Zum Fermat-Problem

Vortrag im Mathematischen Institut der Universität Heidelberg
am 24.1.98 am Tag der offenen Tür[1])

Bereits vor fünf Jahren wurde die Lösung des Fermat-Problems mit grossem Pressewirbel angekündigt. Inzwischen ist eine Vielzahl von Artikeln zu diesem Thema erschienen, darunter auch manche, die ich sowohl für Mathematiker als auch für Nichtmathematiker empfehlen kann. Vgl. die Literaturangaben am Schluß. Auch wenn Sie den einen oder den anderen Artikel darüber bereits gelesen haben, so finden Sie vielleicht im folgenden noch einiges, was bisher nicht so bekannt geworden ist.

Das Fermat-Problem lautet wie folgt: Gibt es ganzzahlige, positive Lösungen der Gleichung

$$x^n + y^n = z^n \qquad (\text{für} \quad n > 2)\,. \tag{1}$$

In Worten: Ist es möglich, daß eine Summe von zwei n-Potenzzahlen wieder eine n-Potenzzahl ist ?

Der Nachdruck liegt dabei auf der Forderung, daß die gesuchten Lösungen **$\mathbf{x}, \mathbf{y}, \mathbf{z}$ ganze, positive Zahlen** sein sollen. Verzichtet man auf die Ganzzahligkeit und wählt man x, y als beliebige positive Zahlen, so erhält man offenbar stets eine Lösung indem man $z = \sqrt[n]{x^n + y^n}$ setzt. Dies wird jedoch i.allg. keine ganze Zahl sein, selbst wenn x und y ganzzahlig sind.

Wird man mit dieser Problemstellung konfrontiert, so fragt man sich wohl:

1. **Motivation**: *Wie kommt man auf dieses Problem* ?
2. **Ansatz**: *Wie kann man möglicherweise zu einer Lösung vordringen* ?
3. **Anwendungen**: *Was ist die Bedeutung dieses Problems im Hinblick auf mögliche Anwendungen* ? Mit anderen Worten: *Lohnt es sich überhaupt, darüber nachzudenken* ?

Diese Fragen will ich im folgenden behandeln.

Für den Exponenten n in der Fermat-Gleichung (1) wird $n > 2$ vorausgesetzt, also $n = 3, 4, 5, \ldots$. Es erscheint aber sinnvoll, zunächst auch den

[1]) *Die Kommentare in den Fußnoten stammen von Gerhard Frey, dem ich das Manuskript nachträglich vorgelegt hatte.*

Fall $n = 2$ zu diskutieren, weil da nämlich schon seit alters her die Lösungen bekannt sind.

Für $n = 2$ handelt es sich um **Quadratzahlen**. Die zugehörige Gleichung

$$x^2 + y^2 = z^2 \tag{2}$$

kennen Sie wohl zumindest aus dem Schulunterricht im Zusammenhang mit dem **Satz des Pythagoras**: In einem rechtwinkligen Dreieck mit den Seitenlängen x, y, z gilt die Gleichung (2) (wobei x, y die beiden Katheten sind und z die Hypothenuse). Und umgekehrt: Aus der Gleichung (2) folgt, wenn wir dabei $x, y, z > 0$ annehmen, daß x, y, z die Seiten eines rechtwinkligen Dreiecks sind.

In unserem Falle sollen jedoch x, y, z nicht irgendwelche positiven Zahlen sein, sondern *ganze Zahlen*. Das Problem für $n = 2$ läuft also auf die folgende Frage hinaus:

Gibt es rechtwinklige Dreiecke, deren Seitenlängen x, y, z ganzzahlig sind?

Sie wissen wahrscheinlich, daß dies mit „JA“ zu beantworten ist, denn zumindest die folgende Gleichung wird in der Regel im Schulunterricht präsentiert:

$$3^2 + 4^2 = 5^2 \tag{3}$$

Es gibt noch andere ganzzahlige Lösungen der Gleichung (2), zum Beispiel:

$$8^2 + 6^2 = 10^2 \tag{4}$$
$$5^2 + 12^2 = 13^2 \tag{5}$$
$$15^2 + 8^2 = 17^2 \tag{6}$$
$$4961^2 + 6480^2 = 8161^2 \tag{7}$$

Dies lässt sich leicht nachrechnen; bei dem letzten Beispiel wird es allerdings wohl einige Zeit dauern, wenn Sie es im Kopf machen wollen.

Es gibt also in der Tat rechtwinklige Dreiecke, bei denen die Seitenlängen ganzzahlig sind.

Jede Lösung $x, y, z > 0$ von (2) kann benutzt werden, um mit Hilfe einer Schnur einen rechten Winkel darzustellen, nach dem folgenden Muster: Man betrachte z.Bsp. die Lösung (3) mit $x = 3, y = 4, z = 5$. Es wird dann eine Schnur aus $3 + 4 + 5 = 12$ gleichlangen Teilen, die z.Bsp. durch Knoten abgeteilt sind, benötigt. Die beiden Enden der Schnur werden zusammengebunden. Wird dann die Schnur an den Stellen $3, 7$ und 12 gefaßt und straff gezogen, dann entsteht ein rechtwinkliges Dreieck.

Es erscheint sicher, daß diese Konstruktion im Altertum bei der Landvermessung und bei Bauvorhaben wirklich benutzt wurde, um rechte Winkel darzustellen. Pythagoras hat das wahrscheinlich bei seinem Besuch in

Ägypten beobachten können und dadurch seinen Satz gefunden – wenn er überhaupt der Entdecker dieses Satzes gewesen ist; manche Historiker meinen, daß der Satz schon lange vor Pythagoras bekannt war. Dafür spricht u.a., daß bereits auf babylonischen Keilschrifttexten, ca. 1500 v.Chr., u.a. die oben zuletzt angeführte Gleichung (7) vorkommt. (Pythagoras lebte um ca. 550 v.Chr.)

Hat man eine Lösung x, y, z gefunden, so kann man offensichtlich diese drei Zahlen mit einem gemeinsamen Proportionalitätsfaktor t multiplizieren, und man erhält wiederum eine Lösung tx, ty, tz. So erhält man z.Bsp. die oben angeführte zweite Lösung $6, 8, 10$ durch Multiplikation mit 2, also durch Verdoppeln, aus der ersten Lösung $3, 4, 5$. Aber die anderen Lösungen (5)–(7) unterscheiden sich nicht nur um einen Proportionalitätsfaktor. Daher entsteht die Frage:

Lassen sich alle ganzzahligen, positiven Lösungen der pythagoräischen Gleichung (2) *systematisch finden* ?

Die Antwort ist bekannt, es gilt nämlich folgende Rechenvorschrift: Man nehme irgend zwei ganze Zahlen $u > v > 0$ und setze

$$x = u^2 - v^2 \tag{8}$$
$$y = 2uv \tag{9}$$
$$z = u^2 + v^2 \tag{10}$$

Dann gilt (2), was Sie leicht nachrechnen können.

