A Concise and Direct Proof of "Fermat's Last Theorem"

by

Roger Ellman

Abstract

Fermat's Last Theorem states:

There can be no non-zero integer solution for $n>2$ to the equation $a^n + b^n = c^n$. A proof is presented

Roger Ellman, The-Origin Foundation, Inc.
1401 Fountaingrove Pkwy.,M-233, Santa Rosa, CA 95403, USA
RogerEllman@The-Origin.org
http://www.The-Origin.org

A Concise and Direct Proof of "Fermat's Last Theorem"

by

Roger Ellman

Introduction

"Fermat's Last Theorem" states: There can be no non-zero integer solution for $n>2$ to the equation

(1) $a^n + b^n = c^n$

Step 1

Restate the problem as follows:

For x, i, n and $f(x,i)$ all non-zero integers and $i<x$ there is no solution for $n>2$ to

(2) $x^n = [x-i]^n + [f(x,i)]^n$

That is, make the following substitutions in equation *(1)*:

$x^n = c^n$ $\qquad [x-i]^n = a^n$ $\qquad [f(x,i)]^n = b^n$

Clearly there is no difficulty with the x^n term nor the $[x-i]^n$ term. Both are integers and perfect n^{th} powers of integers.

The issue now is:

Can $f(x,i)$ be a non-zero integer for $n>2$ and equation *(2)* still valid ?

Step 2

The first constraint on b^n is that it must be the difference of c^n and a^n.

(3) $b^n = [f(x,i)]^n$

$= x^n - [x-i]^n$ [from equation *(2)*]

$= x^n - [x^n - n \cdot x^{n-1} \cdot i + \ldots \pm i^n]$ [binomial expansion]

$= n \cdot x^{n-1} \cdot i - \ldots \pm i^n$

Step 3

The second constraint on b^n is that it must be a perfect n^{th} power.

(4) $b^n = [x-j]^n = [x-j]_1 \cdot [x-j]_2 \cdot [x-j]_3 \cdot \cdots \cdot [x-j]_n$

where: $b = x-j$ (just as $a = x-i$)
j is a non-zero integer, $j<x$

Step 4

These two constraints are simultaneous. They are for the same b^n. Therefore, the two expressions must be identical; they must always simultaneously deliver the same value of b^n.

The order of equation *(3)* is one less than the order of equation *(4)*. To compare the two expressions as an identity their order must be the same. That is accomplished by removing one factor of b from each of equations *(3)* and *(4)*, as follows.

(5) $b^n = n\cdot x^{n-1}\cdot i - \dots \pm i^n$ [equation *(3)*]

$$= \underbrace{\frac{n\cdot i}{m}}_{b} \cdot \underbrace{m\cdot\left[x^{n-1} - \dots \pm \frac{i^{n-1}}{n}\right]}_{b^{n-1}}$$

The parameter m is necessary because the quantity, $n\cdot i$, which factored out normalizes the expressing, is not necessarily equal to b.

(6) $b^n = \underbrace{[x-j]_1}_{b} \cdot \underbrace{[x-j]_2\cdots[x-j]_n}_{b^{n-1}}$ [equation *(4)*]

$$= \underbrace{[x-j]_1}_{b} \cdot \underbrace{m\cdot\left[[x-k]_2\cdot[x-k]_3\cdot\ \cdots\ \cdot[x-k]_n\right]}_{b^{n-1}}$$

The m here is for identity to be possible – for the coefficient of the x^{n-1} term in the two expressions to be able to be equal, when $m\neq1$.

Step 5

Now, equation *(5)* and equation *(6)* must yield the same value for b^n for all values of x. To establish that condition for convenience we will require, rather than the entire expressions, that $[b^{n-1}/_m]$ in each expression yield the same value for all values of x.

The two expressions are (using the binomial theorem expansion formula) as follows.

In equation (5)

(7)
$$x^{n-1} - \frac{[n-1]}{2\cdot1}\cdot x^{n-2}i + \frac{[n-1][n-2]}{3\cdot2\cdot1}\cdot x^{n-3}i^2 - \dots \pm \frac{i^{n-1}}{n}$$

In equation (6)

(8)
$$x^{n-1} - \frac{[n-1]}{+1}\cdot x^{n-2}k^1 + \frac{[n-1][n-2]}{2\cdot1}\cdot x^{n-3}k^2 - \dots \pm k^{n-1}$$

Equating the pair of terms of zero order in equations (7) and (8):

(9)
$$\pm\frac{i^{n-1}}{n} = \pm k^{n-1}$$

$k = {}^{i}/_{[n-1]^{th}}$ root of n

The $[n-1]^{th}$ root of n is irrational for $n>2$. [See Step 7, page 4]. Therefore, for $n>2$, k is irrational and b is irrational and cannot be an integer, which proves the theorem.

