A Short Proof of Fermat's Last Theorem

Morgan D. Rosenberg

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 $c = a + i$ and $c = b + j$ 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 the theorem 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; Binomial Theorem; 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 $c = a + i$ and $c = b + j$, 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 the theorem that $\sqrt[n-1]{n}$ only has rational solutions for *n*=1 and *n*=2. 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 $\sqrt[n-1]{n}$, 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 $\sqrt[n-1]{n}$, 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. Binomial expansions

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

$$a^n + b^n = c^n \tag{1}$$

yields

$$b^n = c^n - (c - i)^n . \tag{2}$$

Expansion of equation (2) by the binomial theorem gives us:

$$b^n = c^n - \left(c^n - nic^{n-1} + \frac{n(n-1)}{2!} i^2 c^{n-2} - \frac{n(n-1)(n-2)}{3!} i^3 c^{n-3} + \ldots \pm i^n \right), \tag{3}$$

which reduces to

$$b^n = nic^{n-1} - \frac{n(n-1)}{2!} i^2 c^{n-2} + \frac{n(n-1)(n-2)}{3!} i^3 c^{n-3} - \ldots \pm i^n , \tag{4}$$

or

$$b^n = ni\left(c^{n-1} - \frac{(n-1)}{2!} ic^{n-2} + \frac{(n-1)(n-2)}{3!} i^2 c^{n-3} - \ldots \pm \frac{1}{n} i^{n-1} \right). \tag{5}$$

We now introduce a constant α, such that $b = \frac{ni}{\alpha}$. Since $\alpha = \frac{ni}{b}$, there is no restriction on α other than the fact that α must be rational, since *n*, *i* and *b* are all integers. This allows us to write equation (5) as:

$$b^n = \frac{ni}{\alpha} \cdot \alpha\left(c^{n-1} - \frac{(n-1)}{2!} ic^{n-2} + \frac{(n-1)(n-2)}{3!} i^2 c^{n-3} - \ldots \pm \frac{1}{n} i^{n-1} \right), \tag{6}$$

where $b = \frac{ni}{\alpha}$ and

$$b^{n-1} = \alpha\left(c^{n-1} - \frac{(n-1)}{2!} ic^{n-2} + \frac{(n-1)(n-2)}{3!} i^2 c^{n-3} \ldots \pm \frac{1}{n} i^{n-1} \right). \tag{7}$$

We can also express b^{n-1} as $\frac{b^n}{b}$, or

$$b^{n-1} = \frac{\alpha}{ni} b^n \tag{8}$$

$$b^{n-1} = \alpha\left[\left(\frac{b^n}{ni} \right)^{1/(n-1)} \right]^{n-1} \tag{9}$$

$$b^{n-1} = \alpha\left[c - \left(c - \left(\frac{b^n}{ni} \right)^{1/(n-1)} \right) \right]^{n-1}, \tag{10}$$

or

$$b^{n-1} = \alpha(c - \beta)^{n-1}, \tag{11}$$

where $\beta = \left[c - \left(\frac{b^n}{ni} \right)^{1/(n-1)} \right]$.

Applying the binomial theorem to equation (11) yields:

$$b^{n-1} = \alpha\left(c^{n-1} - (n-1)\beta c^{n-2} + \frac{(n-1)(n-2)}{2!} \beta^2 c^{n-3} - \ldots \pm \beta^{n-1} \right). \tag{12}$$

Matching the (n-1), (n-2), … zero-th order terms in c in equations (7) and (12) results in the progression $\beta = \frac{i}{2!}$, $\frac{1}{2!}\beta^2 = \frac{i^2}{3!}$, …, to the zero-th order term:

$$\beta^{n-1} = \frac{(n-1)!}{n!} i^{n-1} = \frac{1}{n} i^{n-1}, \tag{13}$$

which can be rewritten as:

$$i = \beta \cdot \sqrt[n-1]{n}\,. \tag{14}$$

In the long history of attempts to prove Fermat's Last Theorem, the expression $\sqrt[n-1]{n}$ has been derived many times previously in binomial theorem-based attempts (such as in Ellman's attempt at a proof [8]), but the necessary subsequent proof that $\sqrt[n-1]{n}$ only has rational values if and only if n=1 or n=2, to the best of the author's knowledge, has not previously been found. This proof is presented in the following sections.

3. Restatement of Fermat's Last Theorem

Equation (14) above gives us the condition $i = \beta^{n-1}\sqrt{n}$. i, though, must be an integer, and though no restrictions have been placed on β, 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. Thus, Fermat's Last Theorem reduces to the following: The expression $\sqrt[n-1]{n}$ has rational solutions *only* for n=1 or n=2.

In the following sections, it will be shown that $\sqrt[n-1]{n}$ only has rational values if and only 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

$$x^{y-x} = \left(\frac{y}{x}\right)^x . \tag{15}$$

For integer x and y, the left-hand side of equation (15) 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 (15) can be rewritten as:

$$x^{kx-x} = k^x \tag{16}$$

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

$$x^{k-1} = k . \tag{17}$$

For $x \geq 2$, equation (17) 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): $x = x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_m$. 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:

$$x^{m-1} = m, \tag{18}$$

or

$$x = \sqrt[m-1]{m}. \tag{19}$$

Equation (19), however, is the same expression from equation (14), 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 $\beta^{\sqrt[n-1]{n}}$ must form an integer value (namely, the integer i). We have now proven that $\sqrt[n-1]{n}$ only has integer values for $n=1$ and $n=2$. What we still seek to prove is that $\sqrt[n-1]{n}$ also only has rational values for $n=1$ and $n=2$ (which will be proven in the following section).

5. $\sqrt[n-1]{n}$ 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, $(u+v)^w - u^w = wu^{w-1}v + ... + v^w > w$. 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 $d = 1, 2, ...$. 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, $\sqrt[n-1]{n}$ must have a rational value, and the only rational values allowed are $n=1$ or $n=2$.

In the above, what we are obviously interested in is the expression $\sqrt[n-1]{n}$ 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 $\sqrt[n-1]{n}$ must also be integer values. The only integer values for $\sqrt[n-1]{n}$ are n=1 and n=2, thus the only rational values for $\sqrt[n-1]{n}$ are also only found at n=1 and n=2.

6. Conclusion

Section 4 above proves that $x = \sqrt[m-1]{m}$ 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 (14) provided that $i = \beta^{\sqrt[n-1]{n}}$, with no restrictions being made on i, n or β, other than that i and n must be integers. The expression $\sqrt[n-1]{n}$ 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 $\sqrt[n-1]{n}$ 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 arithmeticorum 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).