Und zwar erhält man auf diese Weise alle *ganzzahligen positiven Lösungen von* (2)*, wenn man noch zusätzlich die Multiplikation von x, y, z mit einem gemeinsamen Proportionalitätsfaktor t erlaubt.*

Das ist übrigens nicht schwer einzusehen; es läßt sich sogar im Schulunterricht im Zusammenhang mit dem Satz des Pythagoras behandeln. Z.Bsp. für $u = 2, v = 1$ erhält man die Lösung (3) und für $u = 3, v = 2$ die Lösung (5). Um die Lösung (7) zu erhalten, muß man u, v schon größer wählen, nämlich $u = 81, v = 40$.

Die Rechenvorschrift (8),(9),(10) zur Erzeugung der Lösungen findet sich in einem Buch des griechischen Mathematikers **Diophantos**. Wir wissen nicht viel über Diophant, eigentlich fast garnichts. Seine genauen Lebensdaten sind nicht bekannt, aber indirekt kann man schließen, daß er wohl etwa um 250 n.Chr. lebte, und daß er 84 Jahre alt wurde. Er wirkte in Alexandria, damals ein Zentrum der Wissenschaft und kulturelles Bindeglied zwischen Ost und West. Er schrieb seine Bücher in griechischer Sprache, das war damals die Wissenschaftssprache, so wie es später Latein war und heute Englisch ist. Aber wir wissen nicht einmal, ob Diophant wirklich griechischer Herkunft war; es könnte auch sein, daß er z.Bsp. aus Babylonien stamm-

te, denn seine Mathematik zeigt starke Einflüsse aus der babylonischen und indischen Mathematik.

Wir wissen auch nicht alles über Diophants Werk **„Arithmetika“** das aus 13 Büchern bestand. Es war lange Zeit verschollen und wurde erst im 16. Jahrhundert in Europa wieder aufgefunden, allerdings nur teilweise, nämlich 6 Bücher. In dem 6. Buch finden sich neben anderem die obigen Formeln für die Lösungen der pythagoräischen Gleichung (2).

Das Werk von Diophant bildet einen der großen Beiträge des Altertums zur theoretischen Mathematik und hat einen wesentlichen Einfluß auf die heutige Mathematik genommen. Unter einem „*diophantischen Problem*“ versteht man heute allgemein ein solches Problem, bei welchem nach *ganzzahligen* Lösungen gesucht wird.

Diophants wiederentdeckte Bücher wurden aus dem Griechischen ins Lateinische, die damals vorherrschende Wissenschaftssprache, übersetzt. Die Bücher erregten ziemliches Aufsehen, zeigten sie doch, wie hoch das Niveau der griechisch-byzantinischen Mathematik gewesen war. So manches aus dem Diophant war den europäischen Mathematikern der damaligen Zeit nicht bekannt. Deshalb wurde Diophant eifrig gelesen.

Einer dieser Leser war **Pierre de Fermat** (1601–1665). [2]) Er war von Beruf Jurist, betrieb jedoch Mathematik als „Hobby“ wie wir heute sagen würden. Er gilt als einer der größten Mathematiker seiner Zeit. Seine mathematischen Entdeckungen hat er jedoch nicht in wissenschaftlichen Büchern oder Zeitschriften publiziert, sondern sie finden sich vornehmlich in seinen Briefen – er korrespondierte mit fast allen bedeutenden Gelehrten seiner Zeit – und in den Randbemerkungen, die er in seine Bücher schrieb. Nach seinem Tod publizierte sein Sohn den wissenschaftlichen Briefwechsel Fermats, und auch die Randbemerkungen.

Fermat lieferte im allgemeinen keine Beweise im heutigen Sinne. Er begnügte sich mit Andeutungen und Plausibilitätsbetrachtungen; in manchen Fällen verschleierte er bewußt die Beweise, um seine Briefpartner damit herauszufordern. Daher interessierte sich die Fachwelt sehr für den publizierten Briefwechsel, nämlich um herauszufinden, wie weit Fermat wirklich gekommen war. Fast alle bei Fermat aufgestellten Behauptungen konnten schließlich bewiesen werden – nur wenige stellten sich als falsch heraus und konnten widerlegt werden. Es blieb schließlich nur ein einziges Problem offen, nämlich das Problem (1).

Fermat notierte dieses Problem als Randbemerkung in sein Exemplar des „Diophant“, neben die Stelle, wo Diophant den Fall $n = 2$ diskutiert.

---

[2]) *Nicht wichtig aber kurios ist, dass wir wohl nicht einmal die Lebensdaten von Fermat wissen. Sein Geburtsdatum ist mit großer Wahrscheinlichkeit falsch.*

Mit anderen Worten: Fermat stellte sich die naheliegende Frage, was aus der pythagoräischen Gleichung (2) wird, wenn man den Exponenten 2 durch 3 oder durch irgendeine natürliche Zahl $n > 2$ ersetzt. Besitzt die entstehende Gleichung ebenfalls ganzzahlige, positive Lösungen ?

Fermat fand nun heraus, daß für $n > 2$ ganz andere Verhältnisse herrschen als für $n = 2$. Denn die Randnotiz von Fermat lautete wie folgt:

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

Auf deutsch:

> *Es ist unmöglich, einen Kubus in zwei Kuben zu zerlegen, oder ein Biquadrat in zwei Biquadrate, oder allgemein irgendeine Potenz größer als die zweite in Potenzen gleichen Grades. Für diese Behauptung habe ich einen wahrhaft wunderbaren Beweis gefunden, aber dieser Rand ist zu schmal, um ihn zu fassen.*

Fermat behauptete also, daß die Gleichung (1) für $n > 2$ **keine ganzzahligen positiven Lösungen** habe. Das ist der **Satz von Fermat**. Die Mathematiker sprechen in diesem Zusammenhang auch von dem „großen“ Fermatschen Satz, im Unterschied zu einem der anderen Sätze von Fermat, welcher als „kleiner“ Fermatscher Satz bezeichnet wird und heute in jeder Einführungsvorlesung in die Zahlentheorie vorkommt.

> Es gibt allerdings noch eine ganze Reihe anderer Sätze, die von Fermat stammen; sie tragen in der Literatur aber nicht seinen Namen. – In der anglo-amerikanischen Literatur spricht man übrigens nicht vom „großen“, sondern vom „letzten“ Fermatschen Satz: Fermat's Last Theorem, abgekürzt FLT.

Fermats Randnotiz besagt lediglich, daß er einen Beweis besitze; den Beweis selbst konnte er wegen „Platzmangels“ nicht dazuschreiben. Es dauerte nun in der Tat 350 Jahre, bis es den vereinten Kräften vieler Mathematikergenerationen gelang, diese von Fermat gesetzte Nuß zu knacken. Heute nimmt man an, daß sich Fermat geirrt hat; er hat wohl später bemerkt, daß sein „wunderbarer Beweis“ nicht stichhaltig war, versäumte es jedoch, seine Randbemerkung entsprechend zu korrigieren. Dafür spricht, daß Fermat in späteren Briefen dieses Problem nur in den Fällen $n = 3$ und $n = 4$ erwähnt

und behandelt. Der Fall eines allgemeinen Exponenten $n > 2$ wird bei Fermat sonst nirgends diskutiert. Die damals verfügbaren mathematischen Hilfsmittel hätten wohl auch kaum ausgereicht, das allgemeine Problem einer Lösung zuzuführen.

Wir geben nun eine kleine zeitliche Übersicht über die ersten wesentlichen Ergebnisse nach der Fermatschen Eintragung: wann und für welche Exponenten n der Fermatsche Satz zunächst bewiesen werden konnte. Man beachte dazu, was wir bereits oben sagten, daß im Falle $n > 2$ ganz andere Verhältnisse vorliegen als für $n = 2$. Im Falle $n > 2$ geht es nicht darum, alle Lösungen von (1) systematisch zu finden, sondern es handelt sich um den Nachweis, *daß es überhaupt keine ganzzahligen positiven Lösungen gibt.* Diese Aussage ist also von negativer Art: egal, wie eifrig man z.Bsp. mit Hilfe von Computern nach Lösungen suchen mag, man wird niemals welche finden.

Wenn wir also im folgenden berichten, daß der Fermatsche Satz für gewisse Exponenten „bewiesen“ sei, dann bedeutet das nicht, daß man Lösungen gefunden hat, sondern daß man sicher weiß, daß es überhaupt keine ganzzahligen, positiven Lösungen für diesen Exponenten gibt.

Fermat (1601–1665) 1637 Problemstellung; Beweis für $n = 4$, und später andeutungsweise für $n = 3$. [3])

Euler (1707–1783) $n = 3$: Beweis unvollständig [4])

Gauß (1777–1850) $n = 3$: vollständiger Beweis

Dirichlet (1805–1859) $n = 5$: 1825 in der Akademie Paris. Dirichlets Beweis war zunächst unvollständig; nach Kritik durch Legendre gab er einen Ansatz zur Vervollständigung; dieser wurde 1828 in Crelles Journal ausführlich publiziert

Dirichlet $n = 14$: 1832 in Crelles Journal

Lamé (1795–1870) $n = 7$: 1839 in Liouvilles Journal

Lamé n beliebig: 1841 in Liouvilles Journal (Beweis erschien unvollständig; Kritik durch Liouville)

Kummer (1810–1893) 1844 in der Festschrift für das Königsberger Universitätsjubiläum: Die Lücke im Beweis bei Lamé kann *nicht* geschlossen werden! Der Beweisversuch von Lamé ist also endgültig als falsch zu bewerten.

Kummers monumentales Theorem: 1850 in Crelles Journal: Beweis für alle Primzahlexponenten $n = p$, bei denen p eine sogenannte „reguläre“ Primzahl ist. (Wir werden weiter unten darauf eingehen, was eine reguläre Primzahl ist.)

Daß Kummer nur Primzahlexponenten $n = p$ betrachtet, ist durchaus sinn-

[3]) *Natürlich ist 1637 als Datum des Eintrags Spekulation.*

[4]) *Wenn man fair ist, dann hat Euler den Fall* $n = 3$ *richtig bewiesen, man muss allerdings zwei Arbeiten von ihm zusammenfassen, was er selbst nicht tat.*

voll: Wenn nämlich der Fermatsche Satz für alle ungeraden Primzahlexponenten $n = p$ und für $n = 4$ als richtig erkannt ist, dann kann man daraus schließen, daß er auch für beliebige zusammengesetzte Exponenten $n > 2$ richtig ist. Und der Fall $n = 4$ war ja schon von Fermat erledigt worden.

Das genannte Monumentaltheorem von Kummer ist von ganz anderer Qualität als alles andere was bis dahin zum Fermat-Problem erreicht worden war. Während nämlich die früheren Arbeiten sich jeweils auf einen einzigen Exponenten bezogen hatten, kann Kummer die Richtigkeit der Fermat-Vermutung mit einem Schlage für viele Primzahlexponenten $n = p$ beweisen. Alle Anzeichen deuten darauf hin, daß es etwas mehr reguläre Primzahlen gibt wie irreguläre Primzahlen; der Anteil der regulären Primzahlen ist wahrscheinlich etwa 61%. Sollte sich das bewahrheiten, dann hat Kummer bereits im Jahre 1850 die Fermatsche Vermutung für mindestens 61% aller Primzahlexponenten bewiesen! Allerdings weiß man über die Häufigkeit der regulären Primzahlen bis heute nichts Genaues; es gibt nur experimentelle, mit Computern gewonnene Erkenntnisse.

Die einzigen irregulären Primzahlen < 100 sind $p = 37, 59, 67$. Übrigens gelang es Kummer durch Verfeinerung seiner Methode, das Fermat-Problem auch noch für diese drei Primzahlexponenten (und mehr) zu erledigen.

Ich will versuchen, wenigstens anzudeuten, worauf der spektakuläre Erfolg Kummers beruhte.

Der Ansatzpunkt ist, es nicht bei dem Rechnen mit den gewöhnlichen ganzen Zahlen $\mathbb{Z}$ bewenden zu lassen, sondern auch mit **komplexen ganzen Zahlen**, wie Kummer sie nennt, zu arbeiten. Vielleicht kennen Sie z.Bsp. aus dem Gymnasium die komplexe Zahl $i = \sqrt{-1}$, also $i^2 = -1$. Rechnet man mit i, so kann man die Summe zweier Quadrate in ein Produkt zerlegen:

$$x^2 + y^2 = (x + iy)(x - iy)\,. \tag{11}$$

Für manchen mag das Rechnen mit komplexen Zahlen schwieriger erscheinen als das Rechnen mit den gewöhnlichen ganzen Zahlen; für den Mathematiker aber bedeutet es in vieler Hinsicht eine Vereinfachung. Zum Beispiel kann man die Diophantischen Regeln (8)-(10) viel besser verstehen, wenn man zur Herleitung komplexe Zahlen benutzt, nämlich: Setzt man

$$\alpha = u + iv$$

so ist

$$\alpha^2 = (u^2 - v^2) + 2iuv$$

wodurch sich die Terme $u^2 - v^2$ und $2uv$ in (8)-(10) erklären: einfach als Realteil und Imaginärteil eines Quadrats.

Auch die Summe zweier Kuben läßt sich als Produkt darstellen, diesmal aber mit drei statt zwei Faktoren. Dabei rechnet man nicht direkt mit i,

sondern mit der komplexen Zahl

$$\varrho = -\frac{-1}{2} + i\frac{\sqrt{3}}{2} = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) = e^{\frac{2\pi i}{3}} .$$

Und die Zerlegung in drei Faktoren lautet:

$$x^3 + y^3 = (x+y)(x+\varrho y)(x+\varrho^2 y) . \tag{12}$$

Für den Exponenten $n = 3$ hat man also zum Ring $\mathbb{Z}$ der ganzen Zahlen noch die komplexe Zahl ϱ zu adjungieren; die entstehenden Rechenausdrücke bilden zusammen einen „komplexen Zahlring“. Dieser wird mit $\mathbb{Z}[\varrho]$ bezeichnet. Beim Rechnen mit ϱ ist die Regel $\varrho^2 = -1 - \varrho$ zu beachten; damit läßt sich (12) leicht nachrechnen.

