British Journal of Mathematics & Computer Science
4(22): 3179-3190, 2014
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

A Simple Short Proof of Fermat's Last Theorem

Fayez Fok Al Adeh[1*]

[1]The Syrian Cosmological Society, P.O. Box, 13187, Damascus, Syria.

Article Information

DOI: 10.9734/BJMCS/2014/12041
Editor(s):
(1) Sheng Zhang, Department of Mathematics, Bohai University, Jinzhou, China.
Reviewers:
(1) Yengkhom Satyendra Singh, Department of Mathematics, Haramaya University, Dire Dawa, Ethiopia.
(2) W. Obeng-Denteh, Mathematics Department, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.
(3) Anonymous, Université Laval, Canada.
Peer review History: http://www.sciencedomain.org/review-history.php?iid=636&id=6&aid=5936

Received: 16 June 2014
Accepted: 06 August 2014
Published: 04 September 2014

Original Research Article

Abstract

Using a theorem closely linked to Fermat's Last Theorem, and borrowing some simple ideas from topology, I formulate a simple short proof of Fermet's Last Theorem.

Keywords: Integer solutions, convergence, topology.
Subj – Class: Number theory, topology, general mathematics.

1 Introduction

Fermat's Last Theorem states that: If N is any natural number greater than two, the equation:

$$X^N + Y^N = Z^N \tag{1}$$

[1] has no solutions in integers ,all different from zero (i.e. it has only the trivial solution ,where one of the integers is equal to zero).

This theorem was first conjectured by Pierre de Fermat in 1637, famously in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin. No successful proof was published until 1995 despite the efforts of countless mathematicians during the 358 intervening years. The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among

**Corresponding author: hayfa@scs-net.org;*

the most famous theorems in the history of mathematics and prior to its 1995 proof by Andrew Wiles was in the Guinness Book of World Records for "most difficult mathematical problems".

Wiles' proof of Fermat's Last Theorem is a proof of the modularity theorem for semistable elliptic curves released by Andrew Wiles, which, together with Ribet's theorem, provides a proof for Fermat's Last Theorem. Both Fermat's Last Theorem and the Modularity Theorem were almost universally considered inaccessible to proof by contemporaneous mathematicians (meaning, impossible or virtually impossible to prove using current knowledge). Wiles first announced his proof in June 1993 [2] in a version that was soon recognized as having a serious gap in a key point. The proof was corrected by Andrew Wiles, in part via collaboration with a colleague, and the final, widely accepted, version was released by Wiles in September 1994, and formally published in 1995. The proof uses many techniques from algebraic geometry and number theory, and has many ramifications in these branches of mathematics. It also uses standard constructions of modern algebraic geometry, such as the category of schemes and Iwasawa theory, and other 20th-century techniques not available to Fermat. The proof itself is over 100 pages long and consumed seven years of Wiles's research time. It is based on hard mathematics.

On the contrary, my proof uses simple ideas from analysis and topology. It is only 11 pages long. In fact, it is simple and short.

2 The Simple Short Proof

In my paper, I employ a very well known theorem which states that [3] **(2)** Theorem: If N, K are integers both ≥ 1, then each of the equations

$$X^N + Y^N = Z^{N+\frac{1}{K}}, \; X^N + Y^N = Z^{NK+1} \tag{2}$$

has infinitely many solutions in integers.

We note that the triple of integers (X, Y, Z) is a solution of the equation

$$X^N + Y^N = Z^{NK+1} \tag{3}$$

if and only if the triple (X, Y, Z^K) is a solution of the equation

$$X^N + Y^N = Z^{N+\frac{1}{K}} \tag{4}$$

From now on, we consider N as an integral exponent greater than two.

