Die Mathematikerin Sophie GERMAIN und ihr Beitrag zum Beweis von FERMAT's letztem Satz

Sophie GERMAIN (1776 – 1831)

Sophie GERMAIN wurde am 01.04.1776 in Paris geboren. Ihre Eltern, Ambroise-François und Marie-Madeleine, gehörten zum wohlhabenden Bürgertum.

Während der wirren Jahre, die durch die französische Revolution ausgelöst wurden, blieb die junge Sophie GERMAIN meist im Haus und zog sich in die Bibliothek ihres Vaters zurück. Es wird erzählt, sie habe dort über das Schicksal des ARCHIMEDES (287 - 212 v. Chr.) gelesen, welches ihr mathematisches Interesse geweckt habe.

Sophie GERMAIN's Eltern waren vom Wunsch ihrer Tochter, sich in die Mathematik zu vertiefen, nicht begeistert und versuchten, das Mädchen davon abzuhalten. So nahmen sie ihr z. B. die Kerzen weg oder löschten das Feuer in ihrem Zimmer. Sie aber schaffte es, ihr Selbststudium – nicht nur auf mathematischem Gebiet – fortzusetzen, las Werke von Étienne BÉZOUT (1730 - 1783), Isaac NEWTON (1643 - 1727) und Leonhard EULER (1707 - 1783) und lernte sogar Latein.

In Paris wurde 1794 die *École central des travaux public* (die spätere *École polytechnique*) gegründet, an der hervorragende Mathematiker wie Joseph-Louis LAGRANGE (1736 - 1813) lehrten und publizierten. Sophie GERMAIN konnte dort nicht studieren, denn Frauen war der Zugang verwehrt. Aber sie las Vorlesungsmitschriften und bearbeitete auch Übungsaufgaben, die sie unter dem Pseudonym „*M. LeBlanc*" verfasste und von Bekannten in die *École* bringen ließ. LAGRANGE war von den Leistungen des „Herrn *LeBlanc*" so angetan, dass er diesen kennenlernen wollte. So erfuhr er, dass Herr *LeBlanc* in Wahrheit eine Frau war, schätzte und respektierte ihre Arbeit aber auch weiterhin, was damals überhaupt nicht selbstverständlich war.

Im Jahre 1804 begann Sophie GERMAIN einen Briefwechsel mit dem berühmten Mathematiker Carl Friedrich GAUSS (1777 - 1855) über zahlentheoretische Probleme, wobei sie sich wieder als *M. LeBlanc* ausgab. Ihre Ideen beeindrucken GAUSS und er lobte ihre Arbeit sehr vor Kollegen. Als Braunschweig, die Heimatstadt von GAUSS, französisch besetzt wurde, fürchtete Sophie GERMAIN, ihm würde es ähnlich ergehen wie ARCHIMEDES und bat einen Offizier, sich nach dem Wohlergehen von GAUSS zu erkundigen. Der Offizier berichtete GAUSS, er sei von *Mlle*. GERMAIN geschickt. Daraufhin klärte Sophie GERMAIN ihre wahre Identität auf. Der Briefwechsel wurde dennoch fortgesetzt.

Neben ihrer Arbeit auf dem Gebiet der Zahlentheorie, bei der wohl ihre Ausführungen zu FERMAT's letztem Satz die bedeutendsten sind, beschäftigte sich Sophie GERMAIN mit der Elastizitätstheorie. Das *Institut de France* schrieb 1809 einen Wettbewerb auf diesem Gebiet aus. Der einzige eingereichte Beitrag bis 1811 stammte von einer Frau: Sophie GERMAIN. Der Preis wurde ihr aber erst 1815, nach zweimaliger Verlängerung des Wettbewerbs, zugesprochen.

Sophie GERMAIN arbeitete weiter auf mathematischem Gebiet, auch als sie 1829 an Brustkrebs erkrankte. Sie beendete bis 1831 einige Aufsätze über Zahlentheorie und Differentialgeometrie. Am 27. Juni 1831 starb sie in Paris. Auf ihrem Totenschein wird sie als *rentier*, nicht etwa als Mathematikerin bezeichnet.

Sophie GERMAIN hatte es schwer auf ihrem mathematischen Weg, da sie keinen Zugang zu wissenschaftlichen Institutionen hatte. Die Kritik ihrer wenigen Lehrer beschränkte sich weitgehend auf Lob. Ihre Ideen in der Elastizitätstheorie waren von großer Bedeutung. Sie wurden von Siméon POISSON (1781 - 1840) aufgegriffen und weiterentwickelt, wobei er in seinen Veröffentlichungen verschwieg, dass die Grundlagen seiner Ergebnisse von Sophie GERMAIN stammten.

