

A short algebraic proof of Fermat's Last Theorem

Morgan D. Rosenberg
 3001 Park Center Drive, #509
 Alexandria, VA 22302
 United States of America
 morgan@darkbuddhism.com

Presented herein is a proof of Fermat's Last Theorem, which is not only short (relative to Wiles' 109 page proof), but is also performed using relatively elementary mathematics. Particularly, the binomial theorem is utilized, which was known in the time of Fermat (as opposed to the elliptic curves of Wiles' proof, which belong to modern mathematics). Using the common integer expression $a^n + b^n = c^n$ for Fermat's Last Theorem, the substitutions $c = b + i$ and $b = a + j$ are made, where i and j are integers. Using a Taylor expansion (i.e., in the form of the binomial theorem), Fermat's Last Theorem reduces to $i = \sqrt[n-1]{\frac{nj^n}{b}}$ and what remains to be proven, from this equation, is that $\sqrt[n-1]{n}$ only has rational solutions for $n=1$ and $n=2$. This proof is presented herein, thus proving that $a^n + b^n = c^n$ only has integer solutions for a , b and c for integer values of the exponent $n=1$ or $n=2$.

Keywords: Fermat; Proof; Taylor Expansion; Fermat's Last Theorem; Irrational; Transcendental

1. Introduction

Fermat's Last Theorem famously states that if an integer n is greater than 2, then $a^n + b^n = c^n$ has no solutions for non-zero integers a, b and c . In 1637, Fermat wrote in the margin of his copy of Claude-Gaspar Bachet's translation of Diophantus' *Arithmetica*: "I have a truly marvelous proof of this proposition which this margin is too narrow to contain." (translated from the original Latin) [1]

After countless failed attempts to prove the theorem, Andrew Wiles finally provided a proof in 1995. [2] Wiles' 109 page paper offers a proper proof, however, it is unquestionable that this is not the proof Fermat had in mind when he made his marginal comment, as Frey curves and the like were unknown in the 1600's. Though it is unknown if Fermat actually had a proof or not, presented below is a short and "marvelous" proof using mathematics which would have been known to Fermat.

The following proof is based upon the substitutions $c = b + i$ and $b = a + j$, where i and j are integers. Using a Taylor expansion (i.e., the binomial theorem, which was known in the time of Fermat), Fermat's Last Theorem reduces to $i = \sqrt[n-1]{\frac{nj^n}{b}}$ and what remains to be proven, from this equation, is that $\sqrt[n-1]{n}$ only has rational solutions for $n=1$ and $n=2$. In other words, Fermat's Last Theorem is reduced to the theorem that $\sqrt[n-1]{n}$ only has rational solutions for $n=1$ and $n=2$, which is shown below. Binomial factorization has been attempted throughout the centuries to prove Fermat's Last Theorem, with varying degrees of success, by Euler [4], Lagrange [5], Legendre [6] and Kummer [7], amongst others. More recently, Ellman was able to derive the expression

$^n\sqrt[n]{n}$, but was unable to prove any conditions on the value of the expression [8]. What follows is a proof that Fermat's Last Theorem reduces to the problem of rational values of n in the expression $^n\sqrt[n]{n}$, and also the proof that only values of $n=1$ and $n=2$ provide such rational values for the expression, thus proving that $a^n + b^n = c^n$ has no solutions for non-zero integers a, b and c for $n > 2$.

2. Taylor expansions

Since a, b and c are each integers, we can easily substitute $c = b + i$ and $b = a + j$, where i and j are also integers. Substituting the first expression into $a^n + b^n = c^n$ yields

$$a^n + b^n = (b + i)^n \quad (2)$$

$$a^n = (b + i)^n - b^n \quad (3)$$

which can now be expanded, using a Taylor expansion (i.e., the binomial theorem), as

$$a^n = nb^{n-1}i + \frac{n(n-1)}{2!}b^{n-2}i^2 + \dots + i^n. \quad (4)$$

We have defined $b = a + j$, thus $a = b - j$ and $a^n = (b - j)^n$. Expanding this expression, once again using the Taylor expansion, yields

$$a^n = b^n - nb^{n-1}j + \frac{n(n-1)}{2!}b^{n-2}j^2 - \dots \pm j^n. \quad (5)$$

In order to equate the coefficients of the powers of b for the two expressions for a^n , we rewrite equation (4) as:

$$a^n = ni \left[b^{n-1} + \frac{(n-1)}{2!}b^{n-2}i + \dots + \frac{1}{n}i^{n-1} \right] \quad (6)$$

and, similarly, equation (5) becomes

$$a^n = b \left[b^{n-1} - nb^{n-2}j + \frac{n(n-1)}{2!} b^{n-3}j^2 - \dots \pm \frac{1}{b} j^n \right]. \quad (7)$$

Thus, by matching exponents, we now have the following condition:

$$\frac{1}{n} i^{n-1} = \frac{1}{b} j^n. \quad (8)$$

3. Restrictions on n

Equation (8) can be rewritten as $i = \sqrt[n-1]{\frac{nj^n}{b}}$, or

$$i = j \cdot \sqrt[n-1]{\frac{j}{b}} \cdot \sqrt[n-1]{n}. \quad (9)$$

Thus far, no restrictions have been placed on i , j , n or b , other than that they must be

integers. The expression $\sqrt[n-1]{\frac{j}{b}}$ can have integer and/or rational values for an infinite

number of selections of j , b and n . i , though, must be an integer, thus the expression $\sqrt[n-1]{n}$ must at least be rational, if not an integer, to be able to produce an integer value for i .

