5-1996

History of Fermat's Last Theorem

Amanda Brown
Utah State University

HISTORY OF FERMAT'S LAST THEOREM

by

Amanda Brown

Thesis submitted in partial fulfillment
of the requirements for the degree

of

UNIVERSITY HONORS
WITH DEPARTMENT HONORS

in

Mathematics

UTAH STATE UNIVERSITY
Logan, UT

1996

HISTORY OF FERMAT'S LAST THEOREM

AMANDA BROWN

1 Pierre de Fermat

Around 1637, Pierre de Fermat made a now-famous mathematical conjecture. However, Fermat's conjecture neither began nor ended with him. Fermat's last theorem, as the conjecture is called, has roots approximately 3600 years old. The proof of the theorem was not realized until 1994, over 350 years after it was proposed by Fermat.

Fermat was born in France in 1601. He was a judge and amateur mathematician. Fermat also wrote poetry in various languages ("Fermat's Last Theorem", 1993). He spent seventeen years of his life in parliament as King's Councilor. When Fermat wasn't working on other things, he spent time on mathematics. He was one of the greatest mathematicians ever (Mielke, 1989). Fermat did several things in mathematics, his "last theorem" being only one.

In his last theorem Fermat conjectured that the equation $x^n + y^n = z^n$, where $n > 2$, has no positive integer solutions. A familiar equation of a similar form is $x^2 + y^2 = z^2$. This equation is part of the Pythagorean theorem, where x, y, and z are the lengths of the sides of a right triangle, z being the length of the hypotenuse. There are clearly positive integer solutions to this equation, such as $x = 3$, $y = 4$, and $z = 5$.

About 3600 years ago, the Babylonians found a formula that provides solutions to the equation $x^2 + y^2 = z^2$. The ancients realized that there are an infinite number of solutions to the equation. Sometime in the period of the second through the

fourth century, a Greek mathematician by the name of Diophantus proved that the Babylonian formula provides all the positive integers, x, y, and z, that satisfy the equation $x^2 + y^2 = z^2$ ("Fermat's Last Theorem", 1993). Diophantus wrote a book entitled Arithmetica. It was in the margin of Fermat's copy of this book that he wrote his famous conjecture. And, in his own words, Fermat's last theorem is:

> To divide a cube into two cubes, a fourth power, or in general any power whatever into two powers of the same denomination above the second is impossible, and I have assuredly found an admirable proof of this, but the margin is too narrow to contain it. (Fey, 1989, pg. 79)

Fermat claimed to have a proof of his theorem but failed to produce it before his death. He basically didn't publish any of his work. Also, it's interesting to note that Fermat rarely met with other mathematicians ("Fermat's Last Theorem", 1993). Fermat did, however, prove his theorem for the case when $n = 4$.

2 Early Work on Fermat's Last Theorem

Since Fermat, thousands of mathematicians have worked on proving the theorem. Most have failed. However, several mathematicians have made progress by proving the theorem for some values of n. In the eighteenth century, Leonard Euler proved that there are no positive integer solutions to the equation $x^3 + y^3 = z^3$. So Euler proved Fermat's theorem for the case $n = 3$. Then, in the nineteenth century Adrien Marie Legendre and P.G. Lejeune Dirichlet independently proved the theorem for $n = 5$. Gabriel Lamé proved it for $n = 7$, in 1839. Ernst Kummer, a German mathematician, produced a proof for Fermat's last theorem in 1843. His proof was found to be flawed, however. Kummer did prove the theorem for "most small n" (Fey, 1989). He also proved that Fermat's theorem is true when n is a regular prime.

In the twentieth century, more work has been done in relation to Fermat's theorem.

In the 1970's, with the use of computer, Fermat's theorem was shown true for all n less that 125,000. Then, in 1983, Gerd Faltings proved that there can only be a finite number of solutions to the equation $x^n + y^n = z^n$, where $n > 2$ (Science News, 1987).

