Der große Satz von Fermat

Schülerinformationstag
Universität Regensburg

5. November 2014

Dieses Skript basiert auf meinem Vortrag zu **Fermats letztem Satz** anlässlich des Schülerinformationstags der Fakultät für Mathematik der Universität Regensburg.

1 Der Ursprung des Problems – Pierre de Fermat

Der sogenannte **Große Satz von Fermat**, auch der **Letzte Satz von Fermat** genannt, ist einer der berühmtesten Sätze der „modernen " Mathematik – wobei modern sich in diesem Fall auf die letzten dreihundert bis vierhundert Jahre bezieht, denn der Satz hat seinen Ursprung in der ersten Hälfte des 17. Jahrhunderts.

Zu dieser Zeit lebte in Toulouse der Richter Pierre de Fermat. Er war, wie es sich für seinen Berufsstand gehörte, ein seriöser und unauffälliger Mann, der sich jedoch ein recht ungewöhnliches Hobby gesucht hatte – die Mathematik. So studierte er unter anderem in seinem stillen Kämmerlein die lateinische Übersetzung eines aus dem dritten Jahrhundert stammenden griechischen Standartwerkes, der Arithmetica des Diophantos von Alexandria [2]. Natürlich hatte er es nicht so einfach wie wir heute. Zu Fermats Zeiten existierten Zahlen, wie wir sie kennen erst seit circa hundert Jahren, und zu Diophantos' Zeiten schon überhaupt nicht.

1.1 Pythagoreische Tripel

Er betrachtete eine Gleichung, die an den Satz von Pythagoreas erinnert. Und den kennen wir natürlich. Er sagt aus, dass wenn mandie Quadrate der Katheten einer rechtwinkligen Dreiecks addiert, man das Quadrat der Hypothenuse erhält. Die zugehörige Gleichung lautet

$$x^2 + y^2 = y^2.$$

Und diese GLeichung hat natürlich Lösungen. Nun interessierte Diophant sich jedoch für ganz bestimmte Lösungen solcher und ähnlihcer Gleichungen, nämlich ganzzahlige Lösungen, das heißt mit $x, y, z \in \mathbb{Z}$. Durch einfaches Ausprobieren findet man rasch einige davon.

Beispiele 1. Das „kleinste" Beispiel ist

$$\begin{aligned} x &= 3 \\ y &= 4 \\ y &= 5 \end{aligned}$$

Man überprüft leicht, dass es sich wirklich um eine Lösung der obengenannten Gleichung handelt.

Wenn man eine Lösung gefunden hat, kann man sich daraus leicht weitere konstruieren. Wähle eine natürliche Zahl $a \in \mathbb{N}$, dann ist

$$\begin{aligned} x &= 3a \\ y &= 4a \\ y &= 5a \end{aligned}$$

eine weitere Lösung wie man leicht zeigt. Und das für jedes gewählte a. So erhält man sogar unendlich viele Lösungen für diese eine Gleichung.

Eine andere algorithmische Methode, Lösungen zu finden, besteht darin, natürliche Zahlen $a, b \in \mathbb{N}$ mit $a > b$ zu wählen. Und dann folgendes Zahlentripel zu betrachten.

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ y &= a^2 + b^2 \end{aligned}$$

In der Tat erhält man bei einsetzten in die pythagoreische Gleichung

$$\begin{aligned} x^2 + y^2 &= (a^2 - b^2)^2 + (2ab)^2 \\ &= a^4 - 2a^2b^2 + b^4 + 4a^2b^2 \\ &= a^4 + 2a^2b^2 + b^4 \\ &= (a^2 + b^2)^2 = z^2 \end{aligned}$$

Lösungen $(x, y, z) \in \mathbb{Z}^3$ der oben genannten Gleichung werden **pythagoreisch Zahlentripel** genannt.

1.2 Gleichungen höherer Ordnung

Dies war auch Fermat bekannt, und wahrscheinlich war ihm recht schnell langweilig dabei, weshalb er die Gleichung etwas abgeändert hat. Anstatt Quadrate der Variablen zu betrachten, hat er sich gefragt, was wohl passiert, wenn man die Potenz um eins erhöht.

$$x^3 + y^3 = y^3$$

Die geometrische Bedeutung dieser Gleichung wäre, Kuben oder Würfel an den Seiten eines (rechtwinkligen) Dreiecks zu betrachten. Aber wir interessieren uns mehr für den arithmetischen Aspekt, nämlich, gibt es ganzzahlige Lösungen? Natürlich gibt es eine triviale, die gleich ins Auge springt.

