**Journal of Advances in Mathematics and Computer Science**

**34(4): 1-4, 2019; Article no.JAMCS.51504**

*ISSN: 2456-9968*

*(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)*

# On Fermat's Last Theorem

**Bibek Baran Nag**[1*]

[1] *Independent Researcher, UK.*

***Author's contribution***

*The sole author designed, analysed, interpreted and prepared the manuscript.*

***Article Information***

DOI: 10.9734/JAMCS/2019/v34i230211

Editor(s):

(1) Prof. Dr. Sheng Zhang, Department of Mathematics, Bohai University, Jinzhou 121013, Jinzhou, China.

Reviewers:

(1) Tunjo Peri, University of Zagreb, Croatia.

(2) Josimar da Silva Rocha, Universidade Tecnolgica do Paran, Brazil.

(3) A. C. Wimal Lalith de Alwis, Sri Lanka.

Complete Peer review History: http://www.sdiarticle4.com/review-history/51504

***Received: 20 July 2019***

***Accepted: 24 September 2019***

***Published: 22 November 2019***

***Original Research Article***

## Abstract

The author presents a simple approach which can be used to tackle some well-known Diophantine problems. A self-contained argument is used to furnish a novel proof of one such result first stated by Pierre de Fermat in the 1630s.

*Keywords: Diophantine; equations; Fermat; elementary; proof; factorize.*

## 1 Introduction

Define $n$ to be any integer such that $n > 1$. Suppose that $a, b, c$ each constitute a general set of all positive integers satisfying

$$c^n = a^n - b^n, \tag{1.1}$$

where $a > b > c$. It is easily established that

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}). \tag{1.2}$$

Some special cases of the insolubility of (1.1) have been examined in both [1] and [2]. Up until now, the proof of Fermat's Last Theorem has been regarded as being a consequence of the modularity

**Corresponding author: E-mail: bibek010101@gmail.com;*

theorem for semistable elliptic curves which was proved in [3] and [4] by Wiles and Taylor, both of whom had paved the way for the proof of the full modularity theorem (in [5], [6] and [7]) which settled a longstanding conjecture formulated by Taniyama, Shimura and Weil. However, these profound accomplishments have acquired such a great deal of admiration that they have significantly strengthened the prevailing belief that any proof of Fermat's Last Theorem lies far beyond the scope of more direct elementary methods. A new proof showing that (1.1) is insoluble for $n \geq 3$ is provided in the subsequent section. The following lemma is a very simple yet stunningly powerful result, as it asserts that if (1.1) holds then $n$ must be strictly bounded from above by $c$.

# 2 Analysis

**Lemma 1.** *Suppose that $n \geq c$. Then (1.1) has no solution.*

*Proof.* Let

$$M = (a^{n-1} + a^{n-2}b + \ldots + b^{n-1}). \tag{2.1}$$

By using the fact that $a > b > c$ and that there are $n$ terms on the right hand side of (2.1), it can be deduced that $M > nc^{n-1}$. Since $n \geq c$, it follows that $M > c^n$. This leads to a contradiction, because it is evident from (1.1), (1.2) and (2.1) that $M \leq c^n$. The statement of the lemma follows. □

*The next lemma is a very basic result which is included for the sake of completeness.*

**Lemma 2.** *Suppose that $x, y, z$ are any distinct positive integers such that*

$$z^{\nu} = x^{\nu} + y^{\nu}, \tag{2.2}$$

*where $x < y < z$ and $\nu$ is some integer strictly greater than 1. Then $\nu$ is a unique integer.*

*Proof.* Suppose that $m$ is some nonzero integer such that

$$z^{\nu+m} = x^{\nu+m} + y^{\nu+m}. \tag{2.3}$$

By multiplying both sides of (2.2) by $z^m$, it is clear that

$$z^{\nu+m} = x^{\nu+m} \cdot \left(\frac{z}{x}\right)^m + y^{\nu+m} \cdot \left(\frac{z}{y}\right)^m. \tag{2.4}$$

Since $x < z$ and $y < z$, the right hand side of (2.4) is either larger or smaller than that of (2.3) if $m > 0$ or $m < 0$, respectively. However, the left hand sides of both (2.3) and (2.4) are equal to each other. This contradiction negates the assumption that there exists some nonzero integer $m$. The statement of the lemma follows easily. □

**Theorem 1.** *Suppose that $n \geq 3$. Then (1.1) has no solution.*

*Proof.* Recall that the triple $(a, b, c)$ is regarded as being a general solution of (1.1) for any integer $n$ greater than or equal to 2. Consider a distinct solution of (1.1) so that $(a, b, c) = (a_1, b_1, c_1)$ in this special case, where $a_1, b_1, c_1$ are each distinct positive integers. By considering Lemma 1, it is evident that $1 < n < c$. By considering that $1 < n < c$, where $n$ and $c$ are each represented by a subset of integers, and that $a_1, b_1, c_1$ may share any common factor greater than 1, it follows that $c = f_1(u_1, \ldots, u_i)$, where $f_1$ is a function exclusively represented by one or more possible positive integer-valued functions of necessarily all of the positive indeterminates $u_1, \ldots, u_i$ and $i \geq 1$. For example, in the case when $n = 2$, it is well-known [8] that $a = u_1(u_2^2 + u_3^2)$ and $\{b, c\} \in \left\{u_1(u_2^2 - u_3^2), u_1(2u_2u_3)\right\}$ such that $b > c$, where $u_1, u_2, u_3$ are all positive integers. (Note