Step 6

However, k in expression (8) is a function of $x.$ The only values of k that are able to make the expression for b^{n-1} in the horizontal bracket to the right in the second line of expression (6) actually be equal to b^{n-1} are as follows:

(10) $$k = \left[x - \left[\frac{b^n}{n\cdot i}\right]^{1/[n-1]}\right]$$ [where *b* is also a function of *x*]

which can readily be verified by substitution, that is

$$m\cdot[x-k]^{n-1} = \frac{n\cdot i}{b}\cdot\left[x - \overbrace{\left[x - \left[\frac{b^n}{n\cdot i}\right]^{1/[n-1]}\right]}^{k}\right]^{n-1}$$

$$= \frac{n\cdot i}{b}\cdot\left[\left[\frac{b^n}{n\cdot i}\right]^{1/[n-1]}\right]^{n-1} = \frac{n\cdot i}{b}\cdot\frac{b^n}{n\cdot i} = b^{n-1}$$

The problem with k being a function of x is that the apparent terms of given orders of x and their coefficients are not necessarily as they appear in equation *(8)* when equation *(9)* is substituted for k in equation *(8)*. However, if the term coefficients experience no net change from the substitution, then the comparison of any pair of coefficients is valid even though $k = f(x)$. That is exactly the situation in the present case (and may relate to why the theorem withstood proof for three centuries) as follows.

The pattern can be developed with two examples.

Example #1: n = 2

Equation Nr.	Content
(5)	$b^n = 2\cdot x\cdot i - i^2$ $= \frac{2\cdot i}{m}\cdot m\cdot\left[x - \frac{i}{2}\right]$
(6)	$b^n = [x-j]\cdot[x-j]$ $= [x-j]\cdot m\cdot[x-k]$
(7)	$[b^{n-1}/_m] = x - {}^{i}/_{2}$
(8)	$[b^{n-1}/_m] = x - k$
(10)	$k = \left[x-\left[\frac{b^2}{2\cdot i}\right]^{1/1}\right]$ $= \left[x-\left[\frac{2\cdot x\cdot i-i^2}{2\cdot i}\right]^{1/1}\right]$ $= {}^{i}/_{2}$
Substituting *(10)* for the *k* in *(8)* gives *(8)* ≡ *(7)*	$\left[b^{n-1}/_m\right] = x - {}^{i}/_{2}$

Example #2: n = 3

Equation Nr.	Content
(5)	$b^n = 3\cdot x^2\cdot i - 3\cdot x\cdot i^2 + i^3$ $= \frac{3\cdot i}{m}\cdot m\cdot\left[x^2 - x\cdot i + \frac{i^2}{3}\right]$

(6) $$b^n = [x-j]\cdot[x-j]\cdot[x-j]$$

$$= [x-j] \cdot m\cdot[x-k]\cdot[x-k]$$

(7) $$[b^{n-1}/_m] = x^2 - x\cdot i + i^2/_3$$

(8) $$[b^{n-1}/_m] = x^2 - 2\cdot k\cdot x + k^2$$

(10) $$k = \left[x-\left[\frac{b^3}{3\cdot i}\right]^{1/2}\right]$$

$$= \left[x-\left[\frac{3\cdot x^2\cdot i-3\cdot x\cdot i^2+i^3}{3\cdot i}\right]^{1/2}\right]$$

$$= x-[x^2-x\cdot i+i^2/_3]^{1/2}$$

Substituting *(10)*
For the *k* in *(8)*
gives *(8)* ≡ *(7)*

$$\left[b^{n-1}/_m\right] = x^2 - x\cdot i + i^2/_3$$

This pattern persists for all positive integer values of n. Therefore, the term coefficients experience no net change from the substitution and the comparison of any pair of coefficients is valid even though $k = f(x)$. Therefore, equation *(9)* is valid and equation *(9)* shows that k, and therefore b, are irrational for $n>2$, which proves the theorem.

Step 7

Proof that the $[n-1]^{th}$ root of n is irrational.

Trial calculations make clear that the numerical value of the $[n-1]^{th}$ root of n lies between 1 and 2 as follows.

(11)

n	[n-1]th root of n
2	2
3	1.732…
4	1.607…
…	…
10	1.291…
10^9	1.000,000,020,7…

Keeping in mind the significance of the positional notation used in representing numbers, the notation of a number such as 1.3, for example, means $1.3 = 1 \times 10^0 + 3 \times 10^{-1}$, the number at issue, the $[n-1]^{th}$ root of n being between 1 and 2 can then be represented as

(12) $$\{ [n-1]^{th} \text{ root of } n \} = [1 \times 10^0] + [a \times 10^{-1}] + [b \times 10^{-2}] + [c \times 10^{-3}] + \ldots$$
where the letters a, b, etc., represent a selection of one of the decimal digits 0 to 9.

That number, the $[n-1]^{th}$ root of n, when multiplied by itself $[n-1]$ times must yield the original number, n, an integer. That is

(13) $$n = \left[[1 \times 10^0] + [a \times 10^{-1}] + [b \times 10^{-2}] + [c \times 10^{-3}] + \ldots\right]^{[n-1]}$$

But, examining what happens when a rational such number is raised to a power greater than one, it becomes clear that the result cannot be an integer.