Using the usual topology as defined on the real line **R [4]**, we consider the limit of the sequence of exponents $(N + \frac{1}{K})$ for ascending sequence of positive integers K .
This limit is given by:

$$\lim (\mathrm{N} + \frac{1}{\mathrm{K}}) = \mathrm{N} \quad \text{as} \quad \mathrm{K} \to \infty \tag{5}$$

Because of this, we note that if the positive integer K increases, the equations of the form (4) corresponding to ascending values of K appear to approach monotonically equation (1). For this to be true, solutions of equations of the form (4) must come close to corresponding solutions of equation (1) for ascending values of K. In addition, the limit (5) must exist.

In trying to prove the above note, we assume that the triple of positive integers

$$(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) \tag{6}$$

is a solution to equation (1) .

Hence for any integer K, the triple of integers

$$(\mathrm{KX}, \mathrm{KY}, \mathrm{KZ}) \tag{7}$$

is also a solution to equation (1) .

We assume here that the integer K is a positive integer greater than one.

Using theorem (2), we construct now a sequence of triples of integers $(\mathrm{X_K}, \mathrm{Y_K}, \mathrm{Z_K})$, each triple being a solution to equation (4) for some positive integer K.

For every positive integer $\mathrm{K}>1$, we consider the variation $\delta (\mathrm{K^N\ Z^N})$ in $(\mathrm{K^N\ Z^N})$ due to a positive variation $\delta\ \mathrm{N}$ in the exponent N:

$$\delta (\mathrm{K^N\ Z^N}) = (\mathrm{KZ} + \delta (\mathrm{KZ}))^{\mathrm{N} + \delta \mathrm{N}} - (\mathrm{K^N\ Z^N}) \tag{8}$$

where $\delta (\mathrm{KZ})$ is the corresponding variation in (KZ).

From (8) we get:

$$\delta (\mathrm{K^N\ Z^N}) = (\mathrm{KZ} + \delta (\mathrm{KZ}))^{\mathrm{N}} \quad ((\mathrm{KZ} + \delta\ \mathrm{KZ}))^{\delta \mathrm{N}} - (\mathrm{K^N\ Z^N})$$

$$= (\mathrm{KZ})^{\mathrm{N}} \ (1 + \frac{\delta(\mathrm{KZ})}{\mathrm{KZ}})^{\mathrm{N}} \ (\mathrm{KZ})^{\delta \mathrm{N}} \quad (1 + \frac{\delta(\mathrm{KZ})}{\mathrm{KZ}})^{\delta \mathrm{N}} - (\mathrm{K^N\ Z^N}) \tag{9}$$

We assume that the variation of $(\mathrm{K^N\ Z^N})$ vanishes.

$$\delta (\mathrm{K^N\ Z^N}) = 0 \tag{10}$$

The truth of this assumption is based on the fact that all triples (KX, KY, KZ) are solutions to equation (1). In a sense, the values $K^N Z^N$ are stable.

We get from (9)

$$(1+\frac{\delta(KZ)}{KZ})^N \quad (1+\frac{\delta(KZ)}{KZ})^{\delta N} - \frac{1}{(KZ)^{\delta N}} = 0 \tag{11}$$

Let us make the following substitution

$$t = \frac{\delta(KZ)}{KZ} \tag{12}$$

Thus (11) becomes

$$(1+t)^N (1+t)^{\delta N} - \frac{1}{(KZ)^{\delta N}} = 0 \tag{13}$$

We make the following approximation

$$(1+t)^{\delta N} = 1+t\delta N \tag{14}$$

Hence (13) transforms into

$$(1+t)^N (1+t\delta N) - \frac{1}{(KZ)^{\delta N}} = 0 \tag{15}$$

$$\text{i.e. } (1+t)^N + t\delta N (1+t)^N - \frac{1}{(KZ)^{\delta N}} = 0$$

that is

$$(1+Nt+\cdots\cdots\cdots\cdots)+t\delta N (1+t)^N - \frac{1}{(KZ)^{\delta N}} = 0 \tag{16}$$

Hence

$$(Nt+\cdots\cdots\cdots\cdots)+t\delta N (1+t)^N + (1-\frac{1}{(KZ)^{\delta N}}) = 0 \tag{17}$$

Since $N > 2$, we truncate the sum

($\mathrm{N\,t} + \cdots\cdots\cdots$) at an odd power s of t ,i.e. we let

$$(\mathrm{N\,t} + \cdots\cdots\cdots) \text{ equals approximately } (\mathrm{N\,t} + \cdots\cdots\cdots + \frac{\mathrm{N}.....(\mathrm{N}-(s-1))}{s!}\ \mathrm{t}^{\,s}) \qquad (18)$$

As to the term $\mathrm{t}\,\delta\mathrm{N}\ \ (1+\mathrm{t})^{\mathrm{N}}$, we expand $(1+\mathrm{t})^{\mathrm{N}}$ and truncate the expansion at the even power (s – 1) of t, i.e. we let

$$(1+\mathrm{t})^{\mathrm{N}} \text{ equals approximately } (1+\mathrm{N\,t} + \cdots\cdots\cdots + \frac{\mathrm{N}.....(\mathrm{N}-(s-2))}{(s-1)!}\ \mathrm{t}^{s-1}) \qquad (19)$$

After multiplying this approximation by $\mathrm{t}\,\delta\mathrm{N}$ we rearrange the terms of the equality (17). As a result, equality (17) becomes an equation of odd degree s in the unknown t. All the coefficients of this equation will be positive. Since this equation is of odd degree, it has at least one real root. And since all of its' coefficients are positive, this real root cannot be positive or zero, it must be negative, i.e.

$$\mathrm{t} < 0 \qquad (20)$$

From (12) we deduce that

$$\delta(\mathrm{KZ}) < 0 \qquad (21)$$

This means that varying the exponent N be an amount $\delta\mathrm{N}$ results in a negative variation in KZ, i.e. KZ decreases by an amount $\left|\delta(\mathrm{KZ})\right|$.

Now we approximate $\delta\mathrm{N}$ by $\frac{1}{\mathrm{K}}$, i.e. we let

$$\delta\mathrm{N} = \frac{1}{\mathrm{K}} \qquad (22)$$

Hence if we vary the exponent N by an amount $\frac{1}{\mathrm{K}}$, (KZ) will decrease by an amount $\left|\delta(\mathrm{KZ})\right|$.

Now, according to theorem (2), we can find a triple of integers ($\mathrm{X_K}$, $\mathrm{Y_K}$, $\mathrm{Z_K}$) which is a solution to equation (4) and such that $\mathrm{Z_K}$ is a positive integer which satisfies the condition that the absolute value $\left|\ (\ \mathrm{KZ} - \left|\delta(\mathrm{KZ})\right|\ )\ -\ \mathrm{Z_K}\ \right|$ is a minimum, i.e.

$$\left| \left(KZ - Z_K \right) - \left| \delta(KZ) \right| \right| \text{ is a minimum.} \tag{23}$$

Thus we have succeeded in constructing a sequence of triples of integers, each triple (X_K , Y_K , Z_K) being a solution to equation (4) for some positive integer K.

Condition (23) entails that

$$\left| \left(KZ - Z_K \right) \right| = O \left| \delta(KZ) \right| \text{ for large enough values of } K \text{, where O is the big oh notation .} \tag{24}$$

To the triple (X_K , Y_K , Z_K) we let correspond the triple (KX, KY, KZ)

Which is a solution to equation (1).This is justified be equality (23)

