen Tripel (a, b, c) besonders verehrt, da sie harmonischen Verhältnissen entsprechen; so bilden z.B. drei Saiten mit dem Längenverhältnis $3 : 4 : 5$ einen harmonischen Dreiklang. Diese sogenannten *pythagoreischen Zahlentripel* waren z.T. aber auch schon den Babyloniern vor 1600 v.Chr. bekannt; damit konnten sie nämlich leicht rechte Winkel konstruieren, was ihnen bei der Landvermessung zu Gute kam.

Im bereits erwähnten Werk Diophants über Zahlentheorie findet sich nun die Frage nach einer systematischen Konstruktion pythagoreischer Zahlentripel; damit hängt insbesondere auch die Frage zusammen, ob es endlich viele oder gar unendlich viele solche Zahlentripel gibt. Unter Verwendung der heutigen Formelsprache findet sich dort folgendes Konstruktionsverfahren: Man wähle zwei positive, natürliche Zahlen m, n derart, daß m größer als n ist; indem man

$$a := m^2 - n^2\,,\; b := 2mn\,,\; c := m^2 + n^2$$

setzt, erhält man nun ein pythagoreisches Zahlentripel, da man mit Hilfe der binomischen Formel leicht

$$a^2 + b^2 = (m^2 - n^2)^2 + (2mn)^2 =$$

$$m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2$$

nachprüft. Da man die natürlichen Zahlen m, n bei dieser Konstruktion, abgesehen von der leicht zu erfüllenden Bedingung $m > n$, beliebig wählen kann, findet man zugleich, daß es *unendlich* viele verschiedene pythagoreische Zahlentripel gibt.

Beim Studium dieser Passage von Diophants Werk hat sich Fermat nun die Frage gestellt, wieviele Lösungstripel (a, b, c), bestehend aus positiven, natürlichen Zahlen, es denn gäbe, wenn in der Gleichung (2) der Exponent 2 durch den Exponenten $n \geq 3$ ersetzt wird. Aufgrund seiner Untersuchungen kam er zum Schluß, daß es unter diesen Umständen - im Gegensatz zum Fall pythagoreischer Zahlentripel - *kein* einziges solches Zahlentripel (a, b, c) gibt. Fermat faßte diese Erkenntnis in der folgenden, berühmten Randnotiz in seinem Exemplar der *Arithmetica* zusammen:

Cubum autem in duos cubos aut quadrato quadratum in duos quadrato quadratos et generaliter nullam in infinitum quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Die deutsche Übersetzung dieser lateinischen Randnotiz lautet:

Es ist nicht möglich, einen Kubus in zwei Kuben oder ein Biquadrat in zwei Biquadrate und allgemein eine Potenz, höher als die zweite, in zwei Poten-

zen mit demselben Exponenten zu zerlegen. Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist der Rand hier zu schmal, um ihn zu fassen.

Kopie der *Arithmetica*-Ausgabe von Samuel Fermat mit Fermats berühmter Vermutung

3 Die Zeit zwischen 1637 und 1980

Was einen Beweis von Fermats Vermutung anbetrifft, so konnte man Fermats Beobachtungen lediglich einen Beweis für den Exponenten $n = 4$ entnehmen. Dabei verwendete Fermat mit Erfolg seine *Methode des unendlichen Abstiegs:* Ausgehend von einem hypothetischen Tripel (a, b, c) positiver, natürlicher Zahlen mit der Eigenschaft

$$a^4 + b^4 = c^4 \tag{3}$$

konstruierte er ein weiteres Tripel (a_1, b_1, c_1) positiver, natürlicher Zahlen mit den Eigenschaften

$$a_1^4 + b_1^4 = c_1^4 \,,$$
$$a_1 < a \,,\ b_1 < b \,,\ c_1 < c \,.$$

In dieser Weise fortfahrend, konnte Fermat *unendlich* viele Tripel positiver, natürlicher Zahlen konstruieren, welche einerseits der Gleichung (3) genügen, andererseits aber immer kleiner, also beliebig klein werden. Aufgrund der Ganzzahligkeit und der Positivität der konstruierten Zahlentripel ergibt dies aber einen Widerspruch.