3 Sophie Germain

Sophie Germain was also one of the people who have worked on Fermat's theorem. She was a French woman who lived at the end of the eighteenth and the beginning of the nineteenth century. She was interested in mathematics, and read books on the subject. However, being a woman, her interest was discouraged by her family. They tried not giving her heat or light in her room at night. That didn't stop Sophie, however. She would light candles and wrap herself in blankets and work on mathematics. Her family finally gave up.

Sophie corresponded with mathematicians of her time. Since she was a woman, she didn't use her own name. LeBlanc was the surname she used. One very important mathematician that Germain corresponded with was Gauss. In 1807, Gauss found out that LeBlanc wasn't a man. Gauss said that it didn't matter much to him.

Sophie Germain was one of the first people to do work on Fermat's theorem as it was. She made progress on a proof for a group of n ("Fermat's Last Theorem", 1993). Sophie Germain was an interesting piece in the "Fermat puzzle".

4 Yoichi Miyaoka

Yoichi Miyaoka was among the many mathematicians to produce a proof of Fermat's last theorem. For his proof, Miyaoka used "arithmetic algebraic geometry".

> In this discipline, mathematicians look at surfaces that result when only integer solutions of equations are considered. Miyaoka tried to show that an inequality, or bound, that applies in algebraic geometry also

> fits an analogous case for equations with integer solutions. (Peterson, 1988, pg. 230)

On February 26, 1988, Miyaoka presented his proof before a group of mathematicians. The word about Miyaoka's "proof" spread. The proof turned out to be flawed, however. Differing opinions existed about the attention given to Miyaoka's proof by the press. Some people felt that news of Miyaoka's proof should not have been published until the proof's validity was confirmed. Some thought it was good for the public to see the "human component" of mathematics (Vanden Eynden, 1989).

5 Taniyama's Conjecture

It wasn't until September of 1994 that a valid proof of the theorem was finally given. The proof was the work of Andrew Wiles and Richard Taylor. However, many events in mathematics lead to the proof.

One event in mathematics that became important in proving Fermat's theorem occurred in 1954. In that year Yutaka Taniyama made a conjecture about *elliptic curves*. Goro Shimura further developed Taniyama's conjecture. In the 1980's, Gerhard Frey conjectured that Taniyama's conjecture was linked to Fermat's last theorem. Then, in 1986, Kenneth Ribet proved that Taniyama's conjecture implies Fermat's last theorem (Kolata, 1993).

An equation that can be written in the form $y^2 = (x)(x-a)(x-b)$, where a and b are integers other than zero and $a \neq b$, provides an elliptic curve. Consider when $y^2 - (x)(x-a)(x-b)$ is equal to an even number (multiple of 2), a multiple of 3, a multiple of 5, and so on for the primes. We could call the "number of times" that $y^2 - (x)(x-a)(x-b)$ is a multiple of 2, $N[2]$, the number of times it's a multiple of 3, $N[3]$, and so on. Now, if we look at the sequence $N[2]$, $N[3]$, $N[5]$, $N[7]$,..., and there is a certain type of pattern to it, the elliptic curve given by $y^2 = (x)(x-a)(x-b)$ is called *modular*. Taniyama's conjecture was that all elliptic curves are modular.

Frey linked Fermat's theorem and Taniyama's conjecture in the following way: If Fermat's theorem states that there are no solutions to the equation $a^n + b^n = c^n$, consider the elliptic curve given by $y^2 = (x)(x - a^n)(x - b^n)$. Frey thought that the elliptic curve was probably not modular. But, if Taniyama was right, all elliptic curves are modular. If the curve given by $y^2 = (x)(x - a^n)(x - b^n)$ was not modular, and Taniyama's conjecture was true, then the curve must not exist, and Fermat's theorem must be true. Something appeared to be incomplete about Frey's work, however.

Jean-Pierre Serre, played a role in this part of the puzzle. Serre stated that if his two conjectures were proven, then Fermat's theorem would follow from Taniyama'a conjecture. Ribet proved Serre's two conjectures ("Fermat's Last Theorem", 1993).

6 Andrew Wiles

On June 23, 1993, Andrew Wiles, an English mathematician, announced a proof of Fermat's last theorem. In his work, Wiles proved a form of the Taniyama conjecture and which implies Fermat's theorem. Wiles made the announcement of his proof during the final lecture in a series he gave at Cambridge University. Electronic mail messages about the surprising proof were sent throughout the world (Kolata, 1993). An article about Wiles' proof was featured on the front page of the New York Times. It was an exciting time in mathematics.

Some authors even compared this monumental event to the Chicago Bulls winning an NBA championship. Dissertations were burned and textbooks were thrown. People were yanked from their cars and given story problems to solve. Police were apparently expecting some violence. They prevented students from tipping cars over on a road in Chicago (Harper's, 1993).

Wiles' proof was 100 pages in length. The proof was extremely technical and complicated. Some estimated that, of mathematicians, only a tenth of one percent

could comprehend the proof (Kolata, 1993).

Wiles' initial proof turned out to be incomplete. A gap was found, and Wiles, still determined, continued to work on a complete proof.

A key part of Wiles' work was proving a "class-number formula". Wiles had looked at gluing Hecke rings together to prove the formula, but forsook this approach in 1991. At that time Wiles began to try and prove the formula with an Euler system. The part of Wiles' 1993 proof that was flawed was the one involving the Euler system.

Sometime after the gap was discovered, Wiles decided to try his original idea of gluing Hecke rings together to prove the class-number formula. However, in August of 1994, Wiles became frustrated and, in his own words, "resigned at that point to a long haul (Cipra, 1996, p.8)." Richard Taylor, who was working with Wiles, suggested looking at Euler systems again. While studying why the Euler system would not work, Wiles had a marvelous idea of how he could use his original idea involving Hecke rings to prove the theorem. Wiles' idea came to him on September 19, 1994 (Cipra, 1996).

A valid proof of Fermat's last theorem was finally given. The proof was the work of both Andrew Wiles and Richard Taylor. In May of 1995 the proof was published in the Annals of Mathematics.

7 Wiles' Proof

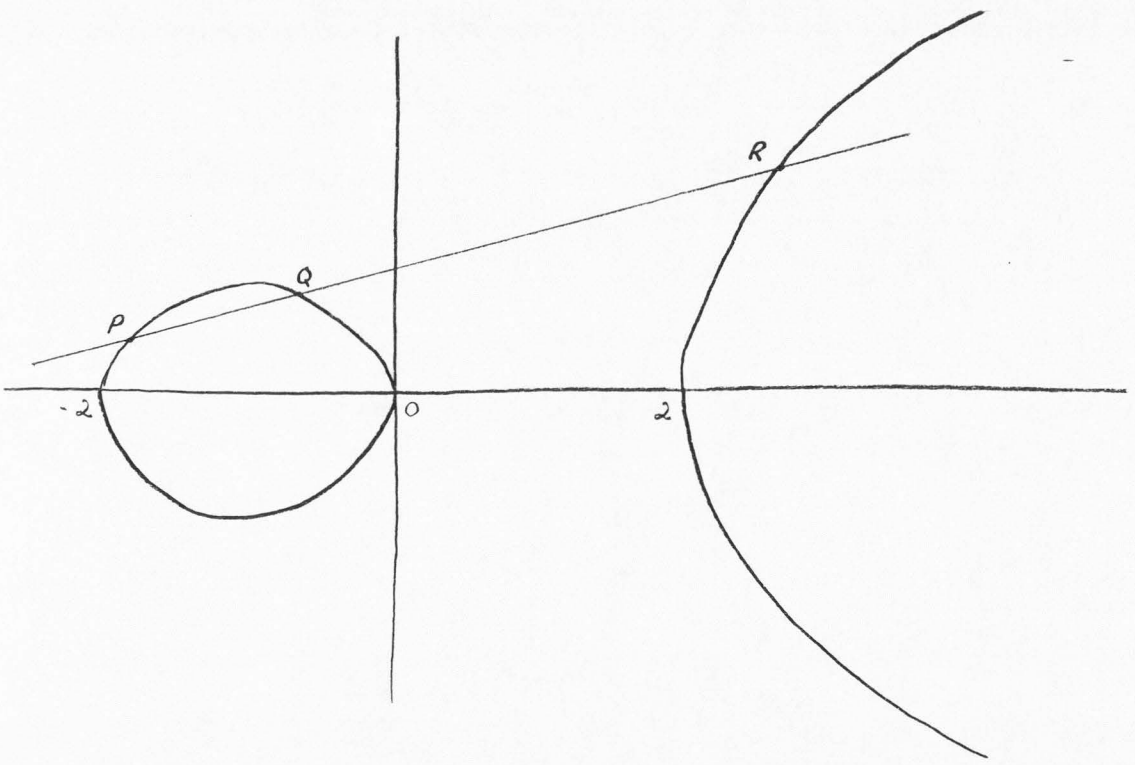
There are three main components to the proof of Fermat's last theorem given by Wiles and Taylor. These are: elliptic curves, modular forms, and Galois representations.