$$\begin{aligned} x &= z \\ y &= 0 \end{aligned}$$

Aber gibt es interessantere Lösungen? Die Gleichung sieht fast genauso aus, wie die Gleichung des Pythagoras. Da sollte es doch Lösungen geben, oder? Und Fermat setzte sich hin, und probierte dies und das – und kam zu keinem Ergebnis. Gab es etwa keine Lösung? Er versuchte die nächsthöhere Potenz.

$$x^4 + y^4 = z^4$$

Und suchte hierfür Lösungen. Und wieder kommt er zu dem gleichen Ergebnis, nämlich keinem. So geht es ihm noch bei allen weiteren Versuchen. Und er beginnt zu vermuten, dass es keine Lösung gibt. Genauer, dass es für $n \geqslant 3$ keine $x, y, z \in \mathbb{Z} \setminus \{0\}$ gibt, die die Gleichung

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

lösen würden.

1.3 Die Vermutung

Das hat Fermat natürlich keine Ruhe gelassen. Er hatte nun zwei Möglichkeiten: die Vermutung zu beweisen, oder ein Gegenbeispiel finden. Da er en letzterem gescheitert war, versuchte er sich an einem Beweis. Und er fand tatsächlich einen! Oder zumindest glaubte er das. Auf dem Rand seines Buches notierte er folgendes.

> „*Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*“
>
> „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. Ich habe hierfür einen wahrhaft wunderbaren Beweis gefunden, doch ist der Rand hier zu schmal, um ihn zu fassen.“

Und das war typisch für ihn. Dieses Buch war übersäht mit solchen Randbemerkungen zu verschiedenen Sätzen, die er endeckt hatte, oder Beweise, die er vereinfacht hatte. Und er hat sich wahrscheinlich nichts dabei gedacht, er hielt seine Gedanken nicht für so wichtig, als dass es die Nachwelt interessieren würde.

2 Erste Lösungsversuche

Später hat allerdings sein Sohn seinen Nachlass durchgesehen, und eine Neuausgabe der Arithmetica des Diophantos herausgegeben, einschließlich der Anmerkungen seines Vaters. Dies wurde so nach und nach aufgearbeitet, wobei insbesondere Leonhard Euler einen beträchtlichen Anteil hatte. So konnte jeder Beweis Fermats sozusagen wiederentdeckt werden – bis auf jenen oben aufegrührten „wahrhaft wunderbaren" Beweis. Daher stammt auch der Name **Fermats letzter Satz**, der letzte Satz, der von diesem genialen Geist ersonnen wurde, der sich fortlaufend den Lösungsversuchen der Mathematikergemeinschaft entzog.

2.1 Einzelfälle

Um Intuition für einen Beweis zu bekommen, ist eine Möglichkeit, sich Einzelfälle anzuschauen. So wurde schon Ende des 17. Jahrhunderts ein Beweis für den Fall $n = 4$ veröffentlicht. Euler fand einen weiteren Beweis dafür, und ebenso für den Fall $n = 3$. Und nach und nach kamen Beweise für weitere Fälle hinzu, meist für Primzahlen.

Man kann relativ leicht einsehen, dass es ausreichen würde, die Vermutung für 4 und ungerade Primzahlen zu Beweisen. Zunächst macht man sich folgendes klar.

Lemma 2. *Jede natürliche Zahl $n > 2$ ist durch 4 oder eine ungerade Primzahl teilbar.*

Beweis. Der Fall wenn n 4 oder eine ungerade Primzahl ist, ist trivial. Sei nun

$$n = \prod_{p \text{ prim}} p^{a_{n,p}}$$

die Zerlegung von n in Primzahlen, wobei $a_{n,p} \in \mathbb{N}_0$. Ist n durch eine ungerade Primzahl teilbar, sind wir fertig. Nehmen wir also an, dass n nicht durch eine ungerade Primzahl teilbar ist, das heißt die Primfaktorzerlegung vereinfacht sich zu

$$n = 2^{a_{n,2}}.$$

Da $n > 2$, muss die Potenz hier größer 1 sein, $a_{n,2} > 1$, und somit n teilbar durch $4 = 2^2$. □

Nun fährt man fort:

Proposition 3. *Es genügt Fermats letzten Satz für $n = 4$ und ungerade Primzahlen zu zeigen.*

Beweis. Sei e ins ungerade Primzahl oder 4, die n teilt. Dann hat man eine Zerlegung $n = d \cdot e$. Findet man nun ein Tripel $(a, b, c) \in \mathbb{Z}^3 \setminus \{0\}$, mit

$$a^n + b^n = c^n$$

so kann man diese Gleichung vereinfachen zu

$$\begin{aligned} a^{d\cdot e} + b^{d\cdot e} &= c^{d\cdot e} \\ (a^d)^e + (b^d)^e &= (c^d)^e \end{aligned}$$

und hat in dem Tripel (a^d, b^d, c^d) eine Lösung für

$$x^e + y^e = z^e$$

gefunden. Oder andersherum, beweist man Fermats Vermutung für e, hat man sie automatisch für alle vielfachen bewiesen. □

