Running head: Fermat’s Last Theorem

300 Years of Mathematical Frustration

Chris Grant

History of Mathematics

Jennifer McCarthy, Annie Cox

July 16, 2010

Abstract

Fermat’s Last Theorem has been a mathematical enigma for over three hundred years. First developed by Pierre de Fermat, it takes its origins from Pythagoras and the Pythagorean Theorem. Fermat’s Last Theorem deals with the equation . Fermat believed that there were no whole number solutions to this equation, and the challenge he left for future mathematicians was to prove this statement. The history of the many attempts to answer Fermat’s challenge is full of both success and failure, (mostly failure) until finally in 1995 a complete proof was discovered for Fermat’s Last Theorem.

There have been few mathematical riddles throughout history that can be compared to the highly debated and controversial Fermat's Last Theorem. First discovered in the 1600s it was three hundred years later before someone created an acceptable proof for the theorem. At a first glance Fermat's riddle looks surprisingly simple. He states that there are no whole number solutions for the equation If one simply substitutes combinations of numbers into the equation, Fermat appears to be correct that no solutions exist. For example if one substitutes the values 6, 8, and 9 into the result is . Other combinations of values produce similar results, however even though Fermat's Theorem seems to be true for a few cases, mathematicians cannot extrapolate those findings to other number combinations, and with an infinite amount of numbers it is impossible to individually check each possible solution. The only way to be sure that Fermat's Theorem is in fact true is to create a mathematical proof, and it is the discovery of such a proof that has stumped some of the greatest mathematicians of the age. Adding insult to injury it appears that Pierre de Fermat had a proof for his Theorem but chose not to write it down. In the margin next to where he proposed that has no solution he wrote *I have a truly marvelous demonstration of this proposition which this margin is to narrow to contain* (Simon Singh 1997). Whether Fermat did in fact have a proof is not known but what is clear is that his cryptic message started a journey of mathematical frustration that did not end until three hundred years later.

The interesting thing about Fermat’s Last Theorem is its close relationship to the Pythagorean Theorem, a topic that is taught in most high schools. The Pythagorean Theorem states that for any right triangle the two shorter legs squared and added together will equal the hypotenuse squared. This can be represented by the equation . Remember that Fermat’s equation is This similarity is not a coincidence, much of Fermat’s work in number theory was in fact inspired by Pythagoras and this equation was no exception. When Fermat’s Theorem was first noticed by the mathematical community they too recognized the resemblance, but they soon found out that this did not make it any easier to prove.

The first real progress in the search for a proof of Fermat’s Theorem was made by Leonard Euler, almost one hundred years after Fermat’s death. Looking through Fermat’s jumbled notes Euler discovered a proof for a different problem that when switched around also proved the equation Fermat had unknowingly or knowingly proved part of his Theorem, specifically that the equation has no whole number solutions. (Remember that the original equation represents an infinite amount of other equations as long as . Using these notes Euler fashioned a proof for and with this success hoped to extrapolate the proof to all the other equations. The method that Fermat and Euler used to prove the two equations is known today as the method of infinite descent which is a type of proof by contradiction. In the case of , Fermat was actually trying to prove that the area of a right triangle cannot be the area of a square with sides of whole numbers. Fermat began his proof by assuming that there does exists a right triangle with an area equal to a square, and that the existence of such a triangle must also mean the existence of a certain equation. This equation derived from Fermat’s own words is . Through some manipulation this equation can also prove . If one substitutes for p in the previous equation one gets which is the Last Theorem. So when Fermat proved that there are no right triangles with the same area as a square he also proved that there are no solutions for the equation (Larry Freeman,2005). A clearer description of how the method of infinite descent works is shown in how Euler constructed his proof.

By assuming that there existed solutions to the equation Euler showed that there would also have to be solutions that were smaller than called Then he showed that there would have to be even smaller solutions . This pattern continued until the solutions become infinitesimally small, however since this contradicts the fact that have to be whole numbers there must be no solutions to (Singh,1997). One major difference between Euler’s and Fermat’s proof is that Euler had to include imaginary numbers to make it work for .

Even after Euler’s work, Fermat’s Last Theorem was still far from being completely proved. At the moment only two cases of the theorem had proofs; However it was soon discovered that the proof for also worked for any multiple of 4, because any number that can be written as a power of 8, 12, 16… (all multiples of four) can also be rewritten as a number to the 4th power. The same is true for What was also realized was that it was only necessary to prove the Last Theorem for the prime values of , because any other number can be found by multiplying different combinations of prime numbers. So if you prove the prime numbers for then you would also automatically prove any other value of The problem with this is that there is an infinite amount of prime numbers so one could not just go through and prove each prime individually (Singh, 1997).

