ISSN: 3066-8131
Short Communication

Science Set Journal of Physics

Fermat's Two Page Claim Verified

Joseph E Brierly

Wayne State University, Detroit, MI, USA

***Corresponding author:** Joseph E Brierly, Wayne State University, Detroit, MI, USA

Submitted: 28 Apr 2023 **Accepted:** 02 May 2023 **Published:** 06 May 2023

https://doi.org/10.63620/MKSSJP.2023.1017

Citation: *Brierly, J. E.(2023) Fermat's Two Page Claim Verified. Sci Set J of Physics 2(2) 01-02.*

Abstract

In the 1650s Fermat claimed a short two-page proof of his last theorem but could not fit it into the margin. This article vindicates Fermat's claim that has never been verified. The proof of Fermat's claim has held up for over 360 years. The solution to the problem given in this article shows that the problem can be solved in two pages and clarifies why the problem resisted solution by thousands of mathematicians both professional and amateur. The author solved the problem in 1998 but opted not to publish it until recent years. However, the author featured the proof publicly in his website challenging anyone to find a flaw in the proof. No objections ever occurred.

The proof uses only theorems and proof techniques available to Fermat. It is a devious proof that can be understood by a gifted high school student because it only uses theorems taught in high school along with an interesting algorithm devised by the author for the purpose of addressing infinity issues obstructing the finding of a simple two-page solution. The algorithm invented by the author ended the quest to solve the theorem and allows the viewer of the proof to understand why this problem has resisted so many attempts. The author believes this solution is the only one possible. The author Dr. Joseph E. L. Brierly is skeptical about the many-page solution claimed by Sir Andrew Wiles some years ago. Even professional mathematicians avoid attempting to verify pages of subtle reasoning. There is a strong likelihood of errors in proofs of that magnitude. As everyone knows a computer operating system invariably has multiple bugs due to the large number of lines of coding. In essence, there is no reason for an impractical-to-verify solution taking pages of subtle reasoning when there exists an easily reviewed two-page solution given in this research article. There exist few important theorems in mathematics and physics that require more than 5 pages of reasoning.

Introduction

Every student of mathematics learns the Pythagorean Theorem in elementary high school algebra. The Pythagorean Theorem is the case of the equation x2+y2=z2 having x,y, and z as whole integers. Fermat's Last Theorem in essence says that xn+yn=zn cannot occur for any integers x,y, and z for integer n>2. The problem is very simple to state. But like many simple looking problems finding a proof seems impossible. The author Dr. J. Brierly spent several months of trial and error before finding the right approach that worked. Anyone studying this short two-page solution will see ample reason why the proof eluded mathematicians both professional and amateur for over 350 years attempting to verify Fermat's claim to have found a proof but could not fit it into the margin.

Background Theorems and Polynomial Algorithm Required

Theorem 1: (Descartes Fundamental Theorem of Algebra) For a polynomial $p(x)=\sum a_k x^k$ for $k=0,1,3\ldots N$ with ac integers the only possible roots are of the form p/q where p and q are relatively primed with p dividing a0 and q dividing an.

Theorem 2: (Binomial Theorem) $(a+b)^n=\sum Bj\ a^{n-j}b^j$ where $Bj=n!/\ [(n-j)!j!]$ for $j=0,2,3\ldots n$ with $0!=1$ and $n!=n(n-1)(n-2)\ldots.1$

Algorithm

Let p1(x) and p2(x) be two arbitrarily selected polynomial equa-

tions satisfying
$p_1(x)= \sum a_i x^i$ and $p_2(x)=\sum b_i x^i$ for i=0,1,2….N and i=0,1,2….M, respectively.