However, as will be proven below $\sqrt[n-1]{n}$ only has rational values if $n=1$ or $n=2$. As will

be further shown below, the value of $\sqrt[n-1]{n}$ must have integer solutions to be rational, and

values of $n=1$ or $n=2$ also produce the only integer values for the expression $\sqrt[n-1]{n}$.

4. $\sqrt[n-1]{n}$ only has integer values if $n=1$ or $n=2$

The above theorem stating that $\sqrt[n-1]{n}$ only has integer values if $n=1$ or $n=2$ is proved easily by considering the transcendental equation $x^y = y^x$. This equation only

has integer solutions if $x=y$ or for values of $(x,y)=\{(2,4), (4,2), (-2,-4),(-4,-2)\}$. The proof of this is as follows:

Assuming that x and y are both positive, then switching the order of x and y allows us to also assume that $y \geq x$. Dividing both sides of $x^y = y^x$ by x^x yields

$$x^{y-x} = \left(\frac{y}{x}\right)^x. \quad (10)$$

For integer x and y , the left-hand side of equation (10) must be an integer. If the left-hand side is an integer, then the right-hand side must also be an integer. However, raising a rational non-integer to an integer power yields a non-integer, thus $k = \frac{y}{x}$ must be an integer. Equation (10) can be rewritten as:

$$x^{kx-x} = k^x \quad (11)$$

which, when the x -th root is taken on both sides of the equation, yields

$$x^{k-1} = k. \quad (12)$$

For $x \geq 2$, equation (12) yields four solutions: a) For $k=1$, $x=y$ is a solution; b) for $k=2$, $x=2$ is a solution; c) $k=3$ implies that $x^{k-1} > k$; and d) by induction for k , $k \geq 3$ implies that $x^{k-1} = x \cdot x^{k-2} > x(k-1) \geq 2k-2 > k$. Thus, $x^y = y^x$ only has integer solutions if $x=y$ or for values of $(x,y)=\{(2,4), (4,2), (-2,-4),(-4,-2)\}$.

Returning to the transcendental equation $x^y = y^x$, where x and y are integers, x can be written as a multiple of prime factors (or as a single prime): $x = x_1 \cdot x_2 \cdot x_3 \cdot \dots \cdot x_m$. The same is, of course, true for y . According to the fundamental theorem of arithmetic, this factorization is unique and the expression x^y has the same factorization (simply raised to the y power). Similarly, y^x has the same factors as y , but raised to the x power.

If $x^y = y^x$, then the left-hand side of the equation must contain the same factors as the right-hand side of the equation, with both sides being raised to the same power. This, however, is only true if $x=y$ (as we've already proven) or if $y = x^m$ with $mx=y$. Simple substitution and reduction of these last two expressions yields:

$$x^{m-1} = m, \quad (13)$$

or

$$x = {}^{m-1}\sqrt{m}. \quad (14)$$

Equation (14), however, is the same expression from equation (9), and we have already proven that for integer x (and y), either $x=y$ (which produces a value of $m=1$) or $x=2$, which produces a value of $m=2$. There are no other values for m .

The above is important, since ${}^{n-1}\sqrt{\frac{j^n}{b}} \cdot {}^{n-1}\sqrt{n}$ must form an integer value (namely, the integer i). We have now proven that ${}^{n-1}\sqrt{n}$ only has integer values for $n=1$ and $n=2$. What we still seek to prove is that ${}^{n-1}\sqrt{n}$ also only has rational values for $n=1$ and $n=2$ (which will be proven in the following section). If ${}^{n-1}\sqrt{n}$ has a rational value, then we also require ${}^{n-1}\sqrt{\frac{j^n}{b}}$ to have a rational value in order for the two factors to form an integer.

However, from the original equation $i = {}^{n-1}\sqrt{\frac{nj^n}{b}}$, we see that ${}^{n-1}\sqrt{\frac{j^n}{b}} = \frac{i}{{}^{n-1}\sqrt{n}}$. i is, of course, defined as an integer, and the only possible integer values of n (and n is defined as an integer in the original problem) are $n=1$ and $n=2$. Thus, ${}^{n-1}\sqrt{\frac{j^n}{b}}$ can only have the

value of either i or $i/2$, both of which are rational. Thus, with $\sqrt[n]{\frac{j^n}{b}}$ proven to be rational, we must only prove the rationality of $\sqrt[n]{n}$.

5. $\sqrt[n]{n}$ only has rational values if $n=1$ or $n=2$

Now, we examine which values of x and y are rational in the transcendental equation $x^y = y^x$. We have already seen that the only integer solutions are of the form

$(x,y)=\{(2,4), (4,2), (-2,-4),(-4,-2)\}$. For rational x and y , then $r = \frac{y}{x}$ must also be rational.

