Eric Williams

Math 3010

4/25/16

The History, Impact, and Proof of Fermat's Last Theorem

In 1637, French mathematician Pierre de Fermat made a conjecture that is now one of the most well-known math problems in the history of mathematics. The conjecture was first mentioned in the margin of Fermat's copy of *Arithmetica* by the Greek mathematician Diophantus where he wrote in Latin:

> *"It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain."* [1]

Although Fermat wrote that he had discovered a demonstration of this conjecture, whatever proof attempt he had made was either lost or wrong, as no further writings of it by Fermat have ever been seen. For the next 358 years, mathematicians would work to prove this theorem, and they would push the boundaries of mathematics along the way. In particular, algebraic number theory was greatly developed as mathematicians attempted to prove Fermat's Last Theorem, in addition to the development of modularity of elliptic curves which was used for its eventual proof. In this paper I will further discuss the history of Fermat and his Last Theorem, the historical impact of the theorem, attempted proofs throughout history, the mathematical developments that resulted from the attempted proofs, and the eventual 20th century proof of the theorem by Andrew Wiles.

Pierre de Fermat was born in 1601 at Beaumont-de-Lomagne, France. Not much is known about his childhood or early education until he began his higher education in the 1620's at the University of Orléans. There he studied law and eventually earned his civil law degree in 1626; notably, he never studied mathematics formally during his educational career. Instead of immediately taking an interest in mathematics, he served as a civil servant and judge upon graduating in 1626--until he first began his research in mathematics in 1629. Despite his late interest, Fermat began producing revolutionary mathematical theorems immediately upon beginning his work in mathematics, such as his developments on maxima and minima. [2]

Throughout his life, Fermat would make contributions in various branches of mathematics such as analytic geometry, probability, optics, (then unknown) differential calculus, and especially number theory. Besides his Last Theorem, Fermat is also known for proposing his 'Little Theorem' in 1640, which states "that if p is prime and a is any whole number, then p divides evenly into $a^p - a$." Although there is no known written proof by Fermat himself, his Little Theorem was eventually proved and is considered "one of the great tools of number theory still today." [3]

Interestingly enough, it was not uncommon for Fermat to produce conjectures or propose theorems publicly without supplying a proof. Although this may sometimes have been because he didn't have proofs for some of his theorems, the fact that Fermat rarely published his work meant that many of his theorems would be proven by other mathematicians for centuries to come. In fact, a lot of his work was done in secrecy, which was not uncommon for mathematics in Europe in the seventeenth century. Often times, Fermat's secrecy caused disputes with other mathematicians such as René Descartes, who is considered the other leading mathematician of the 17th century along with Fermat. [2] In one particular case, Descartes and Fermat feuded over Fermat's work on minima and maxima--a result of Fermat's secrecy regarding the proof of his methods. When Fermat demonstrated the full proof of his methods, Descartes conceded and remarked:

> *"...seeing the last method that you use for finding tangents to curved lines, I can reply to it in no other way than to say that it is very good and that, if you had explained it in this manner at the outset, I would have not contradicted it at all."*

Because of Fermat's secretive work in mathematics, there are very few modern records of him proving his theorems.

After Pierre de Fermat's death in 1665, his son Clément-Samuel Fermat would spend years compiling and rewriting his father's work. As a result, Fermat's theorems became public, but many of them remained unproven. Mathematicians would spend decades proving all of Fermat's theorems until just one remained--which was thus named Fermat's Last Theorem.

At the time when he first wrote his 'last' theorem, Fermat was presumably reading out of the Greek text *Arithmetica* about Diophantine equations, which are polynomial equations that have two or more unknowns where only integer solutions are considered. The one form of the equation Fermat was interested in was Diophantine's equation $x^n + y^n = z^n$. Upon reviewing the equation, Fermat was able to determine that no integer solutions exist when $n > 2$ while infinitely many solutions exist for n=1 and n=2. Although he had written that he had a proof for his conjecture, most historians agree that either his proof was incorrect, incomplete, or was never written. This is mostly because of the difficulty of the problem in conjunction with the fact that that Fermat would go on to further attempt partial proofs, such as specifically for the case $n = 4$.[1]

Although Fermat's Last Theorem was just a few scrawled sentences in the margin of his copy of *Arithmetica*, numerous mathematicians would attempt to find a proof for the next several centuries. 105 years after Fermat's death, Euler proved there were no solutions for $n = 3$using the technique of infinite descent and assuming a solution to $x^3 + y^3 + z^3 = 0$ (where not all x, y, and z are necessarily positive). Carl Friedrich Gauss also did some work on the problem, providing a unique proof for $n = 3$ as well as proving the $n = 4$ case. However, Gauss was not nearly as interested in proving the general case and considered it trivial, remarking, "I confess that Fermat's

Theorem as an isolated proposition has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of." [5]

Despite Gauss's disinterest in proving the theorem for the general case, his study of the theorem led to him discovering that Diophantine equations "could be solved by extending outside the realm of ordinary integers and into new systems of complex numbers." [6]In fact, it was not uncommon for scholars to make mathematical discoveries while attempting to prove Fermat's Last Theorem. In 1847, Augustin Louis Cauchy and Gabriel Lamé both worked unsuccessfully to prove Fermat's Last Theorem. But regardless of their failure, they did, prompt the mathematicians at the time to further research the nature of complex numbers. In their proofs, Cauchy and Lamé used complex numbers as an extension of the real number system.

