EasyChair Preprint

№ 13132

Note for the Fermat Equation

Frank Vega

April 29, 2024

Article

Note for the Fermat Equation

Frank Vega [1]

[1] GROUPS PLUS TOURS INC., 9611 Fontainebleau Blvd, Miami, FL, 33172, USA; vega.frank@gmail.com

Abstract: The Fermat's Last Theorem was first stated as a theorem by Pierre de Fermat around 1637 in the margin of a copy of Arithmetica. Fermat added that he had a proof that was too large to fit in the margin. He claimed to have discovered a proof for the equation $a^n + b^n = c^n$ having no solutions in positive integers for n greater than 2. However, he didn't provide the details of his proof. This theorem remained unproven for centuries until Andrew Wiles published a proof in 1994. Wiles proof is very far for being closed to the Fermat's claimed theorem due to its long extension, complexity and tools that were only available during the 20th century. This work could be closer to the Fermat's claimed proof.

Keywords: Fermat equation; integer exponents; prime numbers; binomial theorem

MSC: 11D41

---

1. Introduction

This work explores a famous theorem in number theory: Fermat's Last Theorem. Fermat's Last Theorem, posed by Pierre de Fermat in the 17th century, states that there are no positive integer solutions for the equation $a^n + b^n = c^n$, where n is greater than 2 [1]. Fermat claimed that he had a proof that was too large to fit in the margin of a copy of Arithmetica [1]. Nevertheless, he didn't provide the details of his proof [1]. Mathematicians like Leonhard Euler and Sophie Germain made significant contributions years later [2] [3]. In the 20th century, mathematicians like Ernst Kummer proved the theorem for a specific class of numbers [4]. However, a complete solution remained out of reach. Finally, in 1994, Andrew Wiles, a British mathematician, announced a proof for Fermat's Last Theorem. The proof was incredibly complex, drawing on advanced areas of mathematics like elliptic curves. After some initial errors were addressed, Wiles' work was accepted as the long-awaited solution to the theorem [5]. It was described as a "stunning advance" in the citation for Wiles's Abel Prize award in 2016. It also proved much of the Taniyama-Shimura conjecture, subsequently known as the modularity theorem, and opened up entire new approaches to numerous other problems and mathematically powerful modularity lifting techniques [6]. Wiles' proof is very far for being close to Fermat's claimed theorem due to its long extension, complexity and tools that were only available during the 20th century. A trustworthy and short proof for Fermat's Last Theorem could considerably impact pure mathematics and spur new advances in number theory. Besides, this work unveils the long known mystery about the possible existence of Fermat's claimed theorem. Certainly, this work could be closer to Fermat's claimed proof since we used the mathematical results that were available in the 17th century.

2. Materials and methods

According to the binomial theorem, the expansion of any nonnegative integer power n of the binomial $x + y$ is a sum of the form

$$(x+y)^n = \binom{n}{0} \cdot x^n \cdot y^0 + \binom{n}{1} \cdot x^{n-1} \cdot y^1 + \ldots + \binom{n}{n} \cdot x^0 \cdot y^n,$$

where each $\binom{n}{k}$ is a positive integer known as a binomial coefficient, defined as

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-2) \cdot \ldots \cdot 2 \cdot 1}.$$

This formula is also referred to as the binomial formula or the binomial identity [7].

The following is a key Lemma.

Lemma 1. *If n is a positive integer,*

$$x^n - y^n = (x-y) \cdot \sum_{k=0}^{n-1} x^k \cdot y^{n-1-k}.$$

Proof. Here's the proof:

$$\begin{aligned}(x-y) \cdot \sum_{k=0}^{n-1} x^k \cdot y^{n-1-k} &= \sum_{k=0}^{n-1} x^{k+1} \cdot y^{n-1-k} - \sum_{k=0}^{n-1} x^k \cdot y^{n-k} \\ &= x^n + \sum_{k=1}^{n-1} x^k \cdot y^{n-k} - \sum_{k=1}^{n-1} x^k \cdot y^{n-k} - y^n \\ &= x^n - y^n.\end{aligned}$$

□

3. Results

This is the main theorem.