Entsprechend für $n = 5$. Jetzt hat man die komplexe Einheit

$$\omega = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5}) = e^{\frac{2\pi i}{5}}$$

heranzuziehen; mit deren Hilfe ergibt sich die Faktorzerlegung in 5 Faktoren:

$$x^5 + y^5 = (x+y)(x+\omega y)(x+\omega^2 y)(x+\omega^3 y)(x+\omega^4 y) \tag{13}$$

Der entstehende komplexe Zahlring wird mit $\mathbb{Z}[\omega]$ bezeichnet. Beim Rechnen in diesem Ring hat man die die Rechenregel $\omega^4 = -1 - \omega - \omega^2 - \omega^3$ zu beachten.

Und so weiter für eine beliebige ungerade Primzahl n. Man hat dann mit der komplexen Einheit

$$\zeta := \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) = e^{\frac{2\pi i}{n}} \tag{14}$$

zu rechnen, wodurch der komplexe Zahlring $\mathbb{Z}[\zeta]$ entsteht. Die Sache wird zwar mit wachsendem n komplizierter zu beschreiben, aber wir sehen deutlich ein Bildungsgesetz für den entstehenden Ring. Und in diesem Ring zerlegt sich wiederum $x^n + y^n$ in n Faktoren, entsprechend wie oben für $n = 5$, nämlich:

$$x^n + y^n = (x+y)(x+\zeta y)\cdots(x+\zeta^{n-1} y) \tag{15}$$

Durch diese Produktdarstellung wird das ursprünglich *additive* Problem (1) übergeführt in ein *multiplikatives* Problem: es geht jetzt um die Frage, ob ein n-faches Produkt, wie es auf der rechten Seite von (15) steht, eine n-te Potenz z^n sein kann.

Das ist also der wesentliche Bestandteil des Ansatzes zur Lösung des Fermat-Problems: *die Umformung von einem additiven in ein multiplikatives Problem*. Der Preis, der für diesen Ansatz zu zahlen ist, besteht darin, daß

man nicht in dem uns gewohnten Ring $\mathbb{Z}$ der ganzen Zahlen zu rechnen hat, sondern in dem Kummerschen komplexen Zahlring $\mathbb{Z}[\zeta]$, wie oben erläutert.

Das Rechnen in diesem komplexen Zahlring ist nicht schwer und geht im Grunde genauso wie in $\mathbb{Z}$; man hat dabei die Rechenregel

$$\zeta^{n-1} = -1 - \zeta - \zeta^2 - \cdots - \zeta^{n-2}$$

zu beachten. Es gibt jedoch einen wesentlichen Unterschied in der multiplikativen Struktur dieser Ringe, nämlich: *in $\mathbb{Z}$ kann jede Zahl eindeutig (bis auf Einheiten) in Primzahlen zerlegt werden, aber dies ist nicht in allen komplexen Zahlringen $\mathbb{Z}[\zeta]$ der Fall.*

Hier liegt nun der Angelpunkt: Vor der Kummerschen Entdeckung krankten die von uns oben als „unvollständig“ bezeichneten Beweisversuche für das Fermat-Problem daran, daß man eine solche Primzahlzerlegung in den betrachteten komplexen Zahlringen als selbstverständlich annahm. Und die Kritik, u.a. von Liouville, stieß sich daran, daß dies keineswegs evident ist, und jedenfalls eines gesonderten Beweises bedarf.

Kummer erkannte als erster, daß nicht in jedem dieser Zahlringe der Satz von der eindeutigen Primzerlegung gilt. Der erste Primzahlexponent n, der dieses bis dahin unbekannte Phänomen zeigte, ist $n = 23$. Es gibt also für $n = 23$ in $\mathbb{Z}[\zeta]$ eine Zahl, die auf zwei wesentlich verschiedene Weisen in Primzahlen zerlegbar ist, d.h. in Zahlen, die selbst nicht mehr zerlegbar sind.

Und dieses Phänomen, nämlich die Nicht-Eindeutigkeit der Primzerlegung in den genannten komplexen Zahlringen, war eines der Hindernisse, die sich dem Versuch entgegenstellten, die bereits bestehenden Beweise für kleine Primzahlen ($n = 3$ und $n = 5$) auf den Fall größerer Exponenten zu übertragen.

Kummer ließ es aber nicht bei dieser Einsicht bewenden. Er untersuchte die Struktur dieser komplexen Zahlringe $\mathbb{Z}[\zeta]$ genauer und fand bald heraus, *woran* die eindeutige Primzerlegung scheitert. Er fand ein Maß für die Größe der Abweichung von der eindeutigen Primzerlegung, nämlich die sogenannte **Klassenzahl**, welche heute meist mit h bezeichnet wird. Und die regulären Primzahlen $n = p$ sind eben diejenigen, für welche h nicht durch p teilbar ist.

Ich will hier nicht auf mathematische Einzelheiten dieser Theorie eingehen. Ich möchte jedoch als die größte Leistung Kummers herausstellen, daß er die Richtung gewiesen hat, wie die Struktur komplexer Zahlringe beschrieben werden kann, und wie man rechnerisch damit umgeht. Und zwar nicht nur für die oben beschriebenen komplexen Zahlringe, sondern auch für algebraische Zahlringe anderer Art. Diese Erkenntnisse haben sich ganz unabhängig von dem Fermat-Problem als fundamental für die Entwicklung der sogenannten **algebraischen Zahlentheorie** erwiesen.

Kummer sprach von „idealen Zahlen“ in seiner Theorie; das waren nicht

wirkliche Zahlen aus den von ihm betrachteten Ring, sondern es handelt sich um damals ganz neuartige Begriffsbildungen. Heute sprechen wir stattdessen von „**Idealen**“ eines Ringes; die von Kummer begonnene Idealtheorie ist heute ein fester Bestandteil der algebraischen Zahlentheorie, und allgemeiner auch der Algebra und algebraischen Geometrie geworden.

Im Jahre 1856 erhielt Kummer für seine Arbeiten eine Goldmedaille der Pariser Akademie,verbunden mit einem Geldpreis. Eigentlich war dieser Preis für die *vollständige* Lösung des Fermat-Problems ausgeschrieben worden. Da aber eine solche Lösung innerhalb von 4 Jahren nicht eingegangen war, so beschloß die Akademie, die Ausschreibung zurückzuziehen und den Preis stattdessen an Kummer zu geben. Damit demonstrierte auch die Pariser Akademie öffentlich, daß sie das Fermat-Problem, welches ja von Kummer nicht vollständig gelöst war, nicht mehr als vorrangig betrachtet. Sondern der systematische Aufbau der algebraischen Zahlentheorie, zu dem Kummer zukunftweisende Arbeiten geliefert hatte, stand nunmehr im Blickpunkt.