Die Fall $n = 4$ war ja schon erledigt, und auch eine ganze Reihe niederer Primzahlen, so dass man sich auf höheren Primzahlen konzentrieren konnte. Trotz dieser Vereinfachung blieb jedoch das Problem bestehen, dass es unendlich viele Primzahlen gab, die man härte testen müssen. Im Laufe der Zeit gab es jedoch weiter Fortschritte. Man konnte die Vermutung zum Beispiel für bestimmte Familien von Primzahlen zeigen. Und immer mal wieder kam jemand daher, sowohl professionelle, als auch zunehmend Amateurmathematiker, der behauptete, er habe einen Beweis gefunden. Die Aufregung war jedesmal groß, doch niemals hielt ein Beweis einer genaueren Überprüfung stand. Je mehr Zeit verstricht, je mehr Fehlversuche ans Licht kamen, desto größer wurde das Verlangen, einen Beweis zu finden. Sollte Fermat sich

geirrt haben? Gab es irgendwo ein Gegenbeispiel? Und das war ja auch sehr seltsam: da hatte man eine Gleichung

$$x^2 + y^2 = z^2$$

mit unendlich vielen Lösungen. Sollte man unendlich viele Gleichungen

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

mit keiner einzigen LL̈osung (außer der trivialen) haben?

2.2 Kontroverse über Existenz von Fermats Beweis

Man kann sich fragen, hatte Fermat wirklich einen Beweis, wie er behauptete? Da gibt es mehrere Möglichkeiten. Entweder, er hatte keinen Beweis, und wusste es. Und hat sich einen Spaß daraus gemacht, der Nachwelt ein Rätsel zu hinterlassen. Doch angesichts dessen, was man über Fermats Leben weiß, erscheint das eher unwahrscheinlich. Die zweite Möglichkeit ist, dass er einen Beweis gefunden hatte, aber alle Mathematiker bis heute zu dumm waren diesen zu finden. Diese These treibt nicht nur die Gerüchtemühle an, sondern bis heute Menschen, sich mit dem Thema zu beschärtigen, und diesen „wahrhaft wunderbaren “ Beweis zu finden. Die dritte Möglichkeit ist, dass Fermat glaubte einen Beweis zu haben, jedoch irgendwo einen Fehler gemacht hatte, so dass er nicht gültig war.

Dies scheint auch dadurch bestätigt zu werden, dass je mehr man sich mit dem Thema beschäftigte, desto deutlicher wurde, dass damit zusammenhängende Konzepte sehr komplexe Mathematik beinhalteten. Insbesondere der Beweis, der schließloch doch gefunden wurde, ruht auf modernsten Techniken der Mathematik.

3 Beweis der fermatschen Vermutung

Dieser Beweis wird von dem britischen Mathematiker Andrew Wiles erbracht. Als er circa zehn Jahre alt war, stolperte er über die fermatsche Vermutung. Er beschloss, dieses Problem, das so einfach darzulegen ist, dass es ein Zehnjädriger leicht verstehen kann, und das doch Jahrhunderte lang Mathematiker in Atem gehalten hat, zu beweisen. Und das hat ihn nie losgelassen, keiner konnte ihm dabei weiterhelfen. Jahre später, als er schon ein erfolgreicher Mathematiker war, und Professor in Princeton, war die Zeit reif für ihn, sich an die LL̈osung des Problems zu machen. Er zog sich zurück, setzte sich in aller Stille, ohne jemandem von seinem Vorhaben mitzuteilen, sieben Jahre hin, in denen sich viele fragten, was er denn machte. Und dann kündichte er eine Vortragsreihe an, in der er Fermats letzten Satz beweisen wollte.

Der Beweis beinhaltete unglaublich komplexe Theorien und Konzepte. eigentlich hat er nicht die fermatsche Vermutung bewiesen, sondern eine andere Vermutung, aus der Fermats letzter Satz folgen sollte. Es war die sogenannte Taniyama–Shimura Vermutung, die man mit dem Satz zusammenfassen kann, dass „jede elliptische Kurve modular sei“.

3.1 Elliptische und modulare Kurven

Eine elliptische Kurve ist ein geometrisches Gebilde, das durch eine Gleichung der Art

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

wobei y und x Variablen und $a_1, \ldots, a_6 \in \mathbb{Z}$ Koeffizienten sind. Darunter kann man sich erstmal nicht so viel vorstellen, doch wenn man nach Lösungen X und y in den reellen Zahlen sucht, bekommt man etwas, das aussieht, wie die Oberfläche eines Donuts.