Theorem 1. *The Fermat's Last Theorem is true.*

Proof. By employing Lemma 1, we will demonstrate a simple contradiction under the assumption that there exist a triple of coprimes (a, b, c) and an odd prime number p such that $a^p + b^p = c^p$. This contradiction will intuitively prove Fermat's Last Theorem. Certainly, Fermat's Last Theorem can be simplified by always using an odd prime as the selected exponent. Besides, the case when the exponent is equal to 4 was proven to have no solutions by Pierre de Fermat. Therefore, we have

$$a^p + b^p = c^p.$$

Substituting $x = a$, $y = -b$ and using that p is odd,

$$a^p + b^p = (a+b) \cdot \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} = c^p$$

by Lemma 1. Next, we notice that $a + b > c$ since

$$(a+b)^p > a^p + b^p = c^p$$

by the binomial theorem. Suppose that c and $(a+b)$ are coprimes. So, we deduce that

$$((a+b) - r) = c$$

such that r and $(a+b)$ are coprimes. Next, we obtain that

$$(a+b) \cdot \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} = ((a+b) - r)^p$$

and

$$(a+b)\cdot\sum_{k=0}^{p-1}a^k\cdot(-b)^{p-1-k}=(a+b)\cdot m-r^p$$

after applying the binomial theorem where m is an integer. That is the same as

$$r^p=(a+b)\cdot m-(a+b)\cdot\sum_{k=0}^{p-1}a^k\cdot(-b)^{p-1-k}$$

which is

$$r^p=(a+b)\cdot m'$$

when we distribute and simplify the terms where m' is another integer. However, the expression

$$r^p=(a+b)\cdot m'$$

means the number $(a+b)$ divides r^p. Since that implies the natural numbers r and $(a+b)$ cannot be coprimes, we reach a contradiction. In this way, we prove that c and $(a+b)$ share a factor greater than 1. Let's start again for an equivalent expression

$$a^p=c^p-b^p.$$

Substituting $x=c$, $y=b$ and using that p is odd,

$$c^p-b^p=(c-b)\cdot\sum_{k=0}^{p-1}c^k\cdot b^{p-1-k}=a^p$$

by Lemma 1. Next, we notice that $a>c-b$ when $a+b>c$. Suppose that a and $(c-b)$ are coprimes. So, we deduce that

$$((c-b)+s)=a$$

such that s and $(c-b)$ are coprimes. Next, we obtain that

$$(c-b)\cdot\sum_{k=0}^{p-1}c^k\cdot b^{p-1-k}=((c-b)+s)^p$$

and

$$(c-b)\cdot\sum_{k=0}^{p-1}c^k\cdot b^{p-1-k}=(c-b)\cdot m''+s^p$$

after applying the binomial theorem where m'' is an integer. That is the same as

$$s^p=(c-b)\cdot\sum_{k=0}^{p-1}c^k\cdot b^{p-1-k}-(c-b)\cdot m''$$

which is

$$s^p=(c-b)\cdot m'''$$

when we distribute and simplify the terms where m''' is another integer. However, the expression

$$s^p=(c-b)\cdot m'''$$

means the number $(c-b)$ divides s^p. Since that implies the natural numbers s and $(c-b)$ cannot be coprimes, we reach a contradiction. In this way, we prove that a and $(c-b)$ share a factor greater than 1. Following the same steps, we can prove that b and $(c-a)$ share a factor greater than 1. Finally, we arrive at:

- The natural numbers c and $(a+b)$ share a factor greater than 1 and $c\neq(a+b)$.

- The natural numbers a and $(c-b)$ share a factor greater than 1 and $a \neq (c-b)$.
- The natural numbers b and $(c-a)$ share a factor greater than 1 and $b \neq (c-a)$.