If we set $r = 1 + \frac{1}{d}$, then d must also be rational. If d is rational, then $x = \left(1 + \frac{1}{d}\right)^d$ is

rational *if and only if* d is an integer.

Letting $d = \frac{f}{g}$, where f and g are relatively prime (i.e., d is a fraction in its lowest terms), then $\left(1 + \frac{1}{d}\right)^d = \left[\frac{(f+g)}{f}\right]^{f/g}$, which is rational only if $g = 1$. If $g > 1$, then,

since f and g are relatively prime, $(f+g)$ and f are also relatively prime. Therefore, for

$\left[\frac{(f+g)}{f}\right]^{f/g}$ to be rational, both $(f+g)$ and f must be perfect g -th powers of integers.

However, this is impossible. For example, if $g = 2$, then $(f+2)$ and f cannot both be perfect squares, because the difference between two positive perfect squares is at least 3.

More generally, if u , v and w are positive integers, with $w > 1$, then using the binomial theorem, $(u+v)^w - u^w = wu^{w-1}v + \dots + v^w > w$. Thus, two distinct perfect g -th

powers cannot differ by g . Therefore, $\left(1 + \frac{1}{d}\right)^d = \left[\frac{(f+g)}{f}\right]^{f/g}$ cannot be rational if $g >$

1.

Thus, $\left(1 + \frac{1}{d}\right)^d$ is rational *if and only if* d is a positive integer. Therefore, all

rational solutions are of the form $x = \left(1 + \frac{1}{d}\right)^d$ and $y = \left(1 + \frac{1}{d}\right)^{d+1}$, where $d = 1, 2, \dots$.

Rational solutions are only within the bounds of $2 \leq x < e < y \leq 4$.

We have already seen that the only integer values for x and y occur either when $x=y$ or for $x=2$ and $y=4$, and now we have shown that these are also the only rational integer values. Since the only restriction on i is that it be an integer, $\sqrt[n]{n}$ must have a rational value (since $\sqrt[n]{\frac{j}{b}}$, without restrictions on b, j or n , would produce only an irrational value if multiplied with an irrational number), and the only rational values allowed are $n=1$ or $n=2$.

In the above, what we are obviously interested in is the expression $\sqrt[n]{n}$ being rational. However, in general, $\sqrt[p]{N}$ is irrational unless N is the p -th power of an integer z [3]. Thus, the only rational values for $\sqrt[n]{n}$ must also be integer values. The only integer values for $\sqrt[n]{n}$ are $n=1$ and $n=2$, thus the only rational values for $\sqrt[n]{n}$ are also only found at $n=1$ and $n=2$.

6. Conclusion

Section 4 above proves that $x = \sqrt[m]{m}$ only produces an integer value for x if $m=1$ or $m=2$. Section 5 goes on to show that these two solutions also provide the only rational values for x . Equation (9) provided that $i = j \cdot \sqrt[n]{\frac{j}{b}} \cdot \sqrt[n]{n}$, with no restrictions being made on i, j, n or b , other than that they must be integers. The expression $\sqrt[n]{n}$ must be a rational number (which also must be an integer, as described above in Section 5) in order to produce an integer value for i . However, we have now proven that $\sqrt[n]{n}$ only has rational integer values if $n=1$ or $n=2$. Thus, the equation $a^n + b^n = c^n$ only has integer solutions for a, b and c when the integer exponent n has a value of $n=1$ or $n=2$.

Q.E.D.

References

- [1] S. Singh, *Fermat's Enigma* (Bantam Books, New York, 1998).
- [2] A. Wiles, "Modular Elliptic Curves and Fermat's Last Theorem", *Annals of Mathematics*, **141** (3): 443-551 (1995).
- [3] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 4th Ed. (Oxford University Press, Oxford, 1975).
- [4] L. Euler, "Theorematum quorundam arithmeticonum demonstrationes", *Comm. Acad. Sci. Petrop.*, **10**, 1738 (1747), 125-146; reprinted in *Opera Omnia*, Vol. II, *Comm. Arithmeticae*, Vol. I, 38-58.
- [5] J.L. Lagrange, "Resolution des equations numeriques", *Mem. Acad. Roy. Sci. Belles-Lettres Berline* **23** (1769); reprinted in *Oeuvres*, Vol. II, 527-532 and 539-578, Gauthier-Villars, Paris (1868).
- [6] A.M. Legendre, *Theorie des Nombres* (3rd Ed.), Vol. I, 226-229, Firmin Didot Freres, Paris (1830); reprinted by A. Blanchard, Paris (1955).

[7] E.E. Kummer, “De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda”, *J. Reine Angew. Math.*, **17** (1837), 203-209; reprinted in *Collected Papers*, Vol. I, 135-141, Springer-Verlag, New York (1975).

[8] R. Ellman, “A Concise and Direct Proof of ‘Fermat’s Last Theorem’”,
arXiv:math/9810027v5 (1999).