Fermat's Enigma: Unraveling the Margins

Fermat’s Last Theorem

By

Aayush Parekh
MATH406

Table of Contents

1. Abstract

In this paper, I present and explain Fermat's Last Theorem. I will go through the history of how this marvelous theory took 350 years to prove. The mathematical methods used to prove the theorem in this paper could be the proof that Fermat used and was too large to fit in the margin of the Arithmatica. These methods used were known during Fermat's time during the 17th century. Every mathematician has shown some interest in finding the proof since Fermat's statement in the Arithmatica. However, Andrew Wiles was the first mathematician to be able to prove the theorem in 1995. Since Fermat was a professional lawyer and math was more like his hobby, he would have a simple proof for the theorem. Therefore, this is a simple proof that can be easily understood by anyone.

2. Background

Fermat's Last Theorem (FLT) is a theory conjectured by Pierre de Fermat in the 17th century. The theorem expressed how there is no positive integers a, b, and c that would satisfy the equation $a^n + b^n = c^n$ where $n \geq 3$. This theorem remained unsolved for 350 years. It is easy to prove something, however, disproving something is very problematic as there are infinitely many numbers. In the same way, there are infinite possibilities for the value of a, b, and c and trying every value is a bit problematic. Until it proved Andrew Wiles in 1995.

This theorem has a very complex history with multiple mathematicians trying to prove the theorem for 350 years. The theory was first stated by Fermat in 1637. He wrote the theorem on a copy of a copy of Diophantus' Arithmetica that he acquired. However, he did not prove the theorem as it was too large to fit on the margin of the book. He claimed that he had a proof, but that the margin of his book was not large enough to contain it.

The theorem remained unsolved for over 350 years, despite the efforts of many mathematicians. One of the biggest obstacles to proving the theorem was the lack of a general theory of numbers that could be used to tackle such a problem. In the 19th century, mathematicians like Legendre, Kummer, Gauss, Euler, Sophie Germain, Jacobi, and Dirichlet made significant progress in developing such a theory, but it was not until the 20th century that the necessary tools were in place to tackle Fermat's Last Theorem. Many proofs for specific exponents were proved through the years. Fermat proved the theorem when n = 4 in 1637. Then Euler solved the theorem when n = 3 in 1753, Legendre proved it when n = 5 in 1825, Lame proved it when n = 7 in 1839 and Kummer proved it when n < 100 and $n \geq 3$ in 1857.

But it wasn't until 1995, that Andrew Wiles proved the theorem. By using Ribet's Theorem and proving the modularity theorem for semi-stable elliptical curves Andrew Wiles was able to prove Fermat's Last theorem. Mathematicians are still trying to figure out a simple proof for the theorem trying to mimic the proof used by Fermat in 1637. Additionally, Fermat's Last Theorem has sparked interest among non-mathematicians and has been the subject of numerous books and articles. It is often cited as an example of the beauty and elegance of mathematics and the power of human reason.

Here is one of the simple proofs for the theorem. This could be the theorem used by Fermat in 1637, however, we can never be sure. I have presented two lemmas that will help me prove the theorem.

3. Lemmas

Lemma 3.1. For all positive integers, if $a^n + b^n = c^n$ and $n \geq 2$, then there exists a triplet (x, y, z) such that

$$a = y + z \qquad b = x + z \qquad c = x + y + z$$

where, *gcd(x, y) = gcd(c, x) = gcd(c, y)* = 1 and $z \equiv 0\ (mod\ (rad(xy))$. *gcd* stands for the greatest common divisor and *rad* stands for radical. The radical of an integer is the product of its prime factors.

