Scientific Research Publishing

Advances in Pure Mathematics, 2021, 11, 735-740
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

An Elementary Proof of Fermat's Last Theorem for Epsilons

Bibek Baran Nag

Independent Researcher, London, UK
Email: bibek010101@gmail.com

How to cite this paper: Nag, B.B. (2021) An Elementary Proof of Fermat's Last Theorem for Epsilons. *Advances in Pure Mathematics*, **11**, 735-740.
https://doi.org/10.4236/apm.2021.118048

Received: September 26, 2020
Accepted: August 21, 2021
Published: August 24, 2021

Abstract

The author presents a new approach which is used to solve an important Diophantine problem. An elementary argument is used to furnish another fully transparent proof of Fermat's Last Theorem. This was first stated by Pierre de Fermat in the seventeenth century. It is widely regarded that no elementary proof of this theorem exists. The author provides evidence to dispel this belief.

Keywords

Diophantine, Equations, Fermat, Fermat's, Last, Theorem, Elementary, Number, Modular, Proof, Factorize

1. Introduction

Define n to be any integer such that $n > 1$. Suppose that a, b, c are positive integers satisfying

$$a^n = b^n + c^n, \tag{1}$$

where $a > b > c$. It was first conjectured by Pierre de Fermat in the 1630s that no solutions of (1) exist for $n > 2$. Fermat once claimed to have found proof of this conjecture, and so it was regarded as a theorem. Because all Fermat's other theorems were subsequently proved, this statement became known as Fermat's Last Theorem. Some special cases of the insolubility of (1) have been examined in both [1] and [2]. The first full proof of Fermat's Last Theorem was established as being a consequence of the modularity theorem for semistable elliptic curves, which was proved in [3] and [4] by Wiles and Taylor. This was succeeded by the proof of the full modularity theorem (in [5] [6] [7]) which settled a longstanding conjecture formulated by Taniyama, Shimura and Weil. The methods in this paper do not involve elliptic curves. Instead, a very simple argument is used to deal with

(1). A brief history of the subject is given in [8]. A new proof showing that (1) is insoluble for $n > 2$ is provided in the subsequent section. The author has previously discovered another simpler proof [9] of Fermat's Last Theorem by deriving the fact that (1) has no solutions for $n \geq c$. A completely different approach is used here. The following lemmas are fundamental results that are necessary for the novel argument employed in the proof of the theorem that follows. Note that the trivial case b = c is discarded by considering Lemma 3.

2. Analysis

Lemma 1. *If* (1) *holds only for* $n > 2$, *then it may be assumed without loss of generality that n is an odd prime.*

Proof. Suppose that $2 < n = p \cdot m$, where p is prime and m is some positive integer. It is possible to rewrite (1) as

$$\left(a^m\right)^p = \left(b^m\right)^p - \left(c^m\right)^p. \tag{2}$$

Suppose that q is some odd prime. The integer n, being at least 3, is divisible by an integer y such that $y \in \{4, q\}$. It is proved in [1] that (1) cannot be satisfied by $n = 4$. The desired result follows from the last two statements together with the last equation. □

Lemma 2. *Suppose that* (1) *is true. Then* $a < (b + c) < 2a$.

Proof. Since $a > b > c > 1$, it is clear that $(b + c) < 2a$. By using (1), it is easily seen that

$$a^n = b^n + c^n < (b + c)^n. \tag{3}$$

The statement of the lemma follows immediately. □

Lemma 3. *Suppose that* (1) *is true. Then it may be assumed without loss of generality that* a, b, c *are pairwise coprime.*

Proof. Divide a^n, b^n, c^n in (1) by their greatest common divisor. The statement of the lemma follows immediately. □

The following theorem is an important result which is established in an original and simple manner.

Theorem 1. *Suppose that* $n > 2$. *Then* (1) *has no solution.*

Proof. Suppose that (1) holds. By considering Lemma 1, it may be assumed without loss of generality that n is an odd prime. Since n is odd,

$$a^n = b^n + c^n = M(b + c), \tag{4}$$

where

$$M = \left(b^{n-1} - b^{n-2}c + \cdots + c^{n-1}\right). \tag{5}$$

It can be deduced from (1) that

$$b^n = a^n - c^n = L(a - c), \tag{6}$$

where

$$L = \left(a^{n-1} + a^{n-2}c + \cdots + c^{n-1}\right). \tag{7}$$

By considering Lemma 2 with the fact that $a > b > c > 0$, it can be determined that $1 < (a-c) < b$. It can also be deduced from (1) that

$$c^n = a^n - b^n = K(a-b), \tag{8}$$

where

$$K = \left(a^{n-1} + a^{n-2}b + \cdots + b^{n-1}\right). \tag{9}$$

By considering Lemma 2 with the fact that $a > b > c > 0$, it can be determined that $1 \le (a-b) < c$. It follows from (4) that $(b+c) \mid a^n$, so that there exists some integer p_a which is a common factor of *a* and $(b+c)$ such that $p_a > 1$. The last three pairs of equations can be used to distinguish various cases. First suppose that $(b+c) \not\perp M$. Then it follows that there exists some p_a such that $p_a \mid M$. Given that $(b+c) \not\perp M$, it may then be assumed without loss of generality in the subsequent argument that p_a can be chosen such that