A rational number is one that can be expressed as the ratio of two integers. Because ∞ is not a specific number but, rather the concept "large without limit", the two integers of a rational number cannot be infinite. Therefore, both of the integers whose ratio makes a rational number have a finite number of non-zero digits and the decimal number representation of the ratio has a finite number of non-zero digits.

That is, a rational number has a finite number of non-zero digits to the right of its decimal point as compared to an irrational number, which has an infinite number of non-zero digits to the right of the decimal point. The only exception to this distinction is the repeating decimal, which always is a rational number, but its infinite number of non-zero digits to the right of the decimal point is characterized by their repetition.

Any rational number between 1 and 2 can then be represented as in equation *(18)*.

$$(18) \quad \begin{array}{rr} n = & 1.ab \dots p0 \\ & +0.00 \dots 0u \\ \cline{2-2} = & 1.ab \dots pu \end{array}$$

Where $a, b, \dots p, u$ are decimal digits able to have value 0 through 9 except that u cannot be zero. The digit p is the penultimate, the next to right-most digit and the digit u is the ultimate, the right-most non-zero digit.

In the terms of equation *(12)*

$$(19) \quad \begin{array}{l} p \text{ is } [p \times 10^{-P}] \\ u \text{ is } [u \times 10^{-U}] \end{array}$$

that is, p is in the P^{th} column to the right of the decimal point and u is in the U^{th} such column.

The number n of equation *(18)* raised to a power can be expressed as

$$(20) \quad \begin{aligned} n^{exp} &= \Big[[1.ab \dots p0] + [0.00 \dots 0u] \Big]^{exp} \\ &= [1.ab \dots p0]^{exp} + exp \cdot [1.ab \dots p0]^{exp-1} \cdot [0.00 \dots 0u] + \dots + [0.00 \dots 0u]^{exp} \end{aligned}$$

The last term of equation *(20)* is the digit u raised to the exp power and positionally notated in the column corresponding to the value of its original column, 10^{-U}, raised to the exp power, that is the $10^{-U \cdot exp}$ column.

The digit u, by definition the right-most significant digit of the decimal number, cannot be zero. That digit raised to any power produces a number the right-most digit of which is never zero, which can readily be verified by examining the decimal digits 1 through 9 raised from power 1 to successively higher powers.

The net effect of all of this is that any non-integer rational number raised to any integer power greater than 1 can never yield an integer result. There will always be at least the u^{exp} "out there" in the $10^{-U \cdot exp}$ column providing a decimal fraction part of the result.

But, that means that for n, an integer $n>2$, the $[n-1]th$ root of n can never be an integer.

Then, how can there be any non-integer roots of integers at all? The answer is irrational numbers, of course. Consider how such numbers are able to operate. An example of irrational roots producing integer powers is the square root of 3. That root is $1.732,050,807,77 \dots$, an irrational number which squared equals the integer 3. Picture the multiplication process as in equation (21), below

$$(21) \quad \begin{array}{ll} & \ 1.732,050,807,77 \dots \\ & \times\ 1.732,050,807,77 \dots \\ \hline \text{Multiply by 1.} & 1.732,050,807,77 \dots \\ \text{Multiply by 0.7} & 1.212,435,565,39 \dots \\ \text{Multiply by 0.03} & 1.051,961,524,22 \dots \\ \quad \dots & \quad \dots \\ \quad \dots & \quad \dots \\ \hline \text{Sum of the above} & 3 \quad \text{exactly} \end{array}$$

Speaking non-mathematically the result coming out to exactly 3 seems like a miracle – it certainly would seem highly improbable. Yet, that is what the infinite string of non-repeating digits to the right of the decimal point in all irrational numbers is capable of.

Irrational numbers have a special power. There is no end to their non-zero digits to the right of the decimal point – they go on and on. They have no "right-most" digit.

But, what about repeating decimals? They appear to have an infinite string of digits to the right of the decimal point.

Yet they are rational. Repeating decimals do not really have an infinite string of digits to the right of the decimal point. That appearance is pseudo. It is a consequence of the number system in use. We use the decimal system, most likely because evolution gave us 5 fingers on each of 2 hands.

Consider, for example, the repeating decimal $0.333 \ldots$ $^{1}/_{3}$. That same numerical value, one item out of three, expressed in the number system using base 3 and the digits $0, 1, 2$ is written $^{1}/_{10} = 0.1$ not a repeating decimal nor a repeating [number system base three]. Any repeating decimal expressed in a number system that uses as its base the number cycle that is repeated appears as an ordinary, not repeating, ”decimal” (number system base) in that number system.

No number system is sacred or prime; only the numerical values involved are so. True irrational numbers have an infinite string of digits to the right of the decimal point regardless of the number system in which they are expressed. The numerical value, itself, is that way. And, that is so because a true irrational number’s digits have no cycle of repetition or, rather, that cycle extends to infinity and so cannot be repeated nor be a number system base.