that if $n = 1$ was considered, then this would imply that $c = f_1(u_1) = u_1$, where $i = 1$, so that $c$ could be any positive integer, $b$ could be any integer strictly greater than $c$ such that $b \geq 2$, and $a$ is equal to the sum of $b$ and $c$ such that $a \geq 3$ by using (1.1). It is clear that $c$ cannot be any positive integer for $n \geq 2$ since $a > b > c \geq 3$ from an application of Lemma 1. For all $n \geq 2$ satisfying (1.1), it follows that $c$ is equal to a function of $u_1, \ldots, u_i$ which is different from what it would be for $n = 1$. Similar arguments apply for $a$ and $b$. Hence the case where $n = 1$ can be disregarded.) Since $n$ and $c$ are each represented by a subset of integers such that $1 < n < c$, it is possible to distinguish two separate cases which characterize $n$. In the first case, $n$ can be expressed by some function $f_2$ of indeterminates which (since $1 < n < c$) in fact are all also used in $f_1$ to determine $c$, so that $n = f_2(u_1, \ldots, u_i)$. In the second case, $n$ is independent of $u_1, \ldots, u_i$ such that it is given by a positive number of fixed integers which are strictly greater than 1 and strictly less than $c$. Suppose that $p$ is any given prime. It can then be determined from (1.1) that the value of $n$ is identical for both the special solutions $(a_1, b_1, c_1)$ and $(a_1 \cdot p, b_1 \cdot p, c_1 \cdot p)$. Assume that $n$ can be written as $n = f_2(u_1, \ldots, u_i)$. The last two statements imply that $n$ is expressible (in terms of one or more of $u_1, \ldots, u_i$ with no other unknowns) as an improper fraction in which no summand from either the numerator or denominator is a unique nonzero integer constant, because, by considering that $f_1(u_1, \ldots, u_i) = c_1 \cdot p$ in the case of the special solution given by $(a_1 \cdot p, b_1 \cdot p, c_1 \cdot p)$ and that for $1 \leq r \leq i$ every $u_r$ can be replaced by $p \cdot u_r$, the same power of $p$ can be factored out of both the numerator and denominator of this top-heavy fraction representing $n$. It follows that the denominator of this improper fraction expressing n is given by $g(u_1, \ldots, u_i)$, where $g$ is some function of necessarily all of $u_1, \ldots, u_i$. Since $n$ is an integer, this implies that the corresponding numerator of the same improper fraction is given by $n \cdot g(u_1, \cdots, u_i)$. Then

$$n = \frac{n \cdot g(u_1, \ldots, u_i)}{g(u_1, \ldots, u_i)}. \tag{2.5}$$

By substituting the right hand side of (2.5) into $n$ on the right hand side of (2.5) and then cancelling common terms, it is apparent that $n$ need not be a function of $u_1, \ldots, u_i$. This contradicts the assumption made earlier that $n$ can be expressed by some function of indeterminates. Hence $n$ is given by one or more fixed integers strictly less than $c$, and $n$ is independent of $u_1, \ldots, u_i$. Since $c = f_1(u_1, \ldots, u_i)$, it follows that $n$ need not be expressed as a function which contains $c$. Similarly, by replacing $c$ with $a$ and $b$ in the preceding arguments (except in the reasoning used earlier to disregard the case where $n = 1$ in which $a$ and $b$ are already considered) involving $f_1$ respectively, it is evident that $n$ need not be expressed as a function of $a, b, c$, i.e. $n$ is independent of $a, b, c$. Recall that it has been established that $n$ need not be expressed by any function of indeterminates. By considering (1.1) with the last two sentences and by applying Lemma 2, it is easily seen that $n$ must be a unique integer which is strictly less than $c$, regardless of the permissible values of $(a, b, c)$. Recall that it may be assumed without loss of generality that $n > 1$. By noting it was mentioned earlier that (1.1) can hold if $n = 2$ and $i = 3$, the desired result follows as a consequence of the last two statements. □

# 3 Conclusion

Fermat's Last Theorem has been established by using an elementary proof. The reasoning involved is accessible to the general public, and it was motivated by the fundamental inequality in Lemma 1.

# Acknowledgement

We thank the Editor and the referees for their comments.

## Competing Interests

The author has declared that no competing interests exist.

## References

[1] Hardy GH, Wright EM. An introduction to the theory of numbers. 4th Edition, Oxford University Press. 1960;190-195.

[2] Ribenboim P. Fermat's last theorem for amateurs. 1st Edition. Springer Verlag. 1999;3-71.

[3] Wiles A. Modular elliptic curves and Fermat's last theorem. Annals of Mathematics. 1995;141(3):443-551.

[4] Wiles A, Taylor R. Ring theoretic properties of certain Hecke algebras. Annals of Mathematics. 1995;141(3):553-572.

[5] Diamond F. On deformation rings and Hecke rings. Annals of Mathematics. 1996;144(1):137-166.

[6] Conrad B, Diamond F, Taylor R. Modularity of certain potentially Barsotti-Tate Galois representations. Journal of the American Mathematical Society. 1999;12(2):521-567.

[7] Breuil C, Conrad B, Diamond F, Taylor R. On the modularity of elliptic curves over Q: wild 3-adic exercises. Journal of the American Mathematical Society. 2001;14(4):843-939.

[8] Hollingdale S. Makers of mathematics. 1st Edition, Dover Publications. 2006;9.



***Peer-review history:***
*The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)*
*http://www.sdiarticle4.com/review-history/51504*