Fermat's Last Theorem: A Proof by Contradiction

Benson Schaeffer*

Portland, OR, USA

Abstract

In this paper I offer an algebraic proof by contradiction of Fermat's Last Theorem. Using an alternative to the standard binomial expansion, $(a+b)^n = a^n + b\sum_{i=1}^{n} a^{n-i}(a+b)^{i-1}$, a and b nonzero integers, n a positive integer, I show that a simple rewrite of the equation stating the theorem,

$$A^p + (A+b)^p = (2A+b-c)^p,$$

A, b and c positive integers, entails the contradiction of two positive integers that sum to less than zero,

$$(2f+g)(f+g)(f+g+b)\sum_{i=1}^{p-2}(2f+g)^{p-2-i}(3f+2g+b)^{i-1} + (f+b)(f+g)(3f+2g+b)^{p-2} + fb(3f+2g+b)^{p-2} < 0,$$

f and g positive integers. This contradiction shows that the rewrite has no non-trivial positive integer solutions and proves Fermat's Last Theorem.

AMS 2020 subject classification:

Diophantine equations, Fermat's equation

*The corresponding author. E-mail: bookie@hevanet.com

1 Introduction

To prove Fermat's Last Theorem, it suffices to show that the equation

$$A^p + B^p = C^p \tag{1}$$

has no solution for A, B, C and p positive integers, A, B and C pairwise relatively prime, $p \geq 3$ and prime [3, pp. 1, 2].

Wiles [5], and Taylor and Wiles [4], used Galois representations, Frey's elliptic curves and the modular forms associated with them, and Wiles' demonstration of the validity of the Shimura-Taniyama Conjecture, to prove the theorem [3, pp. 366-374]. Much of the mathematics involved was developed after World War II. Excellent earlier work, beginning in the late 18th century [3, pp. 24], resulted in proofs of the theorem for many exponent powers, but not a general proof, and "led to the creation of the theory of algebraic numbers" [3, pp. 366]

The proof by contradiction I offer below employs algebra that would have been available to Fermat in the 17th century. Using an alternative to the standard binomial expansion, $(a+b)^n = a^n + b\sum_{i=1}^{n} a^{n-i}(a+b)^{i-1}$, a and b nonzero integers, n a positive integer, I show that a simple rewrite of equation (1),

$$A^p + (A+b)^p = (2A+b-c)^p,$$

A, b and c positive integers, entails the contradiction of two positive integers that sum to less than zero,

$$(2f+g)(f+g)(f+g+b)\sum_{i=1}^{p-2}(2f+g)^{p-2-i}(3f+2g+b)^{i-1}$$
$$+ (f+b)(f+g)(3f+2g+b)^{p-2} + fb(3f+2g+b)^{p-2} < 0,$$

f and g positive integers. This contradiction shows that the rewrite has no non-trivial positive integer solutions and proves Fermat's Last Theorem.

2 Proof

2.1 Lemma: Alternative Binomial Formula

An alternative to the standard binomial expansion formula [2, p. 9] for a and b nonzero integers, n a positive integer, is

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

The validity of the alternative binomial formula can be demonstrated using the formula for the sum of a finite geometric series [1, p. 10], $S_n = \dfrac{d(1-r^n)}{1-r}$, with $d = 1$ and $r = \left(\dfrac{a}{a+b}\right)$, as follows,

$$\begin{aligned}
a^n + b\sum_{i=1}^{n} a^{n-i}(a+b)^{i-1} &= a^n + b(a+b)^{n-i}\sum_{i=1}^{n}\frac{a^{n-1}(a+b)^{i-1}}{(a+b)^{n-1}} \\
&= a^n + b(a+b)^{n-i}\sum_{i=1}^{n}\left(\frac{a}{a+b}\right)^{n-i} \\
&= a^n + b(a+b)^{n-i}\left[\frac{1-\left(\frac{a}{a+b}\right)^n}{1-\left(\frac{a}{a+b}\right)}\right] \\
&= a^n + b(a+b)^{n-i}\left[\frac{[(a+b)^n - a^n](a+b)}{b(a+b)^n}\right] \\
&= a^n + (a+b)^n - a^n \\
&= (a+b)^n.
\end{aligned}$$

2.2 Contradiction

I now show that a simple rewrite of Fermat's equation (1) entails a contradiction: two positive integers sum to zero.

Without loss of generality, I rewrite equation (1) as

$$C^p - A^p - B^p = 0,$$

$$C^p - A^p - (A+b)^p = 0,$$

$$(A + (A+b))^p - A^p - B^p = (2A+b)^p - A^p - (A+b)^p > 0,$$

$$(2A+b-c)^p - A^p - (A+b)^p = 0, \tag{3}$$

$(A+b) = B$, $(2A+b-c) = C$, b and c positive integers.