Danach war also das Fermat-Problem in den Hintergrund getreten; die Mathematiker waren damit beschäftigt, die Idealtheorie weiter auszubauen und für verschiedene andere Problemstellungen nutzbar zu machen. Viele Mathematiker vertraten die Meinung, daß das Fermat-Problem zwar als Anlaß gedient habe, die Grundlagen der Zahlentheorie zu entwickeln; damit habe es eine wichtige Funktion in der Mathematikgeschichte inne gehabt. Aber sonst sei es an sich nicht besonders interessant. Zum Beispiel haben sich **Gauß** und auch **Hilbert** in dieser Richtung geäußert.

Immerhin gab es doch noch eine Reihe von Mathematikern, die sich trotzdem direkt mit dem Fermatproblem beschäftigten. Es wurden beachtliche Ergebnisse erzielt. Der Kummersche Monumentalsatz wurde erweitert und verallgemeinert, und auf viele irreguläre Primzahlen ausgedehnt. Nach Einsetzen des Computerzeitalters wurden umfangreiche Rechnungen durchgeführt, um für größer und größer werdende Primzahlen $n = p$ die Struktur des zugehörigen komplexen Zahlrings $\mathbb{Z}[\zeta]$ so weit wie möglich aufzuklären. Bis etwa 1990 gelang es, die Gültigkeit der Fermat-Vermutung für alle Exponenten n kleiner als 4 Millionen zu beweisen: $n < 4 \cdot 10^6$.

Gäbe es nun tatsächlich für einen Exponenten n eine nichttriviale Lösung der Fermat-Gleichung (1), dann wäre also $n > 4 \cdot 10^6$. Außerdem konnte gezeigt werden, daß dann die beteiligten Zahlen selbst größer als n^n wären. Für $n > 4 \cdot 10^6$ ergäbe das riesige Zahlen, größer als die Zahl der Elementarteilchen im Universum. Man würde also eine evtl. Lösung niemals in irgendein Buch schreiben können.

Trotzdem waren die Mathematiker mit dem erhaltenen Ergebnis nicht zufrieden; das Fermat-Problem galt weiterhin als ungelöst. Es zeigt sich hierin deutlich der Unterschied zwischen der „Praxis“ und der „theoretischen“ Ma-

thematik. Obwohl überhaupt keine Chance mehr bestand, eine nichttriviale Lösung der Fermat-Gleichung (1) explizit aufzufinden, so war der „theoretische“ Mathematiker damit nicht zufrieden; er wollte sicher sein, daß es überhaupt keine nichttriviale Lösung gibt, wie groß auch immer der Exponent n dabei sein mag.

Das war die Situation etwa im Jahre 1990. Es verbreitete sich die Überzeugung, daß die durch Kummer begonnenen Ideen und Methoden zur Lösung des Fermat-Problems inzwischen ausgereizt wären, so fruchtbar sie sich auch für andere Probleme erwiesen hatten. Für das Fermat-Problem selbst wären damit kaum noch weitere essentielle Fortschritte zu erwarten. Und für die Göttinger Akademie der Wissenschaften zeichnete es sich ab, daß sie den Wolfskehl-Preis vielleicht nicht vergeben könne.

Vielleicht sollte ich an dieser Stelle etwas über diesen berühmten Preis sagen.

Paul Wolfskehl lebte Ende des letzten Jahrhunderts und war eigentlich ein ausgebildeter Arzt. Er hatte aber keine Aussicht, seinen Arztberuf auszuüben, da er an einer schweren unheilbaren Krankheit litt, der Multiplen Sklerose. Er entschloß sich daher, Mathematik zu studieren, weil er dafür Interesse hatte und er sich vorstellen konnte, daß er auch im Rollstuhl noch aktiv mathematisch tätig sein könne. Wolfskehl, der aus Darmstadt stammte, studierte eine Zeitlang in Berlin bei Kummer. Dort ist er u.a. auch mit dem Fermat-Problem bekannt geworden.

Offenbar hat ihn dies so fasziniert, daß er in seinem Testament die beachtliche Summe von 100000 Goldmark für denjenigen stiftete, der das Fermat-Problem vollständig lösen würde. Das war eine ungeheure Summe; in heutiger Währung entspricht das etwa 3 Millionen DM. Wolfskehl stammte aus einer reichen Familie, konnte sich das offenbar leisten. Spötter allerdings behaupteten, daß diese Stiftung nicht ausschließlich aus Begeisterung für das Fermat-Problem errichtet worden war, sondern daß auch der Gedanke mitspielte, seiner Frau dieses Vermögen nicht zu vererben. Nach den vorliegenden Berichten soll Wolfskehls Frau ein wahres Scheusal gewesen sein.

Nach der Stiftungssatzung sollte die Summe von der Göttinger Akademie der Wissenschaften verwaltet werden, die auch die Richtigkeit der eingegangenen Lösungen zu prüfen hatte. Nach Ablauf von 100 Jahren sollte das Stiftungsgeld an die Akademie fallen, wenn sich bis dahin niemand mit einer richtigen Lösung gemeldet hatte.

Wolfskehl starb im Jahre 1907. Demnach war also der Wolfskehl-Preis bis zum Jahre 2007 befristet. Und es sah also schon so aus, als ob der Wolfskehl-Preis, der allerdings infolge diverser Abwertungen im Laufe des bewegten Jahrhunderts ziemlich zusammengeschmolzen war, in der Tat an die Göttinger Akademie zurückfallen würde.

Da trat jedoch eine unvorhergesehene Wende ein, die dem Fermat-Problem eine neue Richtung gab. Diese Wende wurde eingeleitet durch den Mathematiker **Gerhard Frey**.

Frey kommt aus unserer Heidelberger Arbeitsgruppe über Zahlentheorie. Er wurde später Professor an der Universität in Saarbrücken, heute ist er einer der Direktoren des Instituts für experimentelle Zahlentheorie in Essen.

Eines Tages, es muß Ende der siebziger Jahre gewesen sein, erhielt ich von Frey einen Anruf aus Saarbrücken, und er kündigte an, daß er nach Heidelberg kommen würde, er habe etwas Wichtiges zu berichten. Es mußte wohl etwas sehr Wichtiges sein, denn er kam schon am nächsten Tag. Im Diskussionsraum des Mathematischen Instituts erläuterte er uns, daß er einen engen Zusammenhang zwischen dem Fermat-Problem und neueren Problemen über **elliptische Kurven** entdeckt habe.

Elliptische Kurven sind keineswegs Ellipsen. Während eine Ellipse durch eine Gleichung 2. Grades beschrieben werden kann, so werden elliptische Kurven durch Gleichungen 3. Grades gegeben. Die zugegebenermaßen irreführende Bezeichnung „elliptische Kurve“ hat historische Gründe; da sie sich heute allgemein eingebürgert hat, so ist sie wohl nicht mehr zu ändern.

Die Theorie der elliptischen Kurven gehört zu den klassischen Sparten der Mathematik; sie nahm zu Beginn des letzten Jahrhunderts ihren Ausgang mit den Mathematikern **Abel** und **Jacobi**, und sie steht bis heute im Zentrum des Interesses, insbesondere die diophantische Frage nach **ganzzahligen Punkten** auf elliptischen Kurven. Wir denken uns eine solche Kurve gegeben in der Form

$$y^2 = x^3 + Ax^2 + Bx + C \tag{16}$$

Im Rahmen der diophantischen Theorie nehmen wir an, daß die Koeffizienten A, B, C ganze Zahlen sind. Einer solchen Kurve kann man eine sog. *Minimaldiskriminante* Δ zuordnen. Ich will hier nicht die allgemeinen Formeln zur Berechnung der Minimaldiskriminante hinschreiben. Nur so viel möchte ich sagen:

Nehmen wir einmal an, die Fermatsche Vermutung sei nicht richtig. Es gibt dann also ganzzahlige, nichttriviale Lösungen der Gleichung (1) mit einem ungeraden Primzahlexponenten n. Sei a, b, c eine solche Lösung; nach geeigneter Vertauschung und Normierung des Vorzeichens können wir annehmen, daß b gerade ist und a durch 4 geteilt den Rest 1 läßt. (Dann läßt c durch 4 den Rest 1.*) Außerdem sollen a, b, c teilerfremd sein. Die Idee von Frey ist es nun, aus dieser Lösung eine elliptische Kurve zu basteln, nämlich

*In einer früheren Fassung stand hier irrtümlich „Rest 3“ statt „Rest 1“. Ich bedanke mich bei dem aufmerksamen Leser Laizio Rodrigues de Oliveira dafür, dass er mich darauf hingewiesen hat.

durch die Gleichung

$$y^2 = x(x - a^n)(x + b^n)\,. \tag{17}$$

Solche Kurven werden heute **Frey-Kurven** genannt. Die Minimaldiskriminante Δ dieser Frey-Kurve berechnet sich dann wie folgt:

$$\Delta = \frac{a^n b^n c^n}{2^8}\,. \tag{18}$$

Wir sehen, daß jede ungerade Primzahl in dieser Minimaldiskriminante mit einer durch n teilbaren Vielfachheit vorkommt, also mit einer sehr hohen Vielfachheit.[5])

Dies aber, so stellte Frey fest, widerspräche allen bisherigen Erfahrungstatsachen und Vorstellungen, die über die Struktur von elliptischen Kurven existierten. Insbesondere widerspräche das der sog. **Taniyama-Vermutung** über elliptische Kurven. Bitte erlassen Sie mir, diese Vermutung hier zu erläutern; das würde ein Eingehen auf mathematische Einzelheiten erfordern, die den Rahmen dieses Vortrags sprengen. Taniyama ist der Name eines sehr begabten japanischen Mathematikers, der in den fünfziger Jahren bedeutende Beiträge zur Mathematik geleistet hatte, aber ziemlich jung (durch Selbstmord) gestorben ist.

Wenn sich die genannte Taniyama-Vermutung als richtig erweisen sollte, so würde das insbesondere implizieren, daß bei elliptischen Kurven die Primteiler der Minimaldiskriminante nicht sämtlich mit einer durch n teilbaren Vielfachheit auftreten können. Aber die obige Formel für die Minimaldiskriminante Δ einer Freyschen Kurve zeigt, daß alle Primteiler von Δ eine durch n teilbare Vielfachheit besitzen. Das ist ein Widerspruch, und es verbleibt als einzige Schlußfolgerung, daß Frey-Kurven (17) überhaupt nicht existieren können, also kann auch keine Lösung a, b, c der Fermat-Gleichung (1) existieren, die ja zur Definition der Frey-Kurve (17) herangezogen wurde.

Wenn also, so erklärte uns Frey, die Taniyama-Vermutung sich als richtig erweisen sollte, dann sähe er einen Lösungsansatz für einen Beweis des Fermatschen Problems.

Meine Reaktion auf diese Mitteilung, ich muß es gestehen, war damals zunächst negativ. Wenn das so ist, so argumentierte ich, dann ist es ziemlich hoffnungslos, die Taniyama-Vermutung anzugreifen. Denn wir wissen ja, daß das Fermatsche Problem enorm schwierig ist, und daß sich die besten Mathematiker der letzten beiden Jahrhunderte daran vergeblich versucht haben. Die Beobachtung von Frey zeige uns nur, daß die Taniyama-Vermutung mindestens ebenso schwierig ist. Man solle seine Zeit nicht mit Arbeiten an aussichtslosen Dingen verbringen.

---

[5]) *Im Zusammenhang mit der Taniyama-Vermutung ist wichtig, dass alle ungeraden Primzahlen mit einer durch das feste n teilbaren Vielfachheit in die Diskriminante aufgehen, die Größe spielt keine Rolle. Ab* $n = 5$ *klappt alles.*

Glücklicherweise teilte Gerhard Frey nicht meine Ansicht. Er dachte weiter über das Problem nach. Insbesondere, da die Taniyama-Vermutung von allen Fachleuten als besonders wichtig in der Theorie der elliptischen Kurven betrachtet wurde. Es gab viele Wissenschaftler, die daran arbeiteten. Aber Frey wußte inzwischen um den Zusammenhang mit dem Fermat-Problem.

Im August 1984 fand im Mathematischen Institut Oberwolfach, im schönen Schwarzwald, wieder einmal eine internationale wissenschaftliche Tagung statt, und zwar über elliptische Kurven. Hier skizzierte Frey seine Ideen noch einmal. Und dort fand er Resonanz. Einer der Teilnehmer, der amerikanische Mathematiker **Kenneth Ribet**, nahm diese Idee auf und produzierte schon 1986 einen ersten, wichtigen Beweisschritt in die von Frey gewiesene Richtung.[6])

Im Jahr 1986 fand in Paris eine weitere internationale Zahlentheorie-Tagung statt. Dabei entwickelte Frey wiederum seine, inzwischen weitergeführten, Ideen über den Zusammenhang zwischen der Fermat-Vermutung und der Taniyama-Vermutung. Die Zuhörer seines Vortrages waren beeindruckt von diesen neuartigen Zusammenhängen. Plötzlich erhob sich einer der Teilnehmer und erklärte, *dies sei wohl der richtige Weg zum Beweis der Fermat-Vermutung.* Der Name dieses Teilnehmers war **Andrew Wiles**.

Andrew Wiles ist Engländer. Schon als Schuljunge hatte er von dem Fermat-Problem gehört und er nahm sich vor, das Problem später zu lösen. Er studierte Mathematik in Cambridge mit außergewöhnlichen Leistungen. Als es darum ging, ein Thema für seine Doktorarbeit zu erhalten, schlug er seinem Betreuer vor, daß er das Fermat-Problem bearbeiten wolle. Der Betreuer war Professor **John Coates**, heute Präsident der europäischen mathematischen Union. Coates erzählt heute, daß es nicht ganz einfach gewesen sei, den jungen Doktoranden Wiles von seinem Plan mit dem Fermat-Problem abzubringen. Das Problem galt ja unter den Fachleuten als außerordentlich schwierig, und kein Professor möchte einen jungen Doktoranden an eine aussichtslose Arbeit setzen.

Es gelang ihm schließlich, Wiles dazu zu bewegen, ein Thema aus der Theorie der elliptischen Kurven als Doktorarbeit zu nehmen. Das war eine aussichtsreiche Arbeitsrichtung. Wiles promovierte schließlich mit einer hervorragenden Arbeit, und er wurde bald als Experte auf dem Gebiet der

---

[6]) *Die Historie ist verworren. Ich war nicht auf der Zahlentheorietagung 1984 in Oberwolfach, sondern am IMPA. Ich war jedoch im November 1984 auf der AG Geyer-Harder in Oberwolfach und habe dort informell erzählt. Das wurde publik. Im Februar 1985 war ich wieder in Oberwolfach und habe nochmals erzählt, und diesmal war M.F. Vigneras da, die damalige Freundin von Ribet. Mit Ribet selbst hatte ich schon Ende der 1970er über Fermat und Serre-Vermutung geredet, aber jetzt wurden er und Serre aufmerksam. Er hat dann im wesentlichen schon 1985 seinen Satz bewiesen. In Paris 1986 habe ich im Zahlentheorieseminar vorgetragen, der Vortrag ist in Progr. Math. veröffentlicht. Ich konnte da schon auf die Ergebnisse von Ribet und Serre aufbauen.*

elliptischen Kurven angesehen; seine Erfolge waren beachtlich, auch auf dem Gebiet der auf Kummer fußenden algebraischen Zahlentheorie. Wiles erhielt eine Professur an der angesehenen Universität in Princeton, USA.

In seinem Herzen aber dachte Wiles immer noch an das Fermat-Problem. Deshalb wurde er bei dem Freyschen Vortrag so aufgebracht; er kannte sich bei den elliptischen Kurven aus und traute sich zu, die Taniyama-Vermutung zu beweisen und damit auch das Fermat-Problem, an dem sein Herz hing, zu lösen.

Nach der erwähnten Tagung in Paris arbeitete Wiles sieben Jahre lang intensiv an dem Problem. Er studierte alles, was in dieser Zeit an relevanten Ergebnissen erzielt wurde, ließ aber niemanden wissen, woran er selbst arbeite. Zum Beispiel gingen auch die Ergebnisse des früheren Heidelberger Assistenten **Matthias Flach** in den Beweis von Wiles ein.

Am 23. Juni 1993 schien es dann soweit zu sein. Anläßlich eines Vortrags auf einer Tagung in Cambridge (England) kündigte Wiles überraschend an, daß er nunmehr das Fermat-Problem gelöst habe. Zwar konnte er die Taniyama-Vermutung nicht in voller Allgemeinheit beweisen, jedoch war es ihm gelungen, einen wichtigen Einzelfall zu erledigen, der dann für die Frey-Kurven zu denselben Konsequenzen führte wie die volle Taniyama-Vermutung.

Die Euphorie unter den Fachleuten war groß. Man kannte und schätzte Wiles als zuverlässigen und kompetenten Forscher; es gab keinen Anlaß, an der Richtigkeit seines Beweises zu zweifeln. Wenige Minuten nach der Ankündigung wurde von Cambridge aus mit elektronischer Post die Nachricht in alle Welt geschickt. Überall war man erstaunt über diese große Leistung. Auch die Medien berichteten euphorisch darüber.

In der Mathematik gilt jedoch ein Satz erst dann als bewiesen, wenn der Beweis auch der sorgfältigsten Prüfung standhält. Der von Wiles angegebene Beweis wurde vor seiner Publikation natürlich von den Spezialisten besonders genau durchgesehen. Und es stellte sich heraus, daß es doch eine Lücke gab, und daß diese Lücke nicht sofort ausgefüllt werden konnte. Auf dem Züricher Weltkongreß der Mathematiker im Jahre 1994 mußte Wiles zugeben, daß sein Beweis unvollständig war. Es schien so, als ob der Wilessche Beweis, so überzeugend er auf den ersten Blick wirkte, schließlich dasselbe Schicksal erleiden würde wie so viele andere vorhergehende Versuche, das Fermatsche Problem zu lösen, nämlich daß er als gescheitert zu gelten hatte.

Es dauerte über ein Jahr, bis schließlich Andrew Wiles mit einem korrigierten Beweis an die Öffentlichkeit trat; er konnte sich dabei auf Ergebnisse seines früheren Schülers **Richard Taylor** stützen. Diesmal wurde der Beweis anerkannt und publiziert. Die Göttinger Akademie der Wissenschaften mußte satzungsgemäß nach der Publikation noch ein Jahr warten, um si-

cher zu sein, daß wirklich kein gültiger Einspruch gegen den Beweis erhoben wurde. Erst danach, nämlich am 27.Juni 1997, wurde der Wolfskehl-Preis in Höhe von 80000,– DM in einer feierlichen Akademiesitzung an Andrew Wiles überreicht.

Beim Hören all der Festreden aus diesem Anlaß, und beim Anblick der mediengerechten Zeremonien bei der Preisverleihung kam mir erneut und deutlich zum Bewußtsein, daß eigentlich die Idee eines hochdotierten Preises für wissenschaftliche mathematische Arbeit heute nicht mehr sachgerecht ist – jedenfalls dann nicht, wenn dieser Preis an eine einzelne Person vergeben wird. [7]) In der Mathematik stehen wir alle auf den Schultern der früheren Generationen; jede neue mathematische Erkenntnis fußt auf den Ergebnissen der Vorgänger, und insbesondere gilt das für die gewaltige Leistung des Beweises der Fermat-Vermutung. Der Preisträger, Andrew Wiles, war nur der letzte einer langen Kette von Wissenschaftlern, deren Ergebnisse wesentlich in den Beweis eingegangen sind.

Im Grunde ist der jetzt vorliegende Beweis der Fermat-Vermutung ein großartiger Erfolg der kumulativen Arbeit von vielen Mathematikern, sowohl aus unserer Zeit als auch aus der Vergangenheit aus mehr als zwei Jahrhunderten.

Diese Einsicht schmälert sicherlich nicht die Anerkennung der Leistungen von Andrew Wiles, der mehr als sieben Jahre seines Lebens diesem Problem gewidmet hat.

Wir sind nun in der Lage, Antworten auf die eingangs gestellten 3 Fragen zu formuliern.

Zu 1. Motivation. *Fermat kam zu seinem Problem* (1) *durch Verallgemeinerung des klassischen, pythagoräischen Problems* (2) *auf höhere Exponenten* $n > 2$.