Proof – Assume a, b, c ,and n are positive integers such that

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

If a, b, and c have any common prime factors then they will cancel each other out on both sides of the equation above. Therefore, we can probably assume that a and b are coprime. Therefore, by standard arithmetic, we have $c^n > a^n$ and $c^n > b^n$. This implies that $c > a$ and $c > b$. But the binomial theorem tells us

(3.1) $$(a+b)^n = a^n + b^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i = c^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i ,$$

where the binomial coefficient is defined as $\binom{n}{i} = \frac{n!}{[(i!)(n-i)!]}$. Since the summation

$$\sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i \geq 0,$$

therefore,

(3.2) $$(a+b)^n \geq c^n,$$

which suggests that $a + b > c$ for any integer $n \geq 2$. Therefore, $c > a$, $c > b$, and a+$b > c$ for any integer $n \geq 2$. This implies that there exist positive integers x and y such that

(3.3) $$c = a + x \qquad x < b$$

(3.4) $$c = b + y \qquad y < a$$

Since $a + b > c$ (using equations 3.3 and 3.4)

(3.5) $$2c = a + b + x + y > c + x + y$$

(3.6) $$c > x + y$$

Therefore, there exists another positive integer z such that

(3.7) $$c = x + y + z$$

(3.8) $$a = c - x = y + z$$

(3.9) $$b = c - y = x + z$$

Using equations 3.3 and 3.4 , $a^n + b^n = c^n$ can be written as

(3.10) $$a^n + b^n = (a + x)^n$$

and

(3.11) $$a^n + b^n = (b + y)^n.$$

Now we can use the binomial theorem to expand the right side of the equations above

(3.12) $$x^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i x^{n-i} - b^n = 0$$

and

(3.13) $$y^n + \sum_{i=1}^{n-1} \binom{n}{i} b^i y^{n-i} - a^n = 0$$

From the equations (3.12 and 3.13) above we can say that

$$b^n \equiv 0 \ (mod\ x)$$

$$a^n \equiv 0 \ (mod\ y)$$

This means that

$$b \equiv 0 \ (mod\ rad(x))$$

$$a \equiv 0 \ (mod\ rad(y))$$

Since the positive integers a, b, c are coprime *gcd(x, y) = gcd(c, x) = gcd(c, y)* = 1

Using equations 3.7, 3.8 and 3.9, $a^n + b^n = c^n$ can be written as

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

If this equation is simplified using the binominal theorem, then we get

$$z^n = \frac{1}{2}n(n-1)z^{n-2}[(x+y)^2-(x^2+y^2)] + \frac{1}{6}n(n-1)(n-2)z^{n-3}[(x+y)^3-(x^3+y^3)] + \ldots.+nz[(x+y)^{n-1}-(x^{n-1}+y^{n-1})]+[(x+y)^n-(x^n+y^n)]$$

$$\therefore z^n = xy[n(n-1)z^{n-2}+\tfrac{1}{2}n(n-1)(n-2)z^{n-3}(x+y)+\ldots. + nz\sum_{i=1}^{n-2}\binom{n-1}{i}(x^{n-i-2})(y^{i-1})+\sum_{i=1}^{n-1}\binom{n}{i}(x^{n-i-1})(y^{i-1})$$

Therefore, the equation above shows that $z \equiv 0\ (mod\ (rad(xy))$. Hence, we have proved that for positive integers if $a^n + b^n = c^n$ and $n \geq 2$, then there exists a triplet (x, y, z) such that

$$a = y + z \qquad b = x + z \qquad c = x + y + z,$$

where *gcd(x, y) = gcd(c, x) = gcd(c, y)* = 1 and $z \equiv 0\ (mod\ (rad(xy))$.

Lemma 3.2. If a and b are positive integers, then

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ldots\ldots - ab^{n-2} + b^{n-1}),$$

for any odd integer n.