In the componential rewrite, equation (3), if $c = A$, then $-A^p = 0$, and if $a = A+d$, d a positive integer, then $(A+b-d)^p - A^p - (A+b)^p = 0$. Therefore, $c = A-f$, $A = c+f$, f a positive integer, and equation (3) becomes,

$$(c+2f+b)^p - (c+f)^p - (c+f+b)^p = 0, \tag{4}$$

Application of the alternative binomial formula equation (2), to the second rewrite, equation (4), yields

$$(c+f+b)\left((c+2f+b)^{p-1} - (c+f+b)^{p-1}\right) + f\left((a+2f-b)^{p-1} - (c+f)^{p-1}\right) - c(c+f)^{p-1} = 0,$$

$$(c+f+b)f\sum_{i=1}^{p-1}(c+f+b)^{p-1-i}(c+2f+b)^{i-1} + f(f+b)\sum_{i=1}^{p-1}(c+f)^{p-1-i}(c+2f+b)^{i-1} - c(c+f)(c+f)^{p-2} = 0,$$

$$(c+f+b)^2 f\sum_{i=1}^{p-2}(c+f+b)^{p-2-i}(c+2f+b)^{i-1} + (c+f)f(f+b)\sum_{i=1}^{p-2}(c+f)^{p-2-i}(c+2f+b)^{i-1} (c+f+b)f(c+2f+b)^{p-2} + f(f+b)(c+2f+b)^{p-2} - c(c+f)(c+f)^{p-2} = 0. \tag{5}$$

In order for equation (5) to sum to zero, however, the negative term must be equal in value to the sum of all of the other terms. Thus the last line of equation (5), with its terms regrouped, must sum to less than zero,

$$2f(f+b)(c+2f+b)^{p-2} + cf\left((c+2f+b)^{p-2} - (c+f)^{p-2}\right) - c^2(c+f)^{p-2} < 0.$$

$$2f(f+b)(c+2f+b)^{p-2} + cf(f+b)\sum_{i=1}^{p-2}(c+f)^{p-2-i}(c+2f+b)^{i-1} - c^2(c+f)^{p-2} < 0,$$

$$2f(f+b)(c+2f+b)^{p-2} - c^2(c+f)^{p-2} < 0.$$

Therefore,

$$c^2 > 2f(f+b), \quad c > f, \quad c = f+g,$$

g a positive integer.

The second rewrite thus becomes,

$$(3f+2g+b)^p - (2f+g)^p - (2f+g+b)^p = 0. \tag{6}$$

Application of the alternative binomial formula, equation (2), to the third rewrite, equation (6), then yields,

$$(2f+g+b)\left((3f+b+g)^{p-1} - (2f+b+g)^{p-1}\right) + f\left((3f+b+g)^{p-1} - (2f+g)^{p-1}\right) - (2f+g)^{p-1} = 0,$$

$$(2f+g+b)(f+g)\sum_{i=1}^{p-1}(2f+g+b)^{p-1-i}(ef+2g+b)^{i-1} + f(f+g+b)\sum_{i=1}^{p-1}(2f+g)^{p-1-i}(3f+2g+b)^{i-1} - (f+g)(2f+g)^{p-1} = 0,$$

$$(2f+g+b)^2(f+g)\sum_{i=1}^{p-2}(2f+g+b)^{p-2-i}(3f+2g+b)^{i-1} + f(2f+g)(f+g+b)\sum_{i=1}^{p-2}(2f+g)^{p-2-i}(3f+2g+b) + (2f+g+b)(f+g)(3f+2g+b)^{p-2} + f(f+g+b)(3f+2g+b)^{p-2} - (f+g)(2f+g)(2f+g)^{p-2} = 0.$$

Again, it must be that,

$$(2f+g+b)(f+g)(3f+2g+b)^{p-2} + f(f+g+b)(3f+2g+b)^{p-2} - (f+g)(2f+g)(2f+g)^{p-2} < 0.$$

Application of the alternative binomial formula, however, yields a contradiction,

$$(2f+g)(f+g)\left((3f+2g+b)^{p-2}-(2f+g)^{p-2}\right)+b(f+g)(3f+2g+b)^{p-2}$$
$$+f(f+g+b)(3c+2g+b)^{p-2}<0,$$

$$(2f+g)(f+g)(f+g+b)\sum_{i=1}^{p-2}(2f+g)^{p-2-i}(3f+2g+b)^{i-1}$$
$$+(f+b)(f+g)(3f+2g+b)^{p-2}+fb(3f+2g+b)^{p-2}<0,$$

two positive integers sum to less than zero.

This contradiction invalidates the three componential rewrites, equation (3), (4) and (6), and their source, equation (1), and proves Fermat's Last Theorem: equation (1) has no nontrivial positive integer solution.

References

[1] Milton Abramowitz and Irene A Stegun (eds.), *Handbook of mathematical functions*, Dover Publications, New York, 1965.

[2] David M Burton, *Elementary number theory*, 5th ed., McGraw-Hill, New York, 2006.

[3] Paulo Ribenboim, *Fermat's last theorem for amateurs,* Springer-Verlag, New York, 1999.

[4] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain hecke algebras,* Annals of Mathematics 141 (1995), no. 3, 553–572.

[5] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem,* Annals of mathematics 141 (1995), no. 3, 443–551.