Sophie GERMAIN gilt als eine der wichtigsten Mathematikerinnen vor Sonja KOVALEVSKAJA (1850 - 1891). In Paris trägt heute ihr zu Ehren eine Schule und eine Straße ihren Namen. Ein mathematischer Satz und eine Klasse von Primzahlen sind nach ihr benannt. Andererseits taucht ihr Name nicht in der Liste am Eiffelturm auf, in der „alle" ForscherInnen auf dem Gebiet der Elastizitätstheorie verzeichnet sind.

Quellen: [Bilder], [Daten], [GrC], [Swi]

Sophie GERMAIN und FERMAT's letzter Satz

Vorüberlegungen. Zum Beweis von FERMAT's letztem Satz ist zu zeigen, dass es keine positiven, ganzzahligen Lösungen x, y, z für die Gleichung $x^n + y^n = z^n$ für $n > 2$ gibt. Eine einfache Überlegung ergibt, dass für ungerade Zahlen $n > 2$ die folgende Aussage äquivalent zu FERMAT's letztem Satz ist: Es gibt keine ganzzahlige Lösung $x, y, z \neq 0$ zu der Gleichung $x^n + y^n + z^n = 0$.

Sophie GERMAIN gelangen wichtige Ergebnisse zu FERMAT's letztem Satz, indem sie ganz spezielle Primzahlen untersuchte, die später nach ihr benannt wurden:

Definition. Eine Primzahl p heißt GERMAIN'sche Primzahl, falls auch $(2p+1)$ eine Primzahl ist.

Beispiel. Die Zahlen $2, 3, 5, 11, 23, 29$ sind GERMAIN'sche Primzahlen.

Lemma. Sei p eine GERMAIN'sche Primzahl und seien $a, x, y, z \in \mathbb{Z}\setminus\{0\}$. Dann gilt:
(1) $a^p \equiv \pm 1 \bmod (2p+1)$ oder $a^p \equiv 0 \bmod (2p+1)$
(2) Aus $x^p + y^p + z^p = 0$ folgt, dass x, y oder z durch $(2p+1)$ teilbar ist.

Beweis. Die Aussage (2) ist eine direkte Konsequenz aus der Aussage (1). Letztere folgt sofort mit dem sogenannten „kleinen" Satz von FERMAT:

Satz von FERMAT. Sei p eine Primzahl und a eine ganze Zahl. Dann gilt $a^p \equiv a \bmod p$. Anders gesagt: Entweder gilt $a \equiv 0 \bmod p$, oder $a^{p-1} \equiv 1 \bmod p$.

Sophie GERMAIN untersuchte also die Gleichung $x^p + y^p + z^p = 0$, wobei p eine GERMAIN'sche Primzahl war und $x, y, z \in \mathbb{Z}\setminus\{0\}$. Zwar konnte sie die Unlösbarkeit der Gleichung nicht beweisen, aber sie konnte mögliche Lösungen genauer charakterisieren:

Satz. Sei $p \neq 2$ eine GERMAIN'sche Primzahl und seien $x, y, z \in \mathbb{Z}\setminus\{0\}$ mit $x^p + y^p + z^p = 0$. Dann ist x, y oder z durch p teilbar.

Beweisidee. Ohne Einschränkung nimmt man an, x, y und z seien paarweise teilerfremd. Dann betrachtet man die Gleichungen

$$-x^p = (y+z)\,(y^{p-1} - y^{p-2}z + y^{p-3}z^2 - \cdots + z^{p-1}) \qquad a_1 := (y+z) \qquad a_2 := (y^{p-1} - y^{p-2}z + y^{p-3}z^2 - \cdots + z^{p-1})$$
$$-y^p = (z+x)\,(z^{p-1} - z^{p-2}x + z^{p-3}x^2 - \cdots + x^{p-1}) \qquad b_1 := (z+x) \qquad b_2 := (z^{p-1} - z^{p-2}x + z^{p-3}x^2 - \cdots + x^{p-1})$$
$$-z^p = (x+y)\,(x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots + y^{p-1}) \qquad c_1 := (x+y) \qquad c_2 := (x^{p-1} - x^{p-2}y + x^{p-3}y^2 - \cdots + y^{p-1})$$