$$M \equiv 0 \left(\operatorname{mod} p_a\right). \tag{10}$$

Because $p_a \mid (b+c)$, it is evident that

$$b \equiv -c \left(\operatorname{mod} p_a\right). \tag{11}$$

By considering the last two equations with (5), it can be established that

$$M \equiv nb^{n-1} \equiv 0 \left(\operatorname{mod} p_a\right), \tag{12}$$

so that $p_a \mid \left(nb^{n-1}\right)$. Since $p_a \mid a$ and $a \perp b$ by an application of Lemma 3 (so that a, b, c are assumed without loss of generality to be pairwise coprime), it is clear that $p_a \nmid b^{n-1}$. It follows from the last two sentences that $p_a \mid n$. By recalling that *n* is an odd prime and that $p_a > 1$, it is immediately apparent that $n = p_a$. Hence, if $(b+c) \not\perp M$ then $n = p_a$, where p_a is the unique common prime factor of *a*, $(b+c)$ and *M*. Suppose that $(b+c) \perp M$. Then it follows from (4) that there exists no prime factor of $(b+c)$ which is also a factor of *M*, so that

$$(b+c) = d^n, \tag{13}$$

for some positive integer *d* such that $d^n \perp M$. Recall that p_a is some common factor of *a* and $(b+c)$, and that, since $(b+c) \mid a^n$ (where $b > c \ge 1$), it is clear that $p_a \ge 2$. However, since $(b+c) \perp M$, p_a cannot be assumed to be prime. It follows from Lemma 2 that $a < (b+c) < 2a$, which implies that $(b+c)$ is not an integer multiple of *a*. Since $a \nmid (b+c)$ and $p_a \mid a$, where p_a is a common factor of *a* and $(b+c)$ such that $p_a \ge 2$, it follows that $a \ge 2p_a \ge 4$. By considering (4) with (13), it can then be determined that there exists some positive integer d_1 such that

$$a^n = d_1^n \cdot d^n, \tag{14}$$

where $d_1 > d > 1$ (since it is clear from applying Lemma 2 with (13) that $a < d^n < 2a$ so that, by considering (14), it is apparent that $\frac{a^{n-1}}{2} < d_1^n < a^{n-1}$, where $a \ge 4$). By using a similar argument to the one used earlier with p_a, it follows from (6) and (7) that if $(a-c) \not\perp L$ then $n = p_b$, where p_b is the unique common prime factor of *b*, $(a-c)$ and *L*. Also, if $(a-c) \perp L$ then it follows from (6) that there exists no prime factor of $(a-c)$ which is also a factor of *L*, so that

$$(a-c) = h^n, \tag{15}$$

for some positive integer *h* such that $h^n \perp L$ and $h^n < b$ by considering Lemma 2. By considering (6), this implies that there exists some positive integer h_1 such that

$$b^n = h_1^n \cdot h^n, \tag{16}$$

where $h_1 > h$ since $1 < h^n < b$. By using a similar argument to the one used earlier with p_a, it follows from (8) and (9) that if $(a-b) \not\perp K$ then $n = p_c$, where p_c is the unique common prime factor of *c*, $(a-b)$ and *K*. Also, if $(a-b) \perp K$ then it follows from (8) that there exists no prime factor of $(a-b)$ which is also a factor of *K*, so that

$$(a-b) = k^n, \tag{17}$$

for some positive integer *k* such that $k^n \perp K$ and $k^n < c$ by considering Lemma 2. By considering (8), this implies that there exists some positive integer k_1 such that

$$c^n = k_1^n \cdot k^n, \tag{18}$$

where $k_1 > k$ since $1 \le k^n < c$. By considering Lemma 3, it follows that at most one of p_a, p_b, p_c can be equal to *n*. Hence, at least two of (13), (15) and (17) hold. These cases can be distinguished as follows:

Case i) Suppose that both (15) and (17) hold. By subtracting (17) from (15), it is clear that

$$(b-c) = h^n - k^n > 0. \tag{19}$$

Note that

$$b^n - c^n = (b-c)\left(b^{n-1} + b^{n-2}c + \cdots + c^{n-1}\right). \tag{20}$$

It can be deduced from the last two equations that $\left(h^n - k^n\right) \mid \left(b^n - c^n\right)$. It follows from the last statement together with (16) and (18), for which $1 < h^n < h_1^n < b$ and $1 \le k^n < k_1^n \le c$, that either

$$\left(h^n - k^n\right)\left(h_1^n + k_1^n\right) = b^n - c^n, \tag{21}$$

or

$$\left(h^n - k^n\right)\left(h_1^n + k_1^n\right) - \left(h^n \cdot k_1^n - k^n \cdot h_1^n\right) = b^n - c^n. \tag{22}$$