Assume the coefficients of x are all integer and nonzero. This assumption does not have to totally restrict to only nonzero integers but for the purpose of this proof it is not necessary to prove minor variations of it because the two polynomials that we derive from the two basic theorems only have non-zero integer coefficients. We can multiply p1(x) by b0 and p2(x) by a0. Then subtract b0p1(x) from a1p2(x). At least one of the two polynomials can have x factored to form a new polynomial p3(x) reduced in degree by -1. Repeat the process again using p3(x) with either p1(x) or p2(x). The procedure will yield a new polynomial p4(x) allowing another iteration of the procedure yielding another polynomial of -1 degree less. This is a finite process that must end with a simple polynomial Kx= 0 for some nonzero K.

The reader of the proof of Fermat's Theorem should see that this algorithm is what handles the infinite possibilities inherent in the solution of the Fermat Last Problem. Realize that K is forced to be zero according to the last equation formed by the algorithm. The next part of the proof is to derive two distinct polynomials of different degrees that must exist according to the two theorems cited.

We first observe that it is only required to prove Fermat's Theorem only for integers 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 substitute b with -b. In this case replace b with -b and the Fermat equation is in the proper format. If N is odd then $-(-b)^N=b^N$. The Fermat equation becomes $c^N=a^N-(-b)^N$,equivalent to $c^N+(-b)^N=a^N$ in the positive integer form of the Fermat equation. All other such cases are resolved using the same strategy reducing the Fermat equation to the positive integer format. Without loss of generality assume that a is greater than b. For if a=b then the proof that the square root of 2 is irrational applies to yield a contradiction. So, there must exist a unique positive integer R satisfying a+R=c. We can view the Fermat problem having R as an integer variable. We now apply the Binomial Theorem to obtain.

(A) $a^N+b^N=(a+R)^N=\sum B_j a^j R^{N-j}$ for j=0.1,2…N. We can rewrite in the form

(B) $\sum B_j a^j R^{N-j}-a^N-b^n=0$

Alternately we can write (A) as a polynomial in a.

(C) $a^N+b^N=(a+R)^N=\sum B_j a^{N-j} R^j$ for j=0,1,2…N which may be expanded explicitly as an N-1 degree polynomial in powers of ai to get

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

Theorem 1 implies that a=p/q where p, q is relatively primed and q divides B_1R and p divides R^N-b^N I.e., there exists non-zero integers k_1 and k_2 satisfying $B_1R=qk_1$ and $R^N-b^N=pk_2$ We observe that k_1,k_2,B_1,R,p,q, and b are all non-zero positive integers.

`

Combining the equations we get a=p/q=(k1/k2)(RN-bN)/(B1R) which may be solved for RN-bN=aB1Rk2/k1

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

(E)

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

So, we have two distinct polynomial equations in R, (B) and (E). One is of degree N-2 and the other of degree N. We apply the algorithm to prove R=0 contradicting that it cannot be 0. Q.E.D.

Simple Example of Algorithm Applied

Suppose we have two polynomials p1(x)=x2+3x-4 and p2(x-)=2x+5. Here is how the algorithm progresses.

$5p_1(x)-(-4)p_2(x)=p_3(x)=5x^2+15x-20—8x-20=5x^2+7x=5x+7=0$. $P_3(x)=5x+7$. Now we apply the algorithm on the two polynomials $p_3(x)$ and $p_2(x)=2x+5$ to get $5p_3(x)-7p_2(x)=25x+35-14x-35=11x=0$.

References

1. Wikipedia contributors. (n.d.). Binomial theorem. Wikipedia. Retrieved July 30, 2025, from https://en.wikipedia.org/wiki/Binomial_theorem
2. Cuemath. (n.d.). Rational root theorem. Cuemath. Retrieved July 30, 2025, from https://www.cuemath.com/algebra/rational-root-theorem/
3. Wikipedia contributors. (n.d.). Gauss's lemma. Wikipedia. Retrieved July 30, 2025, from https://en.wikipedia.org/wiki/Gauss%27s_lemma
4. Wikipedia contributors. (n.d.). Fundamental theorem of algebra. Wikipedia. Retrieved July 30, 2025, from https://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra