Sch J Appl Sci Res 2019
Volume 2: 4

InnoVationInfo Scholar Journal of Applied Sciences and Research

A Simple Proof of Fermat's Last Theorem

JE Brierly*
Takashi Ito
Hidegoro Nakano

Department of Mathematics, Wayne State University, Detroit, Michigan, USA

Introduction

Fermat claimed to prove his last theorem in the 17th century but was unable to fit it into the margin of his manuscript. Since then, many generations of mathematicians have attempted to find a simple proof to his last theorem. Some mathematicians believe that Fermat was mistaken in claiming that he had a clever solution to his last theorem. Examples of false proofs supposedly are found in Fermat's manuscripts as corroboration that Fermat was capable of error. It is also well-documented that many errors occur in respected and current refereed journals. For example, Glivenko's Theorem, appeared in the highly renown book by Birkhoff on Lattice theory for many years with what was purported to be a proof of it. A doctoral student of Nakano's at that time studying at Wayne State university found the proof to be in error. He and Nakano published a correct proof of the theorem, subsequently. No doubt many fine mathematicians read over the proof without catching the error during the many years of the book's circulation.

Mathematics can be perversely subtle at times. Difficult and/or tricky proofs require many reviews over years to establish their veracity, conclusively. Consider, for example, that the Four Color Problem was first proposed in 1852 and the first claimed proof by Alfred Bray in 1879 using an argument known as the Kempke Chain method was found to be wrong eleven years later. Eighty years after that a computer proof for the famous problem was claimed by Hakim and Appel in 1976. In the nineties the computer proof was found to have errors by several mathematicians working jointly who published an improved version correcting computer code and fixing parts of the proof using standard proving methods. It is still questionable whether a proof relying on a highly complex computer operating system algorithm known to almost assuredly have errors in it can be the platform for proving a difficult theorem in mathematics. Purists would argue the impracticality of such proofs.

In 1993, Andrew Wiles from Princeton University claimed a solution to the famous Fermat's Last Theorem as a corollary to his research results. Later, he recanted. According to Wiles the review process of his first attempt to prove a needed special case of the Shamura-Taniyama-Weal conjecture produced a number of unanswered questions. By December 1993, Wiles claimed that most of the objections were resolved, but one major objection still had to be addressed. In 1994, Wiles finally claimed to have a flash of insight in modifying one of his previously abandonned methods to answer the last and most serious objection. Wiles had the proof reviewed by three of his colleagues who added improvements and agreed that the proof was on solid ground. Regardless of Wile's somewhat restricted review by three colleagues, only time will tell whether there are not more errors of omission or commission in his claimed proof. After all is said and done, the review

Article Information

Article Type: Analysis Article
Article Number: SJASR226
Received Date: 27 March, 2019
Accepted Date: 03 April, 2019
Published Date: 10 April, 2019

***Corresponding author:** JE Brierly, Department of Mathematics, Wayne State University, Detroit, Michigan, USA. Tel: 248-229-7909; Email: jbrierly(at)comcast.net

Citation: Brierly JE, Ito T, Nakano H (2019) A Simple Proof of Fermat's Last Theorem. Sch J Appl Sci Res Vol: 2, Issu: 4 (26-29).

Copyright: © 2019 Brierly JE. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

process is in reality an ongoing process that must take place over years by many mathematicians.

Proofs are best when they are short and comprehensible by many. Still, a lengthy review process is required even in this case. In 1991, the author found a simple standard proof for the Four Color Problem and generalized its solution to N dimensions. The author considers his proof to be airtight. Yet, the proof has not been accepted by the mathematical world to this day. The author challenges anyone to find fault with the proof at this time. Many have tried without success. Shortly after publicizing the proof, some objections were submitted to the author. All were addressed. Most were simple misunderstandings. None were strong enough to negate the proof. A few of the objections resulted in modifications, however. Specifically, Yue Zhao forced the author to correct one of the key results used to prove the Four Color Theorem. Another comment by Professor Vandervate at Georgia Tech resulted in tightening the definition of hyper-planarity.