7.1 Elliptic Curves

Let $f(x)$ be a cubic polynomial. If $f(x) \in \mathbb{Z}[x]$, that is if $f(x)$ has integer co-

efficients, and $f(x)$ has distinct roots, then $y^2 = f(x)$ provides an elliptic curve. We call the elliptic curve E. Consider the example $E : y^2 = x^3 - 4x$. Since $y^2 = (x)(x-2)(x+2)$, the roots of E are 0, 2, and -2.

Now, $E(K) = \{(x,y) \in K^2 : y^2 = f(x)\} \cup \{\infty\}$, where K is a field. That is, the *K-rational points*, $E(K)$, are the set of points in $K \times K$ that satisfy the elliptic curve alongwith a point at infinity. The graph of $E(\mathbb{R})$ for our example is given below.



In general $E(K)$ is a group. If $P, Q, R \in E(K)$ are collinear, then $P + Q + R = 0$. So, for any points $P, Q \in E(K)$, $P + Q = -R$.

Frey provided a relationship between Fermat's theorem and elliptic curves. In particular, Frey associated an elliptic curve to a non-trivial solution of the equation $x^n + y^n = z^n$. This elliptic curve represents a counterexample to the theorem.

7.2 Galois Representations

We should note that $E(\mathbb{C})$ provides a torus. Now, let $P(x, y)$ be a point satisfying the equation for an elliptic curve E. Let $E[n] = \{P \in E(\mathbb{C}) \ : \ nP = 0\}$. $E[n]$ is a subgroup of $E(\mathbb{C})$, and $E[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n$.

For all $P(x, y) \in E[n]$, x and y are algebraic numbers. That is x is a zero of some polynomial with rational coefficients, and so is y. Let $\mathrm{Aut}(E[n])$ be the set of automorphisms on the group $E[n]$. So $\mathrm{Aut}(E[n])$ is the set of all group isomorphisms from $E[n]$ into $E[n]$.

Now, let G be the set of all automorphisms on the field of algebraic numbers. Note that elements in $E[n]$ are permuted by the action of G. Let $\rho_n : G \to \mathrm{Aut}(E[n])$. The group $\mathrm{Aut}(E[n])$ is isomorphic to the set of invertible two-by-two matrices with entries in $\mathbb{Z}/n$. That is, $\mathrm{Aut}(E[n]) \cong GL(2, \mathbb{Z}/n)$, and ρ_n is a *Galois representation.*

7.3 Modular Forms

It is possible to produce a Galois representation from a modular form. If an elliptic curve E can be produced from a modular form, then E is *modular.*

Taniyama conjectured that all elliptic curves over the rational numbers are modular. If Taniyama's conjecture is true, then the elliptic curve given by Frey is modular. However, Ribet found that if the curve were modular that it could be produced from a certain modular form that does not exist. Hence, if Taniyama's conjecture is true, then Fermat's last theorem is true. In order to prove Fermat's last theorem, Wiles proved that Taniyama's conjecture is true for the elliptic curves given by Frey (Boston, 1995).

8 Why Try?

Why did so many people attempt to prove a theorem that was so difficult to prove?

Reasons may vary. In the time since Fermat proposed his theorem, a few prizes have been made available for a proof of it. In 1815 and in 1860, a gold medal and 300 francs were offered by the French Academy of Sciences. Then in 1908, 100,000 marks were offered by the German Academy of Sciences (Kolata, 1993). Money seems to have been a factor contributing to the number of people who have attempted proofs.

Some people may have tried to prove Fermat's theorem in an attempt to gain fame. However, this was not the case with Andrew Wiles. The shy Wiles has tried to avoid the press. He even refused to appear in an add for Gap jeans (Jackson, 1994). Wiles claims to have been intrigued by the theorem when he was just 10 years old ("Fermat's Last Theorem", 1993). After spending over seven years of his life proving the theorem, Wiles realized his boyhood dream.

References

[1] Begley, S., Ramo, J.C. (July 5, 1993). New answer for an old question: The proof's in the putting. *Newsweek.* 122:52-3.

[2] Boston, N. (March, 1995). *The College Mathematics Journal.* 26:100-105.

[3] Cipra, B. (1996). Fermat's theorem - At last! *What's Happening in the Mathematical Sciences 1995-1996.* 3:2-13.

[4] Closing in on Fermat's last theorem (June 20, 1987). *Science News.* 131:397.

[5] Faltings, G. (July, 1995). The proof of Fermat's last thorem by R. Taylor and A. Wiles. *Notices of the American Mathematical Society.* 42:743-6.

[6] Fey, J. (1989). Fermat's last theorem. *Historical Topics for the Mathematics Classroom.* VA: National Council of Teachers of Mathematics. Pgs. 79-80.

[7] Fermat, Pierre de (1994). *Encarta.*

[8] The Fermat riots (Sep, 1993). *Harper's.* 287:19.

[9] Jackson, A. (March, 1994). Update on proof of Fermat's last theorem: Gap appears in proof but experts laud Wiles' accomplishment. *Notices of the American Mathematical Society.* 41:185-6.

[10] Kolata, G. (June 24, 1993). At last, shout of 'Eureka!' in age-old math mystery. *New York Times.*

[11] Mielke, P.T. (1989). Pierre de Fermat. *Historical Topics for the Mathematics Classroom.* VA: National Council of Teachers of Mathematics. Pgs. 410-3.

[12] Murty, R. (Sep, 1993). A long standing mathematical problem is solved: Fermat's last theorem. *CMS Notes.* Pgs. 16-20.

[13] Peterson, I. (March 19, 1988). Fermat's last theorem: A promising approach. *Science News.* 133:180-1.

[14] Peterson, I. (April 9, 1988). Doubts about Fermat solution. *Science News.* 133:230.

[15] Singer, J. (1994). Fermat's last theorem. *Encarta.*

[16] Vanden Eynden, C. (Nov, 1989). Fermat's last theorem: 1637-1988. *Mathematics Teacher.* Pgs. 637-40.

[17] Video: "Fermat's Last Theorem: The Theorem and Its Proof: An Exploration of Issues and Ideas" (1993). Berkeley, CA: *Mathematical Sciences Research Institute.*

[18] Andrew Wiles (Dec 27, 1993 - Jan 3, 1994). *People Weekly.* 40:104.