It follows from (16), (18) and (21) that

$$h^n \cdot k_1^n = k^n \cdot h_1^n, \tag{23}$$

where $1 < h < h_1$ and $1 \le k < k_1$. By an application of the statement of the fundamental theorem of arithmetic [1], it follows that $h_1^n \not\perp k_1^n$. By considering (16) and (18), it is clear that the last statement leads to a contradiction because it violates the condition established earlier from an application of Lemma 3 that $b^n \perp c^n$. Therefore, (21) cannot hold. Since $\left(h^n - k^n\right) | \left(b^n - c^n\right)$, it is evident that (22) can be satisfied only if $h_1^n = k_1^n$. However, this also leads to a contradiction because $h_1^n \perp k_1^n$ by using (16) and (18) with the fact that $b^n \perp c^n$. Hence it is not possible for both (15) and (17) to hold. Therefore this case can be eliminated.

Case ii) Suppose that both (13) and (15) hold. By adding (13) and (15), it is clear that

$$\left(a+b\right) = d^n + h^n. \tag{24}$$

Note that

$$a^n + b^n = \left(a+b\right)\left(a^{n-1} - a^{n-2}b + \cdots + b^{n-1}\right). \tag{25}$$

It can be deduced from the last two equations that $\left(d^n + h^n\right) | \left(a^n + b^n\right)$. It follows from (14) and (16) that

$$\left(d^n + h^n\right)\left(d_1^n + h_1^n\right) - d^n \cdot h_1^n - d_1^n \cdot h^n = a^n + b^n. \tag{26}$$

Since $d_1^n \perp h_1^n$ by using the fact that $a^n \perp b^n$ (from an application of Lemma 3 made earlier), where both d_1 and h_1 have been proved to be integers strictly greater than 1, it is clear from the last equation that $\left(d^n + h^n\right) \nmid \left(a^n + b^n\right)$. Therefore, it is impossible for all of the last three equations to hold, and so a contradiction has been reached. Hence it is not possible for both (13) and (15) to hold. Therefore this case can be discarded.

Case iii) Suppose that both (13) and (17) hold. This case is equivalent to replacing b, h, h_1 in the previous case with c, k, k_1, respectively. It follows that this case can also be eliminated.

The statement of the theorem follows immediately. □

3. Conclusion and Discussion

A Diophantine problem known as Fermat's Last Theorem has been solved by using a new elementary proof by contradiction. It was motivated by considering factoring an equation with odd exponents. The method of proof involved analyzes three pairs of cases before using them to formulate a novel proof by contradiction. This method is more economical than using more advanced techniques to prove the desired result that the original Diophantine equation has no solutions for $n > 2$. Despite several attempts to obtain readers spanning the course of almost a year, the author could not find anyone who was prepared to properly read and check this proof of Fermat's Last Theorem. As the author has not been aware of any possible mistakes in the proof before publication, a decision has been made to publish this paper in case it may be noticed. Only in this instance can the proof be properly checked. It is mentioned here that the author has established Fermat's Last Theorem in a completely different manner in [9]. In this paper, the author has attempted to supply another elementary proof which is intended to be of a more conventional nature than the proof in [9].

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Hardy, G.H. and Wright, E.M. (1960) An Introduction to the Theory of Numbers. 4th Edition, Oxford University Press, Oxford.

[2] Ribenboim, P. (1999) Fermat's Last Theorem for Amateurs. 1st Edition. Springer Verlag, New York, 3-71.

[3] Wiles, A. (1995) Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, **141**, 443-551. https://doi.org/10.2307/2118559

[4] Wiles, A. and Taylor, R. (1995) Ring Theoretic Properties of Certain Hecke Algebras. *Annals of Mathematics*, **141**, 553-572. https://doi.org/10.2307/2118560

[5] Diamond, F. (1996) On Deformation Rings and Hecke Rings. *Annals of Mathematics*, **144**, 137-166. https://doi.org/10.2307/2118586

[6] Conrad, B., Diamond, F. and Taylor, R. (1999) Modularity of Certain Potentially Barsotti-Tate Galois Representations. *Journal of the American Mathematical Society*, **12**, 521-567. https://doi.org/10.1090/S0894-0347-99-00287-8

[7] Breuil, C., Conrad, B., Diamond, F. and Taylor, R. (2001) On the Modularity of Elliptic Curves over Q: Wild 3-Adic Exercises. *Journal of the American Mathematical Society*, **14**, 843-939. https://doi.org/10.1090/S0894-0347-01-00370-8

[8] Hollingdale, S. (2006) Makers of Mathematics. 1st Edition, Dover Publications, New York.

[9] Nag, B.B. (2019) On Fermat's Last Theorem. *Journal of Advances in Mathematics and Computer Science*, **34**, 1-4. https://doi.org/10.9734/JAMCS/2019/v34i230211