We now calculate

$$\lim \left(\delta(KZ) \right) \text{ as } K \to \infty \tag{25}$$

To this end, we substitute from (22) in (11) and get

$$\left(1+ \frac{\delta(KZ)}{KZ} \right)^N \quad \left(1+ \frac{\delta(KZ)}{KZ} \right)^{\frac{1}{K}} = \frac{1}{(KZ)^{\frac{1}{K}}} \tag{26}$$

$$\text{i.e } \left(1+ \frac{\delta(KZ)}{KZ} \right)^{KN+1} = \frac{1}{KZ}$$

$$\left(1+ \frac{\delta(KZ)}{KZ} \right) = \frac{1}{(KZ)^{\frac{1}{KN+1}}}$$

That is

$$KZ + \delta(KZ) - (KZ)^{\frac{KN}{KN+1}} = 0 \tag{27}$$

We take the limit of (27) as $K \to \infty$

First we calculate

$$\lim_{K \to \infty} (KZ)^{\frac{KN}{KN+1}} \tag{28}$$

For this we calculate:

$$\lim_{K \to \infty} \log\left((KZ)^{\frac{KN}{KN+1}}\right) = \lim_{K \to \infty} \left(\frac{KN}{KN+1} \log(KZ)\right) \tag{29}$$

$$= \lim_{K \to \infty} \log(KZ)$$

Therefore we deduce that

$$\lim_{K \to \infty} \left((KZ)^{\frac{KN}{KN+1}}\right) = \lim_{K \to \infty} (KZ) \tag{30}$$

Hence we have for the limit of (27)

$$\lim_{K \to \infty} \left(KZ + \delta(KZ) - (KZ)^{\frac{KN}{KN+1}} = 0\right) \tag{31}$$

$$\text{i.e. } \lim_{K \to \infty} \left(KZ + \delta(KZ) - KZ = 0\right)$$

We conclude that

$$\lim_{K \to \infty} (\delta(KZ)) = 0 \tag{32}$$

From (24) we deduce that

$$\lim_{K \to \infty} \left| (KZ - Z_K) \right| = 0 \tag{33}$$

We conclude from the above that for every positive integer.

$K > 1$ we can find a triple of integers (X_K, Y_K, Z_K) which is a solution to equation (4). For this triple, we can find a corresponding triple of integers (KX, KY, KZ) which is a solution to equation (1) and such that the absolute value $\left| (KZ - Z_K) \right|$ is a minimum. The triples (X_K, Y_K, Z_K) and (KX, KY, KZ) come close to each other as $K \to \infty$. In a sense, the equations of the form (4) corresponding to ascending values of K approach monotonically equation (1).

Consider now the triple of rational numbers

$$(\frac{X_K}{K},\frac{Y_K}{K},\frac{Z_K}{K}) \tag{34}$$

Substitute this triple in equation (4) and get

$$(\frac{X_K}{K})^N+(\frac{Y_K}{K})^N=(\frac{Z_K}{K})^{N+\frac{1}{K}} \tag{35}$$

$$\text{i.e. } {X_K}^N+{Y_K}^N={Z_K}^{N+\frac{1}{K}}\times\frac{1}{K^{\frac{1}{K}}}$$

Therfore, we deduce that, for large enough values of K and to a very good approximation. The triple (34) is a solution to equation (4). Moreover, the triples (34) converge to triple (6) as $K\to\infty$.

In fact, as $K\to\infty$ equality (35) induces the equality

$$X^N+Y^N=Z^N \tag{36}$$

All in all, we have the following result:

Result: equations of the form (4) converge to equation (1) as $K\to\infty$. The truth of this result is based on the existence of the limit (5).

(37)

For the result (37) to be true, we must appeal to theorem (2) and check the validity of this result on the basis of that theorem. In other words, the result (37) cannot be true unless we can formulate and prove a similar result with equation (3) replacing equation (4). For the new result to be true, a limit like the one in (5) must exist for exponents of equations of the form (3) whenever K increases without limit.

Following similar steps as above we can calculate $\delta(KZ^K)$ and deduce that

$$\delta(KZ^K)<0 \tag{38}$$

and that

$$\lim_{K\to\infty}(\delta(KZ^K))=0 \tag{39}$$

Now according to theorem (2), we can find a triple of integers $({X_K},{Y_K},{Z_K}^K)$ which is a solution to equation (4) and such that ${Z_K}^K$ is a positive integer which satisfies the condition that

$$\left|\ (KZ^K-\left|\delta(KZ^K)\right|)-{Z_K}^K\ \right| \text{ is a minimum.} \tag{40}$$

Thus we deduce that

$$\left|\ (KZ^K-{Z_K}^K)-\left|\delta(KZ^K)\right|\ \right| \text{ is a minimum.} \tag{41}$$

i.e.

$$\left| \left(KZ^K - Z_K{}^K \right) \right| = O\left(\left| \delta(KZ^K) \right| \right) \tag{42}$$

for large enough values of K where O is the big oh notation

According to (39) we have

$$\lim_{K \to \infty} \left| \left(KZ^K - Z_K{}^K \right) \right| = 0 \tag{43}$$

That is

$$\lim_{K \to \infty} \left(\frac{Z_K}{K^{\frac{1}{K}}} = Z \right) \tag{44}$$

Since the triple $(X_K , Y_K , Z_K{}^K)$ is a solution to equation (4) , then the triple (X_K , Y_K , Z_K) is a solution to equation (3)

$$X_K{}^N + Y_K{}^N = \left(Z_K{}^K \right)^{N+\frac{1}{K}} \tag{45}$$

$$\text{i.e. } X_K{}^N + Y_K{}^N = Z_K{}^{KN+1}$$

As we have done above, we let the triple $(X_K , Y_K , Z_K{}^K)$ correspond to the triple (KX , KY , KZ^K) . This is justified following equality (42). Also we note that the triple $(\frac{X_K}{K} , \frac{Y_K}{K} , \frac{Z_K{}^K}{K})$ is an approximate solution to equation (4) . This means that the triple $(\frac{X_K}{K} , \frac{Y_K}{K} , (\frac{Z_K{}^K}{K})^{\frac{1}{K}})$ is an approximate solution to equation (3). This can be checked as follows:

$(\frac{X_K}{K})^N + (\frac{Y_K}{K})^N = ((\frac{Z_K{}^K}{K})^{\frac{1}{K}})^{KN+1}$ approximately i.e.

$(\frac{X_K}{K})^N + (\frac{Y_K}{K})^N = (\frac{Z_K{}^K}{K})^{N+\frac{1}{K}}$ approximately hence

$$X_K{}^N + Y_K{}^N = Z_K{}^{KN+1} \times \frac{1}{K^{\frac{1}{K}}} \tag{46}$$

Comparing with (45), the result follows.

It is a very good approximation for large enough values of K.

Using (44) we deduce that

$$\lim_{K \to \infty} \left(\frac{Z_K^{\,K}}{K}\right)^{\frac{1}{K}} = \lim_{K \to \infty} \frac{Z_K}{K^{\frac{1}{K}}} = \lim_{K \to \infty} Z = Z \tag{47}$$

We conclude that the triples $\left(\frac{X_K}{K}, \frac{Y_K}{K}, \left(\frac{Z_K^{\,K}}{K}\right)^{\frac{1}{K}}\right)$ each of which is an approximate solution of an equation of the form (3) for some value of K , converge as K approaches infinity to the triple (X, Y, Z).

Which is a solution to equation (1).

We now formulate a new result similar to the result (37)

New result: equations of the form (3) converge to equation (1) as K approaches infinity (48). Amalgamating theorem (2) with result (37) and remembering that the truth of result (37) is based on the existence of the limit (5), we deduce that the truth of the new result (48) necessitates the existence of a similar limit to the exponents of equations of the form (3).

That is we must show that

$$\lim_{K \to \infty} (KN + 1) = N \text{ in some suitable topology.} \tag{49}$$

The necessity of the existence of this limit becomes evident upon viewing equations (1) and (3). We search now for a suitable topology to check the existence of the limit (49). It is known that the class of open intervals (a, b) with rational endpoints a, b is countable and is a base for the usual topology on the real line. Since the exponents ($KN + 1$) we are dealing with now are all integers, we form the class of all intersections of these open intervals (with rational endpoints) with the set of integers **Z**.

We get the relative topology on the set **Z**. It is an easy exercise to prove that the relative topology in this case is the discrete topology.

This means that each singleton containing any integer, and especially the singleton { N } is an open set. Hence N is not the limit of any sequence of integers in this topology.

Therefore, the limit in (49) does not exist. This means that the formulation and proof of the sought after new result (48) is not justified. Returning to theorem (2) we deduce that the result (37) is not

valid. The final conclusion is that our original assumption that equation (1) has a non – trivial solution in integers, is not true.

We can arrive at this final conclusion via another route by using a different topology.

3 Reviewing Topology

To this end, we consider the following curious topology on the set **Z** of integers. [5] For a, b ∈ **Z**, b > 0 we set

$$N_{a,b} = \{ a + mb : m \in \mathbf{Z} \} \tag{50}$$

Each set $N_{a,b}$ is a two way infinite arithmetic progression .Now call a set $O \subseteq \mathbf{Z}$ open if either O is empty, or if to every $a \in O$, there exists some $b > 0$ with $N_{a,b} \subseteq O$. Clearly, the union of open sets is open again. If O1,O2 are open ,and $a \in O1 \bigcap O2$ with $N_{a,b1} \subseteq O1$ and $N_{a,b2} \subseteq O2$, then $a \in N_{a,b1b2} \subseteq O1 \bigcap O2$. So we conclude that any finite intersection of open sets is again open. So, this family of open sets induces a bona fide topology on **Z**.

Now we consider the open set:

$$N_{0,} \mathbf{N} \tag{51}$$

in this curious topology.

Any element belonging to this set can be written in the form

$$\mathbf{N} m \quad m \in \mathbf{Z} \tag{52}$$

Note that

$$\mathbf{N} \in N_{0,} \mathbf{N} \text{ (take m = 1)} \tag{53}$$

Assume that an exponent ($KN+1$) belongs to this set i.e.

$$(KN+1) = \mathbf{N} m \; m \in \mathbf{Z}, \; K > 1 \tag{54}$$

This means that

$$\mathbf{N} (m - K) = 1 \qquad (N > 2) \tag{55}$$

But this is an impossible equation.

Therefore we deduce that for every $K > 1$

$$(KN+1) \text{ does not belong to } N_{0,} \mathbf{N} \tag{56}$$

This means that $\mathbf{N}$ is not a limit of the sequence of exponents $(KN+1)$ in the curious topology.

Therefore, the limit in (49) does not exist. This means that the formulation and proof of the sought after new result (48) is not justified. Returning to theorem (2) we deduce that the result (37) is not valid. The final conclusion is that our original assumption that equation (1) has a non – trivial solution in integers, is not true.

This concludes the proof of Fermat's Last Theorem.

4 Conclusion

I have shown in my paper, that for any complicated problem like Fermats' Last Theorem, there always exists a simple short proof. It needs some contemplation.

Competing Interests

Author has declared that no competing interests exist.

References

[1] Borevich ZI, Shafarevich IR. Number theory. New York: Academic Press; 1966.

[2] Ribenboim, Paulo. Fermat's last theorem for amateurs. New York: Springer – Verlag; 1999.

[3] Ribenboim, Paulo. 13 lectures on Fermat's last theorem. New York: Springer –Verlag; 1979.

[4] Lipschuts, Seymour. Theory and problems of general topology. New York: Schaum Publishing Co; 1965.

[5] Steen, Lynn Arthur, Seebach Jr, Arthur Seebach J. Counterexamples in topology. New York: Springer – Verlag; 1978.

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)
www.sciencedomain.org/review-history.php?iid=636&id=6&aid=5936