und untersucht die Faktoren a_1, a_2, b_1, b_2, c_1 und c_2. Nimmt man an, eines der Paare a_1, a_2 oder b_1, b_2 oder c_1, c_2 hat einen gemeinsamen Teiler, so läßt sich schnell zeigen, dass dieser Teiler $\pm p$ sein muss. Daraus folgt schließlich, dass x, y oder z von p geteilt wird. Wesentlich schwieriger ist der Fall, dass keines der Paare a_1, a_2 oder b_1, b_2 oder c_1, c_2 einen gemeinsamen Teiler hat. Hier stellt man fest, dass $a_1, a_2, b_1, b_2, c_1, c_2$ alle p-te Potenzen sind und führt durch geschickte Umformungen unter Ausnutzung des Lemmas einen Widerspruch herbei.

Sicherlich war das Ergebnis von Sophie GERMAIN ein großer Fortschritt, aber leider fallen viele Primzahlen nicht in die Klasse der GERMAIN'schen Primzahlen: So kann der obige Satz beispielsweise *nicht* für $p = 7, 13, 17, 19$ angewendet werden.
Aber es gelang Sophie GERMAIN, durch eine leichte Änderung der Voraussetzungen ein stärkeres Ergebnis zu erzielen:

Satz von Sophie GERMAIN. Sei $p \neq 2$ eine Primzahl und seien $x, y, z \in \mathbb{Z}\setminus\{0\}$ mit $x^p + y^p + z^p = 0$. Weiter gebe es eine „Hilfsprimzahl" q mit folgenden Eigenschaften:
(1) Aus $x^q + y^q + z^q = 0$ folgt, dass x, y oder z durch q teilbar ist.
(2) $a^p \equiv p \bmod q$ ist unmöglich für jedes $a \in \mathbb{Z}\setminus\{0\}$.
Dann ist x, y oder z durch p teilbar.

Offenbar stellt der Satz von Sophie GERMAIN eine echte Verallgemeinerung ihres Ergebnisses für GERMAIN'sche Primzahlen dar. Der Beweis läuft fast analog, nur das obige Lemma kann nicht angewendet werden. Ein „Ersatz" dafür ist die Voraussetzung (2).

Sophie GERMAIN schaffte es, für jede ungerade Primzahl $p < 100$, eine passende „Hilfsprimzahl" zu finden, welche die Bedingungen aus dem Satz von Sophie GERMAIN erfüllt. Somit konnte sie in gewisser Weise die „Lösungsmenge" der Gleichung $x^p + y^p + z^p = 0$ „einschränken". (LEGENDRE benutzte später ihren Satz, um ein entsprechendes Ergebnis für ungerade Primzahlen kleiner als 197 zu erhalten).

Beispiel. Betrachte den Fall $p = 7$. Offenbar ist p keine GERMAIN'sche Primzahl, denn $(2 \cdot 7 + 1) = 15$ ist nicht prim. Untersuche, ob die Primzahl $(4 \cdot 7 + 1) = 29$ als „Hilfsprimzahl" geeignet ist. Beachte dazu: Es gibt für jede ganze Zahl a eine Zahl $b \in \{0, \pm 1, \pm 12\}$, so dass $a^7 \equiv b \bmod 29$. Damit kann man sich leicht überlegen, dass alle Voraussetzungen des Satzes von Sophie GERMAIN erfüllt sind.

Quelle: [Edw]

Einige Stationen in der Geschichte eines mathematischen Problems

Um 500 v. Chr.	Der berühmte „Satz des PYTHAGORAS" (PYTHAGORAS lebte etwa 569 - 475 v. Chr.) wird fester Bestandteil des mathematischen Wissens. Die Pythogoräer können zeigen, dass die Gleichung $x^2 + y^2 = z^2$ unendlich viele ganzzahlige Lösungen hat, die sogenannten *pythagoräischen Zahlentripel*.
Um 1630	Pierre de FERMAT (1601-1665) notiert bei der Lektüre des Lehrwerkes *Arithmetica* von DIOPHANT (etwa 200 - 284) auf den Rand des Buches einen Satz, den wir heute „FERMAT's letzten Satz" nennen und so formulieren können:

Die Gleichung $x^n + y^n = z^n$ hat für $n > 2$ keine positive, ganzzahlige Lösung.