Eine modulare Kurve ist ein geometrisches Gebilde, das als ein Quotient einer Halbebene dargestellt werden kann. Genauer gesagt, betrachtet man Vektoren auf einer Halbebene $\begin{pmatrix} x \\ y \end{pmatrix}$ und operiert mit Matrizen auf ihnen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

Nun betrachtet man nicht irgendwelche Matrizen, sondern solche, deren Determinante 1 ist, und die auf der Diagonalen Einträge haben, die Vielfache einer natürlichen Zahl $N \neq 0$ sind. Die Menge aller solcher Matrizen formt eine sogenannte modulare Gruppe und wird mit $\Gamma_0(N)$ bezeichnet. Nun identifiziert man

auf der gegebenen Halbebene zwei Vektoren $\begin{pmatrix} x \\ y \end{pmatrix}$ und $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, wenn man den einen aus dem anderen erhält durch Multiplikation mit einer Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. So erhält man eine modulare Kurve $X_0(N)$.

Kann man nun eine elliptische Kurve in der Form $X_0(N)$ darstellen, heißt sie modular.

3.2 Fermats letzter Satz und Modularität

Welcher mysteriöser Zusammenhang besteht nun zwischen modularen elliptischen Kurven und Fermats letztem Satz?

Theorem 4. *Fermats letzter Satz folgt aus der Taniyama–Shimura Vermutung.*

Beweis. (Skizze) Angenommen Fermats letzter Satz ist falsch. Dann findet man eine Lösung $a, b, c \in \mathbb{Z} \setminus \{0\}$so dass für eine Primzahl $p \geqslant 3$

$$a^p + b^p = c^p.$$

Hieraus kann man folgende elliptische Kurve konstruieren

$$y^2 = x(x - a^p)(x + a^p).$$

Diese Kurve wird auch Frey-Kurve genannt, da sie von Gerhard Frey [1] konstruiert wurde. Ken Ribet zeigte nun, dass die so konstruierte Kurve auf keinen Fall modular sein kann [4]. Somit hätte man ein Gegenbeispiel zur Taniyama–Shimura Vermutung gefunden. □

Das Problem wurde also verschoben, und die Herausforderung bestand darin, die Taniyama–Shimura Vermutung zu beweisen – dann würde man quasi umsonst Fermats letzten Satz bekommen.

3.3 Vollendung des Beweises

Wiles glaubte, er könnte diese Vermutung zeigen. In den folgenden sieben Jahren widmete er sich ausschließlich diesem Problem. Und natürlich war die Aufregung groß als er seinen Beweis, welcher mehrere hundert Seiten umfasste, endlich präsentierte. Doch um ein solches Ergebnis zu zementieren, musste der Beweis Zeile für Zeile von Experten untersucht und nachgeprüft werden. Es kam, wie es kommen musste: ein Fehler wurde gefunden. Zuerst hielt man ihn für einen kleinen leicht zu behebenden Fehler, doch das stellte sich als Trugschluss heraus. In dieser Situation suchte sich Andrew Wiles einen Vertrauten, Richard Taylor, und gemeinsam behoben sie innerhalb eines Jahres den Fehler.

Endlich war ein relevanter Teil der Taniyama–Shimura Vermutung, die nunmehr Modularitätssatz hieß, und im gleichen Atemzug Fermats letzter Satz bewießen.

Dieses Rätsel, dass vor über 300 Jahren in Form von Zahlenspielereien seinen Anfang nahm, und die Mathematikerwelt so lange in Atem hielt war gelïst. Wichtiger als diese Tatsache jedoch ist vielleicht der Weg dorthin, denn auf diesem wurden neue Theorien entwickelt, Sätze gefunden, Beweise vereinfacht, Brücken zwischen verschiedenen Teilgebieten der Mathematik geschlagen. Damit hat der Nachlass von Fermat einen weit größÄren Einfluss auf die moderne Mathematik, als man von Zahlenspielen, die Nichtexperten zugänglich sind, erwarten könnte.

Literatur

[1] Gerhard Frey. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sarav.*, 1(1):pp. 40, 1986.

[2] Diophantos of Alexandria. *Aritmetica.* 1621. translated into Latin by Claude Gaspard Bachet de Méziriac.

[3] P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer, 1979.

[4] Kenneth A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *inventions mathematicae*, 100(2):431–476, 1990.

[5] Simon Singh. *Fermat's Last Theorem.* Harper Collins Publishers, 2012.