Nach dem Tode Fermats im Jahre 1665 erkannte glücklicherweise sein Sohn Samuel die Bedeutung der mathematischen Entdeckungen seines Vaters; er editierte 1670 Diophants *Arithmetica* erneut, nun aber noch ergänzt durch Fermats Beobachtungen *(observationes)*. So standen den nachfolgenden Mathematikergenerationen Fermats Arbeiten zur Zahlentheorie zur Verfügung. Viele der von Fermat nicht rigoros bewiesenen Beobachtungen wurden in der Folge vervollständigt, unter anderem auch durch den berühmten Mathematiker Leonhard Euler (1707-1783). Auch er versuchte sich an Fermats Vermutung; es gelang ihm aber „nur“ ein Beweis im Falle des Exponenten $n = 3$. Nach Eulers Tod erfolgte zunächst ein wesentlicher Beitrag zur Lösung der Fermat-Vermutung durch die Mathematikerin Sophie Germain (1776-1833), die zu jener Zeit gezwungen war, ihre Arbeiten unter dem männlichen Pseudonym *Monsieur Le Blanc* zu publizieren. Im Jahre 1825 gelang dann Adrien-Marie Legendre (1752-1833) und - unabhängig von ihm - dem jungen Peter Gustav Lejeune Dirichlet (1805-1859) ein Beweis der Fermat-Vermutung für den Exponenten $n = 5$. Im Jahr 1839 folgte schließlich Gabriel Lamé (1795-1870) mit einem Beweis für den Exponenten $n = 7$. Aufsehenerregend war das Jahr 1847, als sowohl Gabriel Lamé als auch der berühmte Augustin Louis Cauchy (1789-1857) bei der französischen Akademie der Wissenschaften in Paris Schriften hinterlegten, in denen ein vollständiger Beweis der Fermat-Vermutung angekündigt wurde. Diese Behauptungen wurden aber durch den Zahlentheoretiker Ernst Eduard Kummer (1810-1893) widerlegt; mit Hilfe seiner Untersuchungen gelang es Kummer zudem, einen großen Schritt bei der Lösung des Fermat-Problems voranzukommen: er knackte die Vermutung für die Exponenten $n = \ell$, wobei ℓ eine Primzahl kleiner als 100 (mit Ausnahme der Primzahlen $37, 59, 67$) ist.

Die im vorhergehenden Abschnitt erwähnten Arbeiten zur Fermat-Vermutung basierten sehr oft auf allgemeineren Forschungsresultaten, die wesentlich zur Entwicklung der Zahlentheorie beitrugen. Obwohl man zu Beginn dieses Jahrhunderts weiter an der Lösung des Fermat-Problems arbeitete und im Jahr 1908 zudem der lukrative Wolfskehl-Preis im Wert von 100'000 RM durch die königliche Gesellschaft der Wissenschaften in Göttingen gestiftet wurde, schien sich die Entwicklung der Zahlentheorie immer mehr von der Fermat-Vermutung zu entfernen. So blieb es bis zu Beginn der achtziger Jahre im wesentlichen bei Verfeinerungen der Kummerschen Arbeiten und - nachdem sich die Computertechnologie mehr und mehr verbessert hatte - bei numerischen Überprüfungen der Fermat-Vermutung; so war z.B. im Jahr 1976 durch S.S. Wagstaff bekannt, daß Fermats Vermutung für Primzahlexponenten, die kleiner als 125'000 sind, richtig ist.

4 Die drei Welten

In diesem Abschnitt stellen wir drei Bereiche der Zahlentheorie vor, die alle voneinander unabhängig zu sein scheinen. Wir nennen diese Bereiche kurz „Welten“. Zwei dieser „Welten“ waren schon seit langer Zeit Gegenstand intensiver mathematischer Forschung, sie schienen aber bis vor zwanzig Jahren nichts mit der Fermat-Vermutung zu tun zu haben. Im nachfolgenden Abschnitt werden wir dann zeigen, wie diese „Welten“ miteinander in Verbindung stehen und wie die entsprechenden „Brücken“ zu einem Beweis der Fermat-Vermutung führen. Diese in der Mitte der achtziger Jahre gewonnene Erkenntnis, den Beweis der Fermat-Vermutung mit den scheinbar nicht in Zusammenhang stehenden neueren Entwicklungen der Zahlentheorie zu bringen, verdanken wir dem damals in Saarbrücken, nun in Essen lehrenden Mathematiker Gerhard Frey.