	FERMAT notiert auch, er habe einen „wahrhaft wunderbaren Beweis", doch sei „dieser Rand hier zu schmal, um ihn zu fassen".
1670	FERMAT's Sohn veröffentlicht die *Arithmetica* mit den Randnotizen seines Vaters. Ein Beweis für FERMAT's letzten Satz findet sich dort nicht.
Um 1750	Leonhard EULER (1707 - 1783) leistet einen wichtigen Beitrag für den Beweis der Fälle $n = 3$ und $n = 4$. Für $n > 4$ kann er seine Argumente aber nicht mehr anwenden.

Nun muss FERMAT's Vermutung „nur noch" für den Fall, dass n eine ungerade Primzahl ist, bewiesen werden, denn jedes $n > 2$ hat eine Darstellung $n = m \cdot k$, wobei k entweder eine ungerade Primzahl oder 4 ist und m eine natürliche Zahl. Damit kann es keine Lösung der Gleichung $x^n + y^n = z^n$ bzw. $(x^m)^k + (y^m)^k = (z^m)^k$ geben, wenn es keine Lösung der Gleichung $x^k + y^k = z^k$ gibt.

Um 1805	Sophie GERMAIN (1776 - 1831) gelingt ein wichtiger Schritt zur Lösung von FERMAT's Problem.
Um 1830	Johann Peter Gustav Lejeune DIRICHLET (1805 - 1859) und Adrien-Marie LEGENDRE (1752 - 1833) beweisen mit Hilfe der Überlegungen von Sophie GERMAIN den Fall $n = 5$, DIRICHLET gelingt ein Beweis für $n = 14$.
1839	Gabriel LAMÉ (1795 - 1870) ergänzt Sophie GERMAINS Verfahren und führt den Beweis für $n = 7$.
1847	LAMÉ und Augustin Louis CAUCHY (1789 - 1857) kündigen am 01.03.1847 beide an, innerhalb der nächsten Wochen das FERMAT'sche Problem zu lösen und liefern sich ein wahres Kopf-an-Kopf-Rennen um den Ruhm, der dem „Gewinner" sicher wäre. Ernst Eduard KUMMER (1810 - 1893) beendet das Wettrennen, indem er auf einen logischen Fehler in den Ausführungen von LAMÉ und CAUCHY hinweist.

KUMMER kann das Problem darauf beschränken, für n „nur noch" die sog. „irregulären Primzahlen" zu betrachten, von denen es aber unendlich viele gibt, wie Johan JENSEN (1859 - 1925) im Jahre1915 zeigt.

1908	Der WOLFSKEHL-Preis wird ausgelobt: Wer FERMAT's letzten Satz beweisen kann, dem winkt ein stattlicher Betrag. Unzählige Laien-MathematikerInnen und HobbytüftlerInnen versuchen sich vergebens am nun so schmackhaft gemachten Beweis.
1931	Kurt GÖDEL (1931-1978) beweist, dass es immer mathematische Aussagen geben wird, die zwar wahr sind, aber nicht bewiesen werden können (sogenannte „unentscheidbare Sätze"). Das ist ein Schock für die MathematikerInnen. Ist vielleicht auch FERMAT's letzter Satz unentscheidbar?
Nach 1945	ComputerwissenschaftlerInnen und MathematikerInnen führen mit Hilfe des Computers den Beweis für viele einzelne irreguläre Primzahlen n. In den achtziger Jahren wird so gezeigt, dass FERMAT's Vermutung für n bis *25 000* wahr ist. (Diese Grenze wurde schließlich bis *4.000.000* vorgeschoben.)
1955	Yakuta TANIYAMA (1927-1958) und Goro SHIMURA (Princeton University, s. [Pri]) tragen auf einem internationalen Symposium in Tokio die überraschende Vermutung vor, dass zwei völlig unterschiedliche mathematische Konzepte, die „Modulformen" und die „elliptischen Kurven", in einer sehr einfachen und starken Beziehung zueinander stehen. Noch ahnt niemand, dass diese TANIYAMA–SHIMURA–Vermutung eng mit FERMAT's letztem Satz zusammenhängt.
1984	Gerhard FREY (Universität Essen, s. [Fre]) skizziert eine Beweisidee dafür, dass FERMAT's letzter Satz wahr sein muss, wenn die Vermutung von TANIYAMA und SHIMURA wahr ist. Leider ist die Vervollständigung des Beweises schwerer, als FREY dachte. Viele MathematikerInnen versuchen, FREY's Idee zu retten.
1986	Kenneth RIBET (University of California, Berkeley, s. [Rib]) erbringt einen richtigen Beweis für FREY's Vermutung.