Proof – By multiplicative identities, we can show that

(3.15) $$(a+b)(a^2 - ab + b^2) = a^3 + b^3$$

(3.16) $$(a+b)(a^4 - a^3b + a^2b^2 - ab^3 + b^4) = a^5 + b^5$$

And so on as the powers keep increasing. Thus, we can show this for any odd integer n

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - a^{n-4}b^3 \ldots\ldots + a^2b^{n-3} - ab^{n-2} + b^{n-1})$$

4. Proof of Fermat's Last Theorem

Suppose x and y are positive integers, where $n = xy$. If $a^n + b^n = c^n$ has solutions that are positive integers, then $(a^x)^y + (b^x)^y = (c^x)^y$ would have (a^k, b^k, c^k), which are positive integers , as solutions when $n = y$. When $n \geq 3$ either n is an odd prime greater than 3, n is a multiple of an odd prime greater than 3, or $n = 2^x$, when $x \geq 2$, which can be written as $n = 4(2^{x-2})$

Therefore, to prove Fermat's little theorem we need to prove that $a^n + b^n = c^n$ has no solutions. We need to prove that the equation has no solution when n = 4 and when n is an odd prime ≥ 3. Therefore, Fermat's little theorem is divided into 2 parts. If we prove that n has no solution in both cases, then we have proved FLT.

Theorem 4.1. If n is an odd prime ≥ 3, then the equation $a^n + b^n = c^n$ has no positive integer solutions

Proof – According to Lemma 3.1, for positive integers, if $a^n + b^n = c^n$ and $n \geq 2$, then there exists a triplet (x,y,z) such that

(4.1) $a = y + z \qquad b = x + z \qquad c = x + y + z$

where *gcd(x, y) = gcd(c, x) = gcd(c, y)* = 1 and $z \equiv 0\ (mod\ (rad(xy))$.

We also know that

(4.2) $a + b = (y + z) + (x + z) = (x + y + z) + z = c + z$

According to Lemma 3.2, for any odd integer $n \geq 3$

$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ a^{n-4}b^3 \ldots\ldots + a^2b^{n-3} - ab^{n-2} + b^{n-1})$

Then for any odd integer $n \geq 3$

$$c^n = a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ a^{n-4}b^3 \ldots\ldots + a^2b^{n-3} - ab^{n-2} + b^{n-1})$$

However, as proved by equation 4.2, $a + b = c + z$. This cannot be a factor of c^n, because according to Lemma 3.1, *gcd(x, y) = gcd(c, x) = gcd(c, y)* = 1 and $z \equiv 0\ (mod\ (rad(xy))$. Therefore, a clear contradiction is depicted proving that the equation $a^n + b^n = c^n$ has no solution when n is an odd prime greater than 3. Hence Theorem 4.1. is proved.

Theorem 4.2. There are no positive integer solutions for the equation $a^4 + b^4 = c^4$

Proof – Assume that for the equation $a^4 + b^4 = v^2$ there is a positive integer solution where the *gcd*(a, b) = 1 and $v = c^2$. Therefore, (a^2, b^2, v) is basically a Pythagoras triplet. For the equation, $a^4 + b^4 = v^2$. Therefore

(4.4) $a^2 = x^2 - y^2 \qquad b^2 = 2xy \qquad v = x^2 + y^2$

where $x > y > 0$ and *gcd*(x, y) = 1. Therefore $a^2 + y^2 = x^2$. Therefore, again the (a, y, x) is a Pythagoras triplet of the equation $a^2 + y^2 = x^2$. Therefore

(4.5) $a = k^2 - l^2 \qquad y = 2kl \qquad x = k^2 + l^2$

where $k > l > 0$ and *gcd*(k, l) = 1. Using the equations in 4.5,

(4.6) $$b^2 = 4(k^2 + l^2)kl$$

or

(4.7) $$(\frac{b}{2})^2 = (k^2 + l^2)kl$$

The above equations are only true when k, l, and $k^2 + l^2$ are squared integers. Therefore, we can further write them as

(4.8) $$k = (a1)^2 \qquad y = (b1)^2 \qquad k^2 + l^2 = (v1)^2$$

Therefore, we can say that

(4.9) $$a1^4 + b1^4 = v1^2$$

This depicts how we have a new solution for the equation $a^4 + b^4 = v^2$.