The next mathematician to make a major contribution towards proving the Last Theorem was Sophie Germain in the early 1800s. Her work was concentrated on a particular set of prime numbers where is also a prime number. For example, eleven would be a Germain prime because which is a prime. Thirteen is not a Germain prime however, because . Germain argued that the equation where was unlikely to have any solutions because, as seen in her calculations, either would have to be a multiple of . (Singh, 1997)

Thanks to Germain’s work, more proofs of individual values began to pop up. In 1825 Gustav Lejeune-Dirichlet and Adrien-Marie Legendre both created proofs for based on Germain’s method. Soon after, Gabriel Lamé proved the case for . Then on March 1, 1847 two separate mathematicians announced they were on the verge of completing a proof for the Last Theorem. The two were Augustin Cauchy and Gabriel Lamé, Lamé being the same one who created the proof for earlier. Only a few weeks later however the race for the proof of the Last Theorem was once again set back.

Ernst Kummer was another well known number theorist of his time and when he heard that Cauchy and Lamé were each coming close to developing a proof he decided to look over the few notes they had published. After reading their work Kummer came to the conclusion that both Cauchy and Lamé were going to fail because of one illogical step in their reasoning. Both proofs contained unique factorization, a property that states that there is only one combination of prime numbers that will multiply together to get another number. For example, the only prime numbers that multiply together to get sixteen is:

Other examples are:

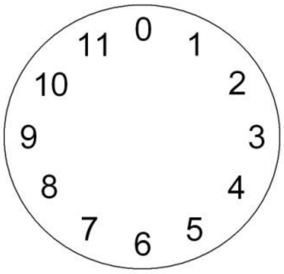
Usually, the inclusion of unique factorization in mathematical proofs is widely accepted, but what makes it different for Cauchy and Lamé is the use of imaginary numbers in their proofs. Kummer asserted that while unique factorization holds true for any real number, it becomes invalid with the addition of complex or imaginary numbers. For instance, the only way the integer sixteen can be factored using real prime numbers is , however if one were to take imaginary numbers into account then sixteen could additionally be factored as:

Or alternately:

As this example shows, the introduction of complex numbers subsequently leads to there being not just one unique factorization, but several factorizations. (Freeman, 2005) Since both Cauchy's and Lamé's proofs heavily relied on unique factorization, Kummer's discovery set them back far. Neither one could sufficiently alter their proof enough to make it work, and eventually they gave up on their efforts. Kummer however, found a way to restore unique factorization for certain prime numbers, and using this technique was able to prove many prime values of for Fermat's Last Theorem. He soon learned however, that there existed "irregular primes" with which he was unable to work with. Some examples of these prime numbers include (Singh, 1997)

It was not until the late 1950s before there were any more significant breakthroughs towards developing a proof for the Last Theorem, and by then most of the mathematical community had given up hope of ever finding a solution. Yutaka Taniyama and Goro Shimura were two highly talented number theorists who, after a chance meeting, decided to work together and combine their research. What they came up with is known as the Taniyama-Shimura conjecture.

The Taniyama-Shimura conjecture states that every elliptic equation has a corresponding modular form that has the same matching elements. In order to comprehend the significance of this finding, it is necessary for one to understand the properties of both elliptic equations and modular forms. An elliptic equation takes the form of . Not unlike Fermat's Last Theorem, the problem with this type of equation is the difficulty in testing for all the possible solutions of . With an infinite number space, it is impossible to simply substitute every known integer in for and see if it works. In order to overcome this obstacle, mathematicians today employ a technique called clock-arithmetic. This method involves taking a number line and looping it around back on itself, so that a finite number space is created.



(http://knol.google.com/k/-/-/1z0lc1vjx1yhu/d3qhrl/image%20(1).jpg)

The picture above is a diagram of 12-clock arithmetic, note that while it does share a close resemblance to a regular clock, one difference is that the number twelve is replaced with a zero. In 12-clock arithmetic instead of the usual , this is calculated by starting at the number seven and then moving around eight spaces until finally reaching three. Similarly . Since clock arithmetic creates a finite number space, once applied to an elliptic equation it limits the total number of solutions. Mathematicians can then list these solutions for each clock arithmetic, creating what is called an L-series. The L-series is used most often to describe a particular elliptic equation. (Singh, 1997)