Comments and criticisms are still welcomed by the author on his proof and generalization of the Four Color Problem. The most current annotated version of the proof which has not changed in many years is available on the author's website interjetic.com. All are welcome to attempt to invalidate either the author's

Four Color or Fermat's last theorem proof. The author believes in an open review not just restricted to his circle of mathematical acquaintances which are few in number due to not being a professor at a major university.

Before attempting the Four Color Problem the author considered devoting energy to solving the Fermat's Last Problem, but opted in favor of addressing the Four Color Problem, because intuitively he felt that it was a more important problem and possibly generalizable to N dimensions making it applicable to applied mathematics, engineering, and physics. This all proved true.

Since retiring from a lengthy career with the Department of Defense the author has decided to become interested in solving difficult and well-known problems in mathematics, again. Finding a simple proof to Fermat's Last Theorem became the author's main objective in year 2002. After six months of experimentation, the author finally devised a simple proof for the famous problem using only methods that could have been known by Fermat in the seventeenth century. The proof is quite innovative, but short and relatively easy to understand. The author invites comments and criticisms via the aforementioned website on the solution. By the time the proof appears in the author's website it will be copyrighted and available for anyone interested in reviewing it. At that time the author did not intend to attempt to publish the proof in any professional journal, only in his website. And, if anyone succeeded in finding an error of omission or commission, the author would have retracted the claim until the objection became resolved.

The proof begins by first listing the main theorems employed.

List of Reference Theorems:

Theorem 1: (DesCartes) For a polynomial $p(x)=\Sigma a_k x^k (k=0,1...N)$ with a_k integral the only possible roots are of the form p/q where p and q are relatively primed and p divides a_0 while q divides a_N

Binomial theorem: $(a+b)^n = \Sigma B_j a^{n-j} b^j$ where $B_j=n!/((n-j)!j!)$ j=0,1,,n, 0!=1 and n!=n(n-1)...1

Note that only the integral form of the binomial theorem is required for the proof, a result proven by finite induction in many elementary college algebra books. As all mathematicians know the binomial coefficients B_j have the important interpretation of being the number of finite elements of size j from a set of size n. Therefore, binomial coefficients are always integral and nonzero.

Statement of Fermat's Last Theorem

There exists no integer N greater than 2 for which $a^N+b^N=c^N$ where a, b, and c are non-zero integers.

Proof of fermat's last theorem:

It is required to only prove Fermat's Theorem for integral a, b, and c greater than 0, since all other cases may be reduced to this case. For example, suppose b is negative while a and c are positive. If N is even, then $b^N=(-b)^N$. In this case, replace b with -b and the Fermat equation is in the desired format. If N is odd, then $-(-b)^N=b^N$. Thus, the Fermat relation becomes $c^N=a^N-(-b)^N$ which is equivalent to $c^N+(-b)^N=a^N$ in the positive integral form of the fermat equation. All other such cases are resolved using the same methodology.

We begin the proof by assuming that there exists three integers greater than zero and N>2 satisfying $a^N+b^N=c^N$. Without any loss of generality we may assume that a>b. If a=b then the proof that the square root of 2 is irrational applies to yield an obvious contradiction. There must exist a unique positive integer R such that a+R=c. We can also view the Fermat problem viewed with R as an integer variable. We apply the binomial theorem to obtain

(A) $a^N+b^N=(a+R)^N= \Sigma B_j a^j R^{N-j}$ (j=0,1..N)

When j=N we have $B_N=a^N$. So, we can subtract a^N from both sides of the above relation to rewrite it as a polynomial equation in R:

(B) $\Sigma B_j a^j R^{N-j} -b^N =0$ (j=0,1,...N-1)

Alternatively, we can write (A) as a polynomial in a:

(C) $a^N+b^N=(a+R)^N= \Sigma B_j a^{N-j} R^j$ j=0,...N which may be expanded explicitly as an N-1 degree polynomial equation in powers of a to get

(D) $B_1 R a^{N-1}+B_2 R^2 a^{N-2}+...B_{N-1} R^{N-1} a^1 +R^N-b^N =0$

Theorem 1 implies that a=p/q where p,q are relatively primed and q divides $B_1 R$ and p divides R^N-b^N i.e. There exists nonzero integers k_1 and k_2 satisfying $B_1 R=qk_1$ and $R^N-b^N=pk_2$.