Nach dem Ergebnis von FREY steht nun fest: Ein Beweis der TANIYAMA–SHIMURA–Vermutung liefert auch einen Beweis von FERMAT's letztem Satz.

1986 – 1993	Als Andrew WILES (Princeton University, s. [Pri]) erfährt, dass FREY's Idee bewiesen ist, will er die TANIYAMA–SHIMURA–Vermutung beweisen. Er benutzt bewährte mathematische Konzepte, z.B. die Ergebnisse von Évariste GALOIS (1811-1832), entwickelt aber vor allem wichtige neue Ideen. Schließlich glaubt er, die TANIYAMA–SHIMURA–Vermutung beweisen zu können.
Juni 1993	WILES trägt in Cambridge auf einer Konferenz seine Ergebnisse vor. Die MathematikerInnen in aller Welt sind begeistert, das Ereignis schlägt große Wogen in der Presse. Aber der Beweis – 200 Seiten lang – muss noch geprüft werden...
August 1993	Nicholas KATZ (Princeton University, s. [Kat]), ein Gutachter des Beweises, findet ein zuerst harmlos erscheinendes Problem, das sich aber schnell als elementarer Fehler herausstellt.
August 1993 bis September 1994	WILES arbeitet intensiv an der Rettung seines Beweises, zunächst versucht er es allein. Schließlich zieht der die Hilfe von Richard TAYLOR (Harvard University, s. [Tay]) hinzu, aber die Arbeiten liefern nicht das gewünschte Resultat. WILES will schon fast aufgeben, als ihm im September 1994 doch noch die richtige Idee kommt. Der nun lückenlose und auf 130 Seiten geschrumpfte Beweis wird veröffentlicht.

Die TANIYAMA–SHIMURA–Vermutung und damit auch Fermat's letzter Satz sind bewiesen.

Juni 1997	Der WOLFSKEHL-Preis wird an Andrew Wiles verliehen.
1998	Andrew WILES erhält beim *International Congress of Mathematicians* in Berlin einen extra für ihn geschaffenen, der FIELDS-Medaille ähnlichen Preis – er kann die FIELDS-Medaille nicht erhalten, weil er „zu alt" ist.

Quellen: [Daten], [Fie], [Sin], [OCR]

Quellen:

[Bilder] *Germain Portraits*. http://www-groups.cs.st-and.ac.uk/~history/PictDisplay/ Germain.html. Februar 2001.
[Daten] *Index of Biographies*. http://www-groups.cs.st-and.ac.uk/~history/ BiogIndex.html. Februar 2001.
[Edw] Edwards, Harold M.; *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*. New York: Springer-Verlag, 1977, S. 23 und S. 61-65.
[Fie] *ICM'98 Welcome Page*. http://elib.zib.de/ICM98/. Februar 2001.
[Fre] *Institute for Experimental Mathematics*. http://www.exp-math.uni-essen.de/zahlentheorie/Zahlentheorie.html. Februar 2001.
[GrC] Grinstein, Louise S.; Campbell, Paul J.; *Women of Mathematics. A Bibleographic Sourcebook*. Greenwood Press, 1987, S. 47-56.
[Kat] Katz, N. M.; *Nicholas M. Katz's Home Page*. http://www.math.princeton.edu/~nmk/. Februar 2001.
[OCR] O'Connor, J. J.; Robertson, E. F.; *Fermat's last theorem*. http://www-groups.cs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html. Februar 2001.
[Pri] *Faculty*. http://www.math.princeton.edu/~web/faculty.html. Februar 2001.
[Rib] Ribet, K.; *Kenneth A. Ribet*. http://www.math.berkeley.edu/~ribet/. Februar 2001.
[Sin] Singh, Simon; *Fermats Letzter Satz. Die abenteuerliche Geschichte eines mathematischen Rätsels*. Deutscher Taschenbuch Verlag, 2000.
[Swi] Swift, Amanda; *Sophie Germain*. http://www.agnesscott.edu/lriddle/women/ germain.htm. Februar 2001.
[Tay] Taylor, R.; *Richard Taylor's Home Page*. http://abel.math.harvard.edu/~rtaylor/. Februar 2001.

Barbara Langfeld • Carl von Ossietzky Universität Oldenburg • Februar 2001