Während sich jedoch das klassische pythagoräische Problem aus der praktischen Anwendung beim Bau- und Vermessungswesen herleitete, so war das Interesse an dieser Verallgemeinerung nicht auf Anwendungen bezogen; es handelt sich um theoretische Mathematik im echten Sinne des Wortes. Ein besonderer Reiz an diesem theoretischen Problem lag erstens darin, daß sich die Verhältnisse für $n > 2$ ganz anders darstellten als für $n = 2$. Zusätzlich bestand der Reiz darin, daß die Lösung so außerordentlich schwer war, was

[7]) *Ich bin nicht ganz deiner Meinung. Wiles war der einzige, der genug Mut und Besessenheit hatte, sich an den Beweis zu wagen, unter sehr großem persönlichen Einsatz und Risiko. Eigentlich hätte B. Mazur den Beweis finden müssen, denn alle wesentlichen Zutaten gehen auf ihn zurück. Ohne Preis hätte sich auch wahrscheinlich Wiles nicht an den Beweis gemacht; wenigstens sagt er, dass ihn in seiner Jugend der Preis stark beeindruckt hat. Allerdings: Wäre nicht der Beweis der Taniyama-Vermutung herausgekommen, so wäre viel Mühe für fast nichts aufgewendet worden. So gesehen hat Wolfskehl viel Glück gehabt!*

für viele Mathematiker eine faszinierende Herausforderung bedeutete.

Zu 2. Beweisansatz. *Der erste systematische Ansatz zur Lösung des Fermatschen Problems beruht darauf, das additive Problem* (1) *mit Hilfe der Produktformel* (15) *in ein multiplikatives Problem umzuwandeln.*

Dabei muß jedoch der Ring $\mathbb{Z}$ der gewöhnlichen ganzen Zahlen erweitert werden zum größeren Ring $\mathbb{Z}[\zeta]$ der von Kummer sogenannten „komplexen ganzen Zahlen". Die multiplikative Struktur dieses größeren Ringes folgt jedoch im allgemeinen ganz anderen Gesetzmäßigkeiten als wir es beim gewöhnlichen Ring $\mathbb{Z}$ der ganzen Zahlen gewohnt sind. Es ist das Verdienst von **Kummer**, diese Gesetzmäßigkeiten aufgedeckt zu haben. Dadurch, und durch Weiterverfolgung der Kummerschen Ideen, konnte schließlich der Fermatsche Satz für alle Exponenten $n < 4 \cdot 10^6$ bewiesen werden, jedoch gelang es damit nicht, den Beweis allgemein für beliebigen Exponenten durchzuführen.

Schließlich gab **Gerhard Frey** einen zusätzlichen, neuen Ansatz durch Herstellung des Zusammenhanges mit den elliptischen Kurven, insbesondere der berühmten Taniyama-Vermutung. Dieser Ansatz wurde von **Ribet** ausgebaut und damit der Anschluß an moderne Forschungsrichtungen gefunden. Darauf aufbauend, gelang schließlich **A. Wiles** unter Mithilfe von **R. Taylor** der Beweis eines Teils der Taniyama-Vermutung, und zwar eines solchen Teils, der für die Lösung des Fermatsche Problems ausreichend war.[8])

Zu 3. Anwendungen. Wie bereits oben gesagt, ist das Interesse an der Fermat-Vermutung rein theoretisch begründet, ohne Bezugnahme auf irgendwelche Anwendungen. In der Tat ist mir keine direkte Anwendung bekannt, weder innerhalb der Mathematik noch außerhalb. Insofern ist also das Fermat-Problem selbst im Grunde uninteressant; es gewinnt seine Attraktion nur durch die ungeheuren Schwierigkeiten, die es seiner Lösung entgegensetzte. So wie z.Bsp. ein besonders schweres Kreuzworträtsel den Rätselfreund anzieht, so hat das Fermat-Problem die Mathematiker der ganzen Welt aus 2 Jahrhunderten angezogen. Andererseits:

Die Versuche zur Lösung des Fermat-Problems führten, durch Kummer und andere, zur Erforschung und Grundlegung des gesamten, der heutigen Mathematik weitgehend zugrundeliegenden Gebäudes der algebraischen Zahlentheorie.

Und weiter:

---

[8]) *Eigentlich müsste man hier das entscheidend Neue nennen, das zur algebraischen Zahlentheorie à la Kummer hinzukommt, nämlich: Die Operation der Galoisgruppe und die algebraisch-geometrische Interpretation der Frobeniusautomorphismen. Die macht diophantische Gleichungen zum Bestandteil der arithmetischen Geometrie, und hier sind natürlich (Artin-)Hasse-Weil bahnbrechend. Taniyamas Vermutung wäre ohne Hasses Vermutung undenkbar. Natürlich ist das schwer populär zu sagen, aber Hasse sollte vielleicht doch erwähnt werden.*

Im Zuge der Ideen von Gerhard Frey ergaben sich Zusammenhänge mit der heute im Zentrum der theoretischen Forschung stehenden Theorie der elliptischen Kurven.

Die Versuche zur Lösung des Fermat-Problems führten zu der (zumindest teilweisen) Bestätigung der wichtigen Taniyama-Vermutung.

Dadurch gewinnt das Fermat-Problem in der Tat eine große Bedeutung, nämlich sozusagen **als Katalysator für sehr viel weitergehende Forschungen aus der Zahlentheorie**.

Zusätzliche Bemerkung: Die Zahlentheorie beschäftigt sich mit der Aufklärung der Gesetzmäßigkeiten zwischen ganzen Zahlen. Sie wird traditionsgemäß zur *Theoretischen Mathematik* gerechnet, sozusagen als theoretischer Überbau der übrigen Mathematik. Seit kurzem gibt es jedoch, was vielen Außenstehenden noch nicht bekannt ist, konkrete Anwendungen zahlentheoretischer Erkenntnisse in externen, d.h. nichtmathematischen Bereichen. Und diese Anwendungen spielen eine immer größere Rolle. Ich möchte an dieser Stelle nur die folgenden Bereiche erwähnen, in denen moderne Methoden und Ergebnisse der Zahlentheorie verwendet werden:

Theoretische Physik: Zur Erforschung der physikalischen Vorgänge bei Entstehung des Kosmos, kurz nach dem sog. Urknall.

Codierungstheorie: Zur effektiven Codierung von Nachrichten bei Übertragung durch gestörte Medien, z.Bsp. Nachrichten, die an Satelliten oder an Raumschiffe gesandt werden.

Kryptographie: Zur Verschlüsselung von Daten gegen Mißbrauch.

In diesem Sinne hat also auch die Arbeit an der Lösung des Fermat-Problems nicht nur auf die Theoretische Mathematik einen großen Einfluß ausgeübt, sondern auch auf Anwendungen. Wenn Sie z.Bsp. eine der heute schon gelegentlich umlaufenden Chip-Karten in der Hand haben, so könnte es durchaus sein, daß die darin gegen Mißbrauch eingebauten Sicherungsprogramme diejenigen Algorithmen benutzen, die im Essener Institut von Professor Frey mit Hilfe von elliptischen Kurven und ihren zahlentheoretischen Eigenschaften entwickelt worden sind.

Eine genauere Schilderung dieser und anderer Anwendungen wäre interessant, würde jedoch den Rahmen dieses Vortrags sprengen.

Empfohlene Literatur:

Elemente der Mathematik, 1995
Verständliche Forschung: Moderne Mathematik, Spektrum 1996
Spektrum der Wissenschaft, Januar 1998

Zusatz: *Mitteilungen der Deutschen Mathematiker-Vereinigung, Heft 2-2002*