We observe that k_1, k_2, B_1, R, p, q, and b are all nonzero positive integers.

Combining the two foregoing equations we may assert that

$a=p/q= (k_1/k_2)(R^N-b^N)/B_1R$

which may be solved for $R^N -b^N$ to get

$R^N-b^N = aB_1Rk_2/k_1$

Substituting in (D), factoring out common factors, a and R, and rearranging yields a new polynomial in R of degree N-2.

(E) $B_{N-1}R^{N-2}+aB_{N-2}R^{N-3}+....+a^{N-3}B_2R+B_1a^{N-2}+B_1k_2/k_1 =0$

So, we have two polynomial equations in R, (B) and (E), one of degree N-2 and the other of degree N. We observe in passing that the polynomial equation in (E) has only integral terms due to the subset sizing combinatorics mentioned and that the remaining terms in equation (E) not involving B_1k_2/k_1 must be integral. This forces k_1 to be an integral divisor of B_1k_2.

In addition, at most one of the like powered coefficients of the two polynomial equations in R can be equal. It is only necessary to check the polynomial term's coefficients in powers of j=2 to N-1, because it is easily seen true for j=0,1 and j=N. Since $-b^N$ is negative and $a^{N-2}B_1+Nk_2/k_1$ is positive the assertion is true for j=N. (E) has zero coefficients for the R^N and R^{N-1} terms whereas (B) does not verifying the case when j=0 and j=1.

Comparing the two polynomial equations shows that corresponding coefficients can be equal for some j=2 to N-1 only when $B_ja^j=B_{N-j+1}a^{j-2}$ which implies $a^2=B_{N-j+1}/B_j$. This equation in j can be satisfied for at most one value of j implying polynomials (B) and (E) can have at most one pair of corresponding coefficients equal. Equivalently, we have established that corresponding coefficients are unequal for at least one pair of corresponding coefficients of (B) and (E), because N is greater than 2. This is an important piece of the proof because were it not so then one might argue that potentially all of the nonzero coefficients of (E) are equal to the ones of corresponding powers of polynomial (B). A nontrivial value for R would be possible in this case. After subtraction of polynomial (E) from (B) one might end up with a polynomial $c_nR^n+c_{n-1}R^{n-1}=0$ that has a solution where R is integral and greater than zero.

Next we show how to devise an algorithm for proving that either of the two distinct polynomial equations in R cannot have a solution other than R=0 after applying the algorithm repeatedly. Though it is important to note that the polynomials in powers are true polynomials in the sense that each may have solutions independent of the other. R is clearly a polynomial variable obtained from the assumptions and the Binomial Theorem applicable to both a and b separately. The polynomial forms derived this way are true equations where each admits possibly more than one solution for R of their own. R is a variable and must be the value that is arrived at via the algorithm since none of the steps reducing the degrees of the algorithm could negate the value of R arrived at when the algorithm terminates! So, when we apply Descartes theorem, we are viewing the theorem as an abstraction of the polynomial forms in R associated with solving the Fermat problem.

The algorithm is perfectly applicable to any pair of polynomials in x. So, Abstractly, the algorithm proceeds for polynomials in x by looking at two polynomial equations of degree N and M where both N and M are greater than 2. Let the equations be given as $\Sigma a_ix^i=0$ i=0,1...N and $\Sigma b_ix^i=0$ i=0,1...M. Suppose that a_i is unequal to b_i for at least one i. The initial coefficients a_0 and b_0 may be zero along with several successive coefficients of higher power. Simply factoring out the highest possible power of x for each polynomial yields new polynomials with a_0 and b_0 nonzero. The only stipulation is that when one uses factoring to obtain nonzero values for a_0 and b_0 that the polynomials do not both become of degree 2 or less so that the algorithm is inoperable. e.g. $x^4+2x^3=0$ reduces to x+2=0 by factoring out x^3.