A. Die Anti-Fermat-Welt. In dieser Welt existiert eine Primzahl $\ell > 5$ und ein Tripel positiver, natürlicher Zahlen (a, b, c), welches der Gleichung

$$a^\ell + b^\ell = c^\ell$$

genügt. Ohne Beschränkung der Allgemeinheit können wir annehmen, daß die Zahlen a, b, c paarweise teilerfremd sind; notwendigerweise ist dann genau eine der Zahlen a, b, c gerade.

Es wird letztendlich unser Bestreben sein zu zeigen, daß die *Anti-Fermat-Welt* nicht existieren kann. In diesem Fall existieren dann also keine positiven, natürlichen Zahlen a, b, c, welche die Gleichung (1) mit einem Primzahlexponenten $n = \ell > 5$ erfüllen. Man überzeugt sich dann leicht, daß unter diesen Umständen die Fermat-Vermutung richtig ist.

B. Die elliptische Welt. Diese Welt besteht aus den sogenannten *elliptischen Kurven*. Eine (über den rationalen Zahlen $\mathbb{Q}$ definierte) elliptische Kurve E ist eine in der X, Y-Ebene liegende Kurve, welche durch die kubische Gleichung

$$E \,:\, Y^2 = X^3 + \alpha X^2 + \beta X + \gamma \tag{4}$$

mit den ganzzahligen Koeffizienten α, β, γ festgelegt ist, wobei wir zudem verlangen, daß die drei Nullstellen des kubischen Polynoms rechter Hand paarweise voneinander verschieden sind.

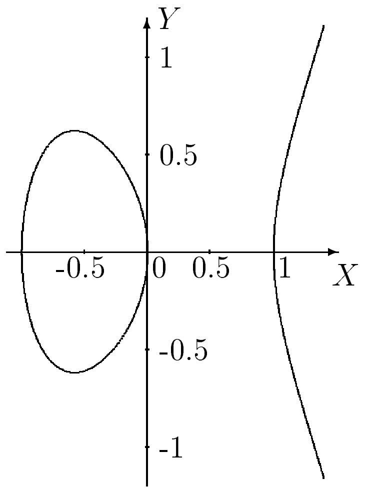

Fig. 2: Das reelle Bild der elliptischen Kurve $Y^2 = X^3 - X$

In der Theorie der algebraischen Kurven hat es sich nun als zweckmäßig erwiesen, die Kurven nicht nur in der affinen X, Y-Ebene zu betrachten, sondern diese in der umfassenderen projektiven Ebene zu untersuchen. Dies bedeutet einfach, daß wir uns die beiden nach $\pm\infty$ verlaufenden Zweige der elliptischen Kurve (s. Fig. 2) durch einen im Unendlichen liegenden Punkt zusammengefügt vorzustellen haben. Lassen wir nun noch stetige Verformungen der nunmehr projektiv betrachteten elliptischen Kurve E zu, so erhalten wir dafür das folgende, aus zwei Kreisen bestehende Bild:

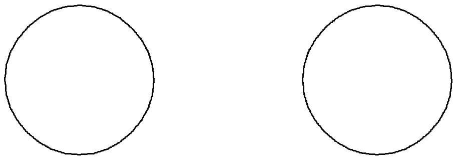

Fig. 3: Das reelle Bild einer elliptischen Kurve nach Hinzufügen des unendlich fernen Punktes: zwei Kreise

Beachten wir schließlich, daß die reelle Welt einen Schnitt durch die komplexe Welt darstellt, so erhalten wir als komplexes Bild der elliptischen Kurve E einen sogenannten *Torus* (s. Fig. 4). Im Folgenden stellen wir uns unter einer elliptischen Kurve jeweils einen solchen Torus vor.