However, in their proofs, Cauchy and Lamé used the assumption that complex numbers (such as numbers of the form $a + bi$) can be factored into *unique* sets of primes. But just a few years later Ernst Kummer showed that there are multiple ways in which you can factor complex numbers into primes. For example, the complex number 6 + 0i is equal to both $2\ x\ (\sqrt{2} + i)\ x\ (\sqrt{2} - i)$ and $(1 + \sqrt{5}i)\ x\ (1 - \sqrt{5}i)$.When it was discovered that Cauchy and Lamé's proofs were based on an incorrect assumption of the properties of complex numbers, their proof was discredited. Despite the error, their attempts still provoked a new mathematical perspective for factoring complex numbers; the usefulness of complex systems were seen in a new light. [7]

In addition to developing complex numbers, attempts to solve Fermat's Last Theorem most notably advanced algebraic number theory. For example, Kummer would go on to further research the nature of prime numbers to prove the theorem. As he developed subsets of prime numbers, he was the first mathematician to prove Fermat's Last Theorem for a class of numbers--specifically, the 'regular prime' numbers. He defined the regular primes to be any prime numbers such that the number p is not divisible by the numerator of the Bernoulli numbers ($k = 2, 4, 6, ..., p - 3$). Kummer demonstrated this by showing that if x, y, and z are integers and n is a regular prime, then $x^n + y^n = z^n \rightarrow xyz = 0$.

In addition to his own work, Kummer inspired mathematicians to start research on the irregular primes, as proving Fermat's Last Theorem holds for irregular primes would complete a proof of the theorem. Kummer's work on the theorem further developed algebraic field theory, as his discovery of relative primes inspired his development of what are now called Kummer Fields.

Despite the far-reaching impact of Fermat's Last Theorem on mathematical research for several centuries after Fermat's death, very little of the pre-1900's research led directly to the discovery of the eventual proof in 1994. Because a proof has never been given without algebraic geometry and number theory (which were not accessible in the seventeenth century), it is clear that Fermat could not have developed a proof anything like the one commonly accepted today. Instead, the first complete and correct proof came from the 1980's and 1990's development of modular elliptic curves.

Unrelated to attempting to prove Fermat's last theorem, in 1956 Japanese mathematician Yutaka Taniyama began work on automorphic properties of L-functions of elliptic curves. Together with Goro Shimura, the two mathematicians made a conjecture stating that elliptic curves over the field of rational numbers are related to modular forms (which is now known as the Taniyama–Shimura conjecture, or simply the modularity theorem). Although Taniyama's original idea pertaining to the elliptic curves over arbitrary number fields has yet to be solved, interest in the modularity theorem immediately began spread when Gerhard Frey suggested that the proof of the modularity theorem would imply Fermat's Last Theorem. He stated that if there was a counterexample to Fermat's Last Theorem, then there must exist at least one non-modular elliptic curve--and thus he set out to prove this implication is true (such implication he called the epsilon conjecture). In 1990, the proof was finally accepted after work from Jean-Pierre Serre and Ken Ribet. [9]As such, all that remained to prove Fermat's Last Theorem was a proof of the Taniyama–Shimura conjecture. Enter Andrew Wiles.

Born April 11th, 1953 in Cambridge, England, Andrew Wiles took an early interest in mathematics and particularly in Fermat's Last Theorem. At age 10, Wiles discovered the theorem and dreamed of one day proving it, but like many people charmed by the simplicity of the equation, he quickly learned that the proof was of substantial difficulty and abandoned his hopes to prove it. That is, until 23 years later when he read Ken Ribet's 1986 proof of the epsilon conjecture. [10]

As a PhD student at Clare College, Cambridge, Wiles studied elliptic curves using the Iwasawa theory under John Coates. Upon reading Ribet's proof that Fermat's Last Theorem could be proved using modular of elliptic curves (Wiles's area of expertise), he set out to fulfill his childhood dream of proving the theorem that had stumped mathematicians for 358 years. All that remained was the proof of the modularity theorem, although it was not even certain that proving the theorem was possible. In fact, as his advisor, Coates, discouraged Wiles from working on such a difficult and potentially impossible theorem--but Wiles was undeterred. Over the course of the next six years, Wiles worked by himself in complete secrecy until at last he emerged with a proof of the modularity theorem for semistable elliptic curves, which finally implied Fermat's Last Theorem was true.