Modular forms are some of the most intriguing and confusing objects in mathematics. What makes them so interesting is that they exist only on the fourth dimension and are represented by two real axis and two imaginary axis. Another unique property of modular forms is their extreme levels of symmetry. No matter how they are rotated, reflected, or shifted, modular forms will almost always remain unchanged. What interested Taniyama and Shimura the most is the fact that all modular forms are made up of the same basic components, the differentiating factor being the amount of each component they contain. Similar to the L-series in elliptic equations, it is then possible to make a list of the components for a particular modular form. This list is sometimes known as a modular series. Taniyama and Shimura made a tremendous discovery when they established a link between these two series. Elliptic equations and modular forms were previously thought to be two entirely different branches mathematics, but there now seemed to be a connection. Some mathematicians remained skeptical however, because of the lack of a proof for the conjecture. Although Taniyama's and Shimura's assertion appeared to be true, there are an infinite amount of both elliptic equations and modular forms, making the possibility that there existed an exception to their rule not unlikely.

The significance of the Taniyama-Shimura conjecture and its relevance to Fermat's Last Theorem was not made apparent until 1984 at a mathematical symposium. Before the conference could start, mathematician Gerhard Frey stood up and made a startling announcement. He claimed that if someone were able to develop a proof for the Taniyama-Shimura conjecture, he or she would also prove Fermat's Last Theorem at the same time. Frey began his argument by assuming that Fermat's equation had a hypothetical solution:

He then went on to manipulate the equation until it looked like this:

Although it may not be clear at first, what Frey had done was change Fermat’s original into an elliptic equation so that:

Frey then asserted that this elliptic equation had an L-series that was so “abnormal”, it was impossible for it to have a matching modular series. This statement directly conflicts with the Taniyama-Shimura conjecture, which states that every elliptic equation *must* have a corresponding modular form. If the Taniyama-Shimura conjecture is true then Frey’s elliptic equation must not exist, so consequently Fermat’s equation must not exist or have any solutions (remember that the two equations are the same, only rearranged differently). If Fermat’s equation has no solutions then Fermat’s Last Theorem must be true. (Singh, 1997)

Frey’s argument was logical at every step except one. When he made the statement that his elliptic equation did not have a matching modular form, he failed to offer any proof of this claim. Until someone developed such a proof, the connection between the Taniyama-Shimura conjecture and Fermat’s Last Theorem could not be made.

Eighteen months later that proof was finally published by Professor Ken Ribet, one of the attending mathematicians at Frey’s lecture. Using complex math he had sufficiently proved that Frey’s elliptic equation could not possibly be modular. At last Fermat’s Last Theorem seemed to provable. Now the only obstacle remaining towards developing a proof for the theorem was proving the Taniyama-Shimura conjecture.

Even though Professor Ribet's completion of the Frey argument was exciting, it did not lead to the fervor or rush that one might expect. Many mathematicians still believed that the Taniyama-Shimura conjecture was impossible to prove, so its connection to Fermat's Last Theorem was irrelevant. One man who thought differently was Andrew Wiles. Using a concept known as group theory Wiles began writing his proof for the Taniyama-Shimura conjecture.

Group theory is an algebraic idea that deals with combined sets of elements, usually by an operation such as addition. Wiles hoped to combine group theory with other known techniques in order to create a proof by induction. (Singh, 1997) In other words, he was trying prove that if the first element in a L-series matches up with the first element in a modular series, all the rest would match up as well. Then he would have to apply that to the infinite amount of elliptic equations and modular forms. It was a daunting task but after eight years of work, Wiles came up with a proof that he finally believed worked. Once published, the initial reaction of the mathematical community was astonishment and utter joy. Here was a riddle that had troubled mathematicians for over three hundred years, but now was finally solved. To be completely sure of its accuracy however, Wiles' proof had to be verified and validated by a few select reviewers. His proof was over one hundred pages long, so chances were he might had made some error in his reasoning. Sure enough, a small mistake was spotted in Wiles' logic that could not be reconciled easily. Not to be denied, Wiles toiled for two more years until finally in 1995, a complete proof of Fermat's Last Theorem was created.

Even though Andrew Wiles was the man who eventually came up with the proof in its entirety, if it were not for the efforts of all the great mathematicians that came before him it is unlikely that Fermat's Last Theorem would ever have been solved. Possibly the most famous and intriguing mathematical riddle to date, it took over three hundred years for its solution to be revealed. At long last mathematicians could rest easy knowing the fact that Fermat’s challenge to the world was finally answered.

References

Freeman, L. (2005, May 17). *Fermat's last theorem*. Retrieved from http://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-n-4.html

Singh, S. (1997). *Fermat's enigma*. United States of America: Walker Publishing Company, Inc.

Wilkinson, D. (1996, December). *Proof of fermat's last theorem*. Retrieved from http://mathforum.org/library/drmath/view/52516.html