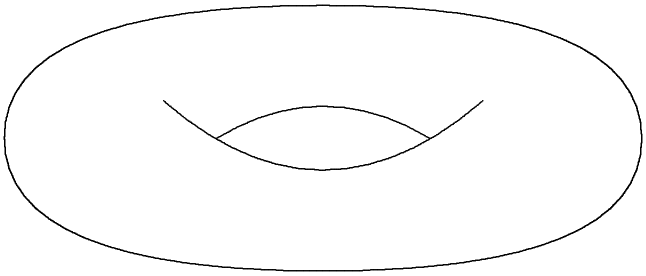

Fig. 4: Das komplexe Bild einer elliptischen Kurve: ein Torus

Eine für das Weitere wichtige Invariante der elliptischen Kurve E ist ihr *Führer* N_E. Die Größe N_E ist dabei wie folgt definiert: Man geht aus von der Gleichung (4) und wählt eine beliebige Primzahl p. Man betrachtet dann (4) als Kongruenz modulo p, d.h.

$$Y^2 \equiv X^3 + \alpha X^2 + \beta X + \gamma \mod p.$$

Für fast alle Primzahlen p, d.h. bis auf endlich viele, werden die Nullstellen des kubischen Polynoms rechter Hand, nun als Restklassen modulo p betrachtet, paarweise voneinander verschieden sein. N_E ist jetzt das Produkt der endlich vielen Ausnahmeprimzahlen, für welche mindestens zwei der drei Nullstellen als Restklassen modulo p zusammenfallen. Wir fügen hier sogleich die Bemerkung an, daß unsere Definition von N_E unvollständig ist, was uns aber hier nicht weiter stören soll.

Beispiel: Elliptische Kurven treten in natürlicher Weise auch bei der Lösung des antiken *Kongruenzzahlproblems* auf: Dazu wird eine positive, natürliche Zahl F vorgegeben. Gesucht wird dann ein rechtwinkliges Dreieck mit rationalzahligen Katheten a, b als auch einer rationalen Hypothenuse c derart, daß der Flächeninhalt des Dreiecks F beträgt. Falls ein solches rechtwinkliges Dreieck existiert, so wird F *Kongruenzzahl* genannt.
Zur Lösung dieses Problems betrachtet man die elliptische Kurve

$$E \,:\, Y^2 = X^3 - F^2X = X(X-F)(X+F).$$

Findet sich nun ein rationaler Punkt $P = (x, y)$ auf dieser Kurve, d.h. gibt es ein Paar rationaler Zahlen (x, y) mit der Eigenschaft

$$y^2 = x^3 - F^2x = x(x^2 - F^2), \tag{5}$$

welches zudem $x > F$ und $y > 0$ erfüllt, so ist das gesuchte Dreieck gegeben durch

$$a = \frac{x^2 - F^2}{y}\,,\; b = \frac{2Fx}{y}\,,\; c = \frac{x^2 + F^2}{y}\,.$$

In der Tat prüft man sofort nach, daß

$$a^2 + b^2 = c^2$$

gilt, d.h. es liegt ein rechtwinkliges Dreieck vor; die Fläche dieses Dreiecks ist aufgrund von Gleichung (5) wie gewünscht gegeben durch

$$\frac{a \cdot b}{2} = \frac{x^2 - F^2}{y} \cdot \frac{Fx}{y} = \frac{x(x^2 - F^2)}{y^2} \cdot F = F.$$

Mit Hilfe dieses Zusammenhangs zwischen dem Kongruenzzahlproblem und der Theorie elliptischer Kurven stellt sich z.B. heraus, daß die Zahlen $F =$

1, 2, 3 keine Kongruenzzahlen sind, daß aber die Zahlen $F = 5$, resp. $F = 6$ Kongruenzzahlen sind; Beispiele entsprechender rechtwinkliger Dreiecke sind in diesen Fällen gegeben durch

$$a = 3/2\,,\ b = 20/3\,,\ c = 41/6\ ,\ \text{resp. } a = 3\,,\ b = 4\,,\ c = 5.$$