On 23 June 1993, Wiles announced his proof in a series of lectures at Cambridge University in England cryptically titled "Elliptic Curves and Galois Representations." At the end of his three part lecture, he was finally able to write "=> FLT." After hundreds of incorrect proofs throughout history, Wiles's work implied Fermat's Last Theorem was true. A shockwave immediately rippled through the mathematical community, and Wiles quickly became a world renowned mathematician. As Ken Ribet said, "the mathematical landscape has changed. You discover that things that seemed completely impossible are more of a reality. This changes the way you approach problems, what you think is possible." [11]

Now all that stood between Wiles and his childhood dream was for peers to check his work on semistable elliptic curves. However, after an intense reviewing of his work, an error was found. In an interview, Wiles remarked on the subject of the error:

> *“I began to realise that this wasn't just a minor difficulty but a fundamental flaw. It was an error in a crucial part of the argument involving the Kolyvagin-Flach method, but it was something so subtle that I'd missed it completely until that point. The error is so abstract that it can't really be described in simple terms. Even explaining it to a mathematician would require the mathematician to spend two or three months studying that part of the manuscript in great detail."* [12]

Wiles would spend the next year back at Princeton University attempting to fix the flaw in his proof with the help of his former student Richard Taylor. Eventually they had another breakthrough and put out another publication that satisfied the mathematics community. Upon its review, the solution was considered sufficient and the proof was finally complete. Fermat’s last unproven conjecture could finally be called a proven theorem.

Upon its completion, Wiles was quick to point out that there was no way his proof was the same as what Fermat’s could have been. When asked if he thought his proof would match Fermat’s, he remarked:

"There's no chance of that. Fermat couldn't possibly have had this proof. It's 150 pages long. It's a 20th-century proof. It couldn't have been done in the 19th century, let alone the 17th century. The techniques used in this proof just weren't around in Fermat's time." [12]

Although the nature of Fermat's original proof will probably forever remain a mystery, his handwritten conjecture in the margin of an ancient text forever changed mathematical history. The problem will go down in history as one of the greatest, most difficult math problems ever solved. The solving of Fermat's Last Theorem is an inspiring story of achieving what appears to be impossible and Andrew Wiles will forever be remembered in mathematical history for his work. Of course, all this was only made possible by mathematician and scholar Pierre de Fermat and his intellect and appreciation for mathematics--as well as the many other people who contributed to the development of mathematics to make the proofs and ideas possible. In a way, the proof of Fermat's Last Theorem is a culmination of several millenniums of human intellect and thought. Although there isn't much practical value to knowing the equation $x^n + y^n = z^n$ has no integer solutions for n>2, there is inherent elegance in the truth of the statement and there's a hidden beauty in the thousands of hours put into proving it to be true.

Sources

1. Diophantus of Alexandria. *Arithmetica.* 3rd century AD. Print.

2. O'Connor, JJ and Robertson, EF. "Pierre de Fermat." 1996.

<http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Fermat.html>

3. William Dunham. *Encyclopedia Britannica*. “Number Theory.” 2012.

<http://www.britannica.com/topic/number-theory>

4. Ball, Walter William Rouse. *A short account of the history of mathematics*. 1888.

Print.

5. Newman, J. R. *The World of Mathematics.* 1956. Print.

6. Radko, Olga. *Fermat’s Last Theorem and the History of Number Theory*.
<http://www.math.ucla.edu/~radko/circles/lib/data/handoutId88-0.pdf>

7. Ribenboim, Paulo. *13 Lectures on Fermat's Last Theorem*. 1979. Print.

8. Varma, Ila. *Kummer, Regular Primes, and Fermat’s Last Theorem*
<http://www.math.harvard.edu/~ila/Kummer.pdf>

9. Ribet, Kenneth A. *From the Taniyama-Shimura Conjecture to Fermat’s Last Theorem.* 1990.
<https://math.berkeley.edu/~ribet/Articles/toulousela.pdf>

10. Chang, Sooyoung. *Academic Genealogy of Mathematicians*. 2010. Print. p. 207.

11.Kolata, Gina "At Last, Shout of 'Eureka!' In Age-Old Math Mystery". *The New York Times*. June 1993.

12. Singh, Simon. *Fermat's Last Theorem*. 1997. Print.

13. Wiles, Andrew. "Modular Elliptic-Curves and Fermat's Last Theorem." 1995.

<http://math.stanford.edu/~lekheng/flt/wiles.pdf>