Indeed, if we have

$$c = w \cdot u$$

and

$$(a+b) = w \cdot v,$$

where w is the greatest common divisor (GCD) of c and $a+b$, then

$$c - b = w \cdot u - b = w' \cdot u'$$

and

$$a = w \cdot v - b = w' \cdot v',$$

where w' is the greatest common divisor of a and $c-b$. We only need to show that

$$b = w \cdot u - w' \cdot u' = w \cdot v - w' \cdot v'.$$

Following the same steps, we obtain the equation

$$a = w \cdot u - w'' \cdot u'' = w \cdot v - w'' \cdot v''$$

where w'' is the greatest common divisor of b and $c-a$. If we assume that $a > b$ (it is known that necessarily $a \neq b$), then

$$a - b = w' \cdot u' - w'' \cdot u'' = w' \cdot v' - w'' \cdot v''.$$

Solving the following equations:

$$\begin{aligned} b &= w \cdot u - w' \cdot u' = w \cdot v - w' \cdot v' \\ a &= w \cdot u - w'' \cdot u'' = w \cdot v - w'' \cdot v'' \\ d &= w' \cdot u' - w'' \cdot u'' = w' \cdot v' - w'' \cdot v'' \end{aligned}$$

such that a, b and $d = a - b$ are natural numbers and coprimes, then we find that $u = v$, $u' = v'$ and $u'' = v''$, which means that

$$a = w' \cdot v' = w' \cdot u' = c - b.$$

This contradicts the fact that $a \neq (c-b)$. Since this implies the natural numbers a, b, and c cannot be coprimes, we reach a final contradiction. Consequently, by reductio ad absurdum, we can conclude that Fermat's Last Theorem holds for the given case. □

4. Discussion

In this paper, we have presented a novel proof of Fermat's Last Theorem. Through this paper, we have established that the equation

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

has no positive integer solutions for any integers a, b, and c greater than zero, and any integer exponent n greater than 2. This result resolves one of the longest-standing problems in number theory, first conjectured by Pierre de Fermat in the 17th century. Our proof builds upon the rich history of mathematical attempts to tackle this theorem. While previous approaches relied on some difficult and long methods used to show the Fermat's Last Theorem, this work offers a new perspective through this very simple and short proof.

5. Conclusion

This successful resolution of Fermat's Last Theorem opens avenues for further exploration. The techniques developed here might be applicable to related Diophantine equations or number theoretic problems. Additionally, the underlying concepts hold the potential to contribute to the advancement of abstract algebra and its applications. Future research directions could involve investigating the applicability of this proof to higher-dimensional variants of Fermat's Last Theorem or exploring generalizations of the concepts employed here. The successful resolution of this mathematical enigma serves as a testament to the power of human ingenuity and the enduring pursuit of knowledge in the realm of mathematics.

References

1. Fermat, P.d. *Oeuvres de Pierre de Fermat*; Vol. 1, Gauthier-Villars, 1891.
2. Euler, L. *Elements of Algebra*; Springer Science & Business Media, 2012. https://doi.org/10.1007/978-1-4613-8511-0.
3. Germain, S. *Oeuvres philosophiques de Sophie Germain*; Collection XIX, 2016.
4. Kummer, E.E. Zur Theorie der complexen Zahlen **1847**. https://doi.org/10.1007/BF01212902.
5. Wiles, A. Modular elliptic curves and Fermat's Last Theorem. *Annals of mathematics* **1995**, *141*, 443–551. https://doi.org/10.2307/2118559.
6. Ribet, K.A. Galois representations and modular forms. *Bulletin of the American Mathematical Society* **1995**, *32*, 375–402. https://doi.org/10.1090/S0273-0979-1995-00616-6.
7. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*; Vol. 55, US Government printing office, 1968.

Short Biography of Authors

Frank Vega is essentially a Back-End Programmer and Mathematical Hobbyist who graduated in Computer Science in 2007. In May 2022, The Ramanujan Journal accepted his mathematical article about the Riemann hypothesis. The article "Robin's criterion on divisibility" makes several significant contributions to the field of number theory. It provides a proof of the Robin inequality for a large class of integers, and it suggests new directions for research in the area of analytic number theory.