The algorithm goes as follows:

if a_0 or b_0 =0, then factor out x to reduce the degree of the polynomial equation. The result will be two polynomials in x having nonzero constant terms. We assume that the resulting values of N and M after factoring satisfy at least one of N or M is greater than 2 while the other is at least of first degree with both having nonzero constant terms. Next reduce the polynomial of highest degree down by multiplying each by the nonzero constant term of the other and then subtracting the polynomial of smallest degree from the one of largest degree. This will result in another polynomial with a zero constant term. Factor out the assumed-to-be nonzero x to some power from the new polynomial to obtain a new polynomial of one or more degree lower and with a nonzero constant term. Continue this process working with any pair of the newly generated and existing polynomials of lowest degrees to finally terminate with a polynomial of the form Fx=0. If F cannot be zero and there must exist a nontrivial solution to the equation, Fx=0, then x must be zero. It is possible, however, that there may not be a valid nonzero x that satisfies the two initial polynomials, simultaneously. The algorithm sounds complicated but in practice it is quite simple. See the example shown at the end of this article.

The salient fact is that when the algorithm is applied to the polynomials in R, (B) and E), the resulting F has to be nonzero forcing R to be zero contrary to assumption that R must satisfy One or both equations (B) and (E). R=0 does not satisfy either of the original equations, because the constant term on (B) is negative whereas the constant term on (E) is positive. When the algorithm arrives at the point where we have generated a polynomial of degree 1 then it is only necessary to apply the algorithm one more time to wind up with an equation of the form FR=0. The algorithm applied to the polynomials generated by assuming that $a^N+b^N=c^N$ is true for integers a,b and c and N>2 implies that R must be equal to zero contrary to the assumption that R has to be nonzero for the fermat equation to hold for N>2. This contradiction establishes Fermat's Theorem.

To help the reader understand the way the algorithm proceeds a numerical example is given next.

Example of algorithm computation

$4x^3-3x^2+2x+1=0 \rightarrow 2(4x^3-3x^2+2x+1)=0 \rightarrow 5x^4+8x^3-4x^2+5x=0$

$5x^4+ +2x^2+ x-2=0 \rightarrow 5x^4+ 2x^2+ x-2=0$

$\rightarrow x(5x^3+8x^2-4x+5)=0 \rightarrow 5x^3+8x^2-4x+5=0 \rightarrow 5x^3+8x^2-4x+5=0$

$\rightarrow 4x^3-3x^2+2x+1=0$

$\rightarrow 5x^3+8x^2-4x+5=0 \rightarrow -15x^3+23x^2-14x=0 \rightarrow -15x^2+23x-14=0$

$\rightarrow -5(4x^3-3x^2+2x+1)=0$

$\rightarrow 4x^3-3x^2+ 2x+1=0 \rightarrow 56x^3-42x^2+28x+14=0 \rightarrow 56x^2-57x+51=0$

$\rightarrow -15x^2+23x-14=0 \rightarrow -15x^2+23x-14=0$

$\rightarrow 56x^2-57x+51=0 \rightarrow 14(56x^2 -57x+51)=0 \rightarrow 19x^2+375x=0$

$\rightarrow -15x^2+23x-14=0 \rightarrow 51(-15x^2+23x-14)=0$

$\rightarrow 19x+375=0 \rightarrow -15x^2+23x-14=0 \rightarrow 375(-15x^2+23x-14)=0$

$\rightarrow 19x+375=0 \rightarrow 14(19x+375)=0$

$\rightarrow -5625x^2+8625x-5250=0 \rightarrow -5625x^2+8891x=0 \rightarrow -5625x+8891=0$

$\rightarrow 266x+5250=0$

$\rightarrow 19x+375=0 \rightarrow 8891(19x+375)=0 \rightarrow 168929x+3334125=0$

$\rightarrow -5625x+8891=0 \rightarrow -375(-5625x+8891)=0 \rightarrow 2109375x-3334125=0$

$\rightarrow 2278304x=0 \rightarrow x=0$ or there exists no valid solution.

Citation: Brierly JE, Ito T, Nakano H (2019) A Simple Proof of Fermat's Last Theorem. Sch J Appl Sci Res Vol: 2, Issu: 4 (26-29).