C. Die modulare Welt. Diese Welt besteht aus den sogenannten *Modulkurven* und *Modulformen*. Der Einfachheit halber wollen wir uns hier damit begnügen, nur die Modulkurven und diese nur andeutungsweise zu beschreiben. Modulkurven sind gewisse, arithmetisch definierte Flächen, die orientiert und geschlossen sind und durch die positiven, natürlichen Zahlen parametrisiert werden. Die zur positiven, natürlichen Zahl N gehörige Modulkurve wird üblicherweise mit $X_0(N)$ bezeichnet; N wird dabei die *Stufe* der Modulkurve $X_0(N)$ genannt. Die Modulkurve $X_0(N)$ kann man sich aufgrund der einfachen Klassifikationstheorie orientierbarer, geschlossener Flächen als Kugel mit einer gewissen Anzahl g_N von Henkeln oder als Brezel mit g_N Löchern vorstellen (s. Fig. 5):

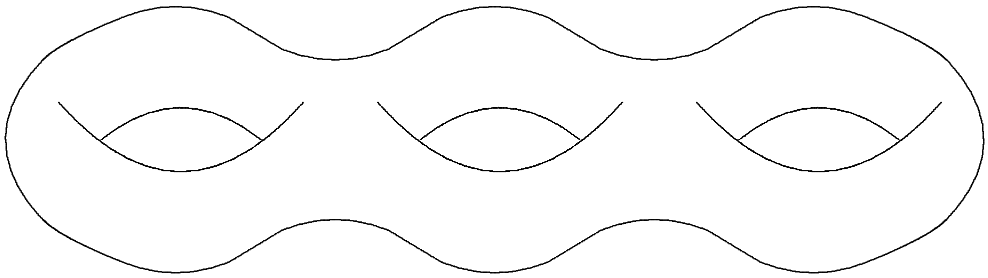

Fig. 5: Das Bild einer Modulkurve $X_0(N)$ vom Geschlecht $g_N = 3$

Die Zahl g_N wird das *Geschlecht* der Modulkurve $X_0(N)$ genannt. Ist z.B. $g_N = 0$, so ist die Modulkurve eine Sphäre, ist $g_N = 1$, so liegt ein Torus vor. Das Geschlecht g_N berechnet sich im wesentlichen mit Hilfe der Formel

$$g_N = \left[\frac{N}{12}\right],$$

wobei $[N/12]$ die größte ganze Zahl, die kleiner als $N/12$ ist, bedeutet.

5 Die Brücken zwischen den drei Welten

In diesem Abschnitt werden wir zunächst zeigen, wie die Anti-Fermat-Welt mit der elliptischen Welt verbunden werden kann; danach werden wir eine Brücke zwischen der elliptischen und der modularen Welt schlagen.

Die Brücke zwischen A und B. Diesen Brückenschlag verdanken wir einer genialen Idee von Gerhard Frey, der dadurch in der Mitte der achtziger Jahre die Fermat-Vermutung wieder ins Zentrum zahlentheoretischer Untersuchungen rückte. Um den Zusammenhang zwischen der Anti-Fermat-Welt und der elliptischen Welt zu beschreiben, gehen wir wie folgt vor: In der Anti-Fermat-Welt finden wir eine Primzahl $\ell > 5$ und paarweise teilerfremde, positive, natürliche Zahlen a, b, c, welche der Gleichung

$$a^\ell + b^\ell = c^\ell$$

genügen. Diesen Daten ordnen wir nun die elliptische Kurve, kurz die *Frey-Kurve*,

$$E_{a,b,c}\ :\ Y^2 = X(X - a^\ell)(X + b^\ell) = X^3 + (b^\ell - a^\ell)X^2 - (ab)^\ell X$$

zu. Es ist nicht schwierig zu zeigen, daß der Führer $N_{a,b,c}$ der Frey-Kurve $E_{a,b,c}$ gegeben ist durch das Produkt aller Primzahlen p, die a, b, c teilen. Da eine der drei Zahlen a, b, c gerade ist, besteht also die Formel

$$N_{a,b,c} = 2 \cdot \prod_{\substack{p \text{ Primzahl} \\ p \mid abc,\, p \neq 2}} p.$$

Damit ist die Brücke zwischen der Anti-Fermat-Welt und der elliptischen Welt geschlagen.

Die Brücke zwischen B und C. Der Brückenschlag zwischen der elliptischen und der modularen Welt ist die großartige Leistung von Andrew Wiles und Richard Taylor. Bereits gegen Ende der fünfziger Jahre begann sich ein Zusammenhang zwischen elliptischer und modularer Welt anzudeuten. Dazu formulierten Goro Shimura und Yutaka Taniyama die folgende Vermutung: Ist E eine (über den rationalen Zahlen $\mathbb{Q}$ definierte) elliptische Kurve mit dem Führer N_E, so wird E von der Modulkurve $X_0(N)$ der Stufe $N = N_E$

überlagert, d.h. es gibt eine arithmetisch definierte, surjektive Abbildung $f : X_0(N) \longrightarrow E$. Man kann sich diese Vermutung grob gesagt auch so vorstellen, daß die Brezelfläche $X_0(N)$ mit g_N Löchern *stetig* in den Torus, der die elliptische Kurve E repräsentiert, deformiert werden kann (s. Fig. 6):

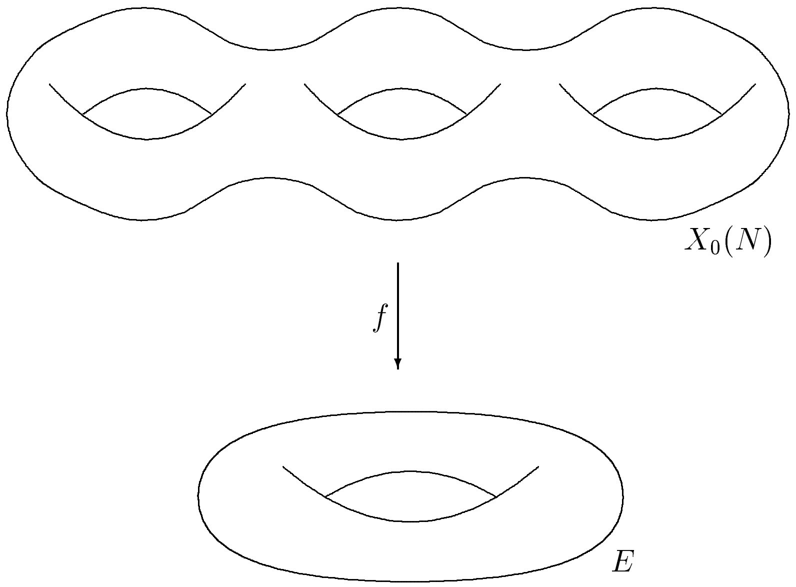

Fig. 6: Überlagerung der elliptischen Kurve E durch die Modulkurve $X_0(N)$

Wir fügen sogleich die Bemerkung an, daß die Stufe $N = N_E$ der Modulkurve, welche die elliptische Kurve E überlagert, nicht notwendigerweise minimal ist, das heißt, es kann unter Umständen eine Modulkurve kleinerer Stufe die gegebene elliptische Kurve E überlagern. Man gelangt zur minimalen Stufe, indem man sukzessive alle „unnötigen" Primteiler von N_E aussondert.

Das Hauptergebnis der von Andrew Wiles und der von Andrew Wiles gemeinsam mit Richard Taylor in den *Annals of Mathematics* publizierten Arbeiten (s. Ann. Math. **141** (1995), 443-551 & 553-572) ist nun die Bestätigung der Vermutung von Shimura und Taniyama. Damit wurde der Brückenschlag zwischen der elliptischen und der modularen Welt vollzogen.

6 Die Anti-Fermat-Welt existiert nicht

Zum Abschluß unseres Vortrags wollen wir nun zeigen, daß es keine Primzahl $\ell > 5$ und kein Tripel positiver, natürlicher Zahlen (a, b, c) mit der Eigenschaft

$$a^\ell + b^\ell = c^\ell$$

gibt; damit wäre dann bewiesen, daß die Anti-Fermat-Welt nicht existiert. Dazu werden wir einen Beweis durch Kontraposition führen, d.h. wir nehmen an, daß die Anti-Fermat-Welt existiert, und werden dies zu einem Widerspruch führen.

