

**A CONCISE AND DIRECT PROOF OF
"FERMAT'S LAST THEOREM"**

by Roger Ellman

FERMAT'S LAST THEOREM states:

There can be no non-zero integer solution for $n > 2$ to the equation

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

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 the equation

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

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

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

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 1st constraint on b^n : it must be the difference of c^n and a^n .

$$(3) \quad \begin{aligned} b^n &= [f(x, i)]^n \\ &= x^n - [x-i]^n && \text{[Solving equation (2)]} \\ &= x^n - [x^n - n \cdot x^{n-1} \cdot i + \dots \pm i^n] && \text{[Binomial expansion]} \\ &= n \cdot x^{n-1} \cdot i - \dots \pm i^n \end{aligned}$$

Step 3

The 2nd constraint on b^n : it must be a perfect n^{th} power.

$$(4) \quad \begin{aligned} b^n &= [x-j]^n = [x-j]_1 \cdot [x-j]_2 \cdot [x-j]_3 \cdot \dots \cdot [x-j]_n \\ \text{where: } &b = x-j \quad (\text{just as } a = x-i) \\ &j \text{ is a non-zero integer, } j < x \end{aligned}$$

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 Step 2, equation (3) is one less than the order of Step 3, 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.

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

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

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

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

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

(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 $m \neq 1$.)

Step 5

Now, expression (5) and expression (6) must yield the same value for b^n for all values of x . To establish that condition we will require, for convenience 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): in expression (5)

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

and in expression (6)

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

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

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

$$k = \frac{i}{\sqrt[n-1]{n}}$$

The $[n-1]^{th}$ root of n is irrational for $n > 2$. [See Step 6, page 5]. Therefore, for $n > 2$, k is irrational and b is irrational and cannot be an integer, which proves the theorem.

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:

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

which can readily be verified by substitution, that is

$$(11) \quad m \cdot [x-k]^{n-1} = \frac{n \cdot i}{b} \cdot \left[x - \left[x - \left[\frac{b^n}{n \cdot i} \right]^{1/[n-1]} \right] \right]^{n-1}$$

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

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 expression (8) when expression (9) is substituted for k in expression (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.

To show this in an overall general form would be too algebraically complex to contemplate. The pattern can be developed with two examples.

<u>Expression Nr</u> <u>As on Page 2</u>	<u>Example #1: n = 2</u> <u>Content</u>
(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) Page 3	$k = \left[x - \left[\frac{b^2}{2 \cdot i} \right]^{1/1} \right]$ $= \left[x - \left[\frac{2 \cdot x \cdot i - i^2}{2 \cdot i} \right]^{1/1} \right]$ $= i/2$
Substituting (10) For the k in (8) gives (8) \equiv (7)	$[b^{n-1}/m] = x - i/2$

Example #2: n = 3

Expression Nr
As on Page 2

Content

$$(5) \quad b^n = 3 \cdot x^2 \cdot i - 3 \cdot x \cdot i^2 + i^3$$

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

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

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

$$(7) \quad [b^{n-1}/m] = x^2 - x \cdot i + i^2/3$$

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

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

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

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

Substituting (10)
For the k in (8)
gives (8) \equiv (7)

$$[b^{n-1}/m] = x^2 - x \cdot i + i^2/3$$

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, expression (9) is valid and expression (9) shows that k , and therefore b , are irrational for $n > 2$, which proves the theorem.

[Step 6 begins on the next page].

Step 6

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.

(14)

<u>n</u>	<u>$\sqrt[n-1]{n}$</u>
2	2
3	1.732,050,807,7 ...
4	1.607,401,052,1 ...
...	...
10	1.291,549,665,0 ...
...	...
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

(15) $1.3 = 1 \times 10^0 + 3 \times 10^{-1}$

The number at issue, the $[n-1]^{th}$ root of n , being between 1 and 2, can then be represented as

(16) $ab \dots = 1 \times 10^0 + a \times 10^{-1} + b \times 10^{-2} + \dots$

where a, b, \dots are decimal digits 0 through 9.

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

(17) $n = [1 \times 10^0 + a \times 10^{-1} + b \times 10^{-2} + \dots]^{[n-1]}$

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 its 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).

$$\begin{aligned}
 (18) \quad n &= 1.ab \cdots p0 \\
 &\quad + 0.00 \cdots 0u \\
 &= \frac{ + 0.00 \cdots 0u}{} \\
 &= 1.ab \cdots pu
 \end{aligned}$$

where $a, b, \cdots p, u$ are decimal digits able to have values 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 (10)

$$(19) \quad p \text{ is } p \times 10^{-P} \qquad u \text{ is } u \times 10^{-U}$$

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.

That number, equation (11), raised to a power can be expressed as

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

The last term of equation (14) 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 as 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 be verified using the following table.

(21)	x	1	2	3	4	5	6	7	8	9
	1	1	2	3	4	5	6	7	8	9
	2	2	4	6	8	10	12	14	16	18
	3	3	6	9	12	15	18	21	24	27
	4	4	8	12	16	20	24	28	32	36
	5	5	10	15	20	25	30	35	40	45
	6	6	12	18	24	30	36	42	48	54
	7	7	14	21	28	35	42	49	56	63
	8	8	16	24	32	40	48	56	64	72
	9	9	18	27	36	45	54	63	72	81

For example, the case of $u = 2$ never involves the product 2×5 and therefore never produces a number ending in zero.

(22) $\left\{ \begin{array}{l} 2 \times 2 = 4 \\ 2 \times 4 = 8 \\ 2 \times 8 = 16 \quad [\text{right-most digit is } 6] \\ 2 \times 6 = 12 \quad [\text{right-most digit is } 2] \end{array} \right.$

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 this means that for n , an integer $n > 2$, the $[n-1]^{th}$ root of n can only be irrational.

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 ..., an irrational number which squared equals the integer 3. Picture the multiplication process.

	1.732.050.807.77 ...
	× 1.732.050.807.77 ...

multiply by 1.	1.732,050,807,77 ...
multiply by .7	1.212,435,565,39 ...
multiply by .03	0.051,961,524,22 ...
...
...

sum the above	3 exactly

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" non-zero digit and consequently can avoid the problem presented above of the right-most non-zero digit always producing a fractional part of the result after raising the number to a power. That that is so is evidenced by the many cases similar to the above example for the square root of 3.

But, what about repeating decimals? They have a "string of non-zero digits infinitely to the right of the decimal point". Yet they are rational.

Repeating decimals do not really "have an infinite string of non-zero digits to the right of the decimal point", it is pseudo, only apparent, 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, as an example, the repeating decimal $\frac{1}{3} = 0.3333 \dots$. 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 $\frac{1}{10} = 0.1$, not a repeating decimal. 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.