(4.10) $$v = x^2 + y^2 = (k^2 + l^2)^2 + (2kl)^2 = v1^4 + 4(a1)^4(b1)^4$$

This implies that $v > v1$. According to the proof by infinite descent or Fermat's method of descent this is a contradiction as the solution cannot be shrinking indefinitely. Therefore, there is no positive integers that satisfy the equation $a^4 + b^4 = c^4$.

5. Results

The proof of theorem 4.1 and 4.2 proves that there is no positive integer solution for the equation

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

when $n \geq 3$. Hence, we have proved Fermat's Last Theorem.

This result was proven by Andrew Wiles in 1994, after many years of work. Wiles's proof was a landmark achievement in mathematics, and it has been hailed as one of the greatest achievements of the 20th century.

6. Applications

There are several possible applications of Fermat's Last Theorem. The FLT can be used as a starting point to explore more complex topics in number theory. The theorem helps prove the non-existence of certain types of numbers. There are a lot of numbers that do satisfy the equation $a^n + b^n = c^n$ as proven by FTL. The theorem can also be used to study the distribution of prime numbers, elliptic curves, and modular forms in number theory. It can be used to study the properties of Diophantine equations and the solutions they may or may not have.

Another application of FTL is cryptography. In RSA, a sender can encrypt a message by raising it to a power determined by the recipient's public key, and the recipient can decrypt the message by raising the encrypted message to a power determined by their private key. The security of the RSA algorithm relies on the fact that it is computationally infeasible to determine the private key from the public key, and this is typically achieved by using very large composite numbers as the keys. Fermat's Last Theorem can be used to prove the non-existence of certain types of numbers that could potentially be used to break the RSA algorithm. For example, the theorem proves that there is no positive integer solution for the equation $a^n + b^n = c^n$ when $n \geq 3$, which means that RSA keys cannot be constructed using these types of numbers. This helps to ensure the security of the RSA algorithm, as it makes it more difficult for attackers to find ways to factor in the large composite numbers that are used as keys.

7. References

1. Wiles, A. J. (n.d.). *Modular elliptic curves and Fermat's last theorem*. Modular elliptic curves and Fermat's Last Theorem. Retrieved December 14, 2022, from http://scienzamedia.uniroma2.it/~eal/Wiles-Fermat.pdf
2. Ribet, K. A. (1990, January 1). *From the taniyama-shimura conjecture to Fermat's last theorem*. Annales de la Faculté des sciences de Toulouse : Mathématiques. Retrieved December 14, 2022, from http://www.numdam.org/item/AFST_1990_5_11_1_116_0/
3. *Proofs by descent - university of connecticut*. (n.d.). Retrieved December 14, 2022, from https://www.math.uconn.edu/~kconrad/ross2007/descent.pdf
4. *Pythagorean triples and Fermat's Last Theorem - Memorial University of ...* (n.d.). Retrieved December 14, 2022, from https://www.math.mun.ca/~drideout/pytrip06.pdf
5. *26 Fermat's Last Theorem - math.mit.edu*. (n.d.). Retrieved December 14, 2022, from https://math.mit.edu/classes/18.783/2017/LectureNotes26.pdf
6. *The proof of Fermat's last theorem by r.taylor and a*. (n.d.). Retrieved December 14, 2022, from https://www.ams.org/notices/199507/faltings.pdf
7. *Fermat's last theorem analysis in 7 understandable forms*. (n.d.). Retrieved December 14, 2022, from https://www.researchgate.net/profile/Nikos-Mantzakouras/publication/342349669_Proof_of_Fermat's_Last_Theorem_Using_7_Methods/links/6351501196e83c26eb3ad75b/Proof-of-Fermats-Last-Theorem-Using 7-Methods.pdf
8. *An overview of the proof of Fermat's last theorem - bu*. (n.d.). Retrieved December 14, 2022, from http://math.bu.edu/people/ghs/papers/FermatOverview.pdf