Andrew John Wiles vor der Wandtafel in seinem Büro an der Princeton University (Keystone/Charles Rex Arbogast/AP Photo)

Wenn wir also davon ausgehen, daß es eine Primzahl $\ell > 5$ und positive, natürliche Zahlen a, b, c gibt, welche der Gleichung

$$a^\ell + b^\ell = c^\ell$$

genügen, so können wir diesen Daten mit Hilfe der Brücke zwischen der Anti-Fermat-Welt und der elliptischen Welt die Frey-Kurve $E_{a,b,c}$ mit dem Führer

$$N_{a,b,c} = 2 \cdot \prod_{\substack{p \text{ Primzahl} \\ p|abc,\, p\neq 2}} p$$

zuordnen. Aufgrund der Ergebnisse von Wiles und Taylor, d.h. aufgrund der Brücke zwischen der elliptischen und der modularen Welt, wird die Frey-Kurve $E_{a,b,c}$ von der Modulkurve der Stufe $N = N_{a,b,c}$ überlagert. In einer bemerkenswerten Arbeit hat der in Berkeley (Kalifornien, USA) lehrende Mathematiker Kenneth Ribet bereits am Ende der achtziger Jahre bewiesen, daß man die Modulkurve mit minimaler Stufe, die die Frey-Kurve $E_{a,b,c}$ überlagert, findet, indem man alle ungeraden Primteiler p der ursprünglichen Stufe $N = N_{a,b,c}$ weglässt, d.h. die Frey-Kurve $E_{a,b,c}$ wird in Tat und Wahrheit bereits von der Modulkurve $X_0(2)$ der Stufe 2 überlagert. Es gibt somit eine stetige Deformation der Modulkurve $X_0(2)$ auf die Frey-Kurve $E_{a,b,c}$. Nach unserer Formel für das Geschlecht g_2 der Modulkurve $X_0(2)$ gilt nun aber

$$g_2 = \left[\frac{2}{12}\right] = \left[\frac{1}{6}\right] = 0,$$

d.h. wir erhalten die Frey-Kurve aus einer stetigen Verformung der Sphäre. Dies ist aber der gewünschte Widerspruch, da man eine Sphäre nicht stetig in einen Torus deformieren kann; will man dies nämlich tun, so kommt man nicht umhin, ein Loch in die Sphäre zu bohren. Dieses Bohren entspricht aber keiner stetigen Verformung der Sphäre (versucht man es z.B. mit einem Luftballon, so wird dieser dabei unweigerlich platzen).

Mit dieser sehr groben Beweisskizze der Fermat-Vermutung wollen wir unseren Vortrag schließen. Wir machen den interessierten Leser auf die nachfolgende kurze Literaturliste aufmerksam; in den genannten Beiträgen finden sich detailliertere Übersichten über die Geschichte und den Beweis der Fermat-Vermutung sowie ausführliche Literaturverzeichnisse mit der aktuellen Forschungsliteratur.

Literatur

Edwards, Harold M.: Fermat's Last Theorem. Graduate Texts in Math. **50**. Springer-Verlag, New York-Heidelberg-Berlin, 1977.

Kramer, Jürg: Über die Fermat-Vermutung. El. Math. **50** (1995), 11-25 & El. Math. **53** (1998), 45-60.

Ribenboim, Paulo: 13 Lectures on Fermat's Last Theorem. Springer-Verlag, New York-Heidelberg-Berlin, 1979.

Singh, Simon: Fermats letzter Satz - Die abenteuerliche Geschichte eines mathematischen Rätsels. Aus dem Englischen von Klaus Fritz. Carl Hanser Verlag, München-Wien, 1998.

Adresse des Autors

Jürg Kramer
Institut für Mathematik
Humboldt-Universität zu Berlin
Unter den Linden 6
D-10099 Berlin
e-mail: kramer@mathematik.hu-berlin.de