AN EXTRAORDINARILY SIMPLE PROOF OF FERMAT'S LAST THEOREM
Fermat's "marvelous proof"?

Miguel Ángel Rodríguez-Roselló
(Ph.D. in Computer Science, B.Sc. in Physics, M.Sc. in Knowledge Engineering)
email: marosellom@gmail.com

This article presents an extraordinarily simple proof of Fermat's Last Theorem (FLT), which may be the "marvelous proof" he claimed to have, but which did not fit in the margin of the book he was reading (the Arithmetica of Diophantus of Alexandria). As a consequence of the proof, an alternative formulation of the Pythagorean terns is arrived at.

Statement of the theorem

If n is an integer greater than 2, there are no positive integers x, y, z, such that they satisfy the so-called "Fermat equation", in short, equation [F].

$$\boxed{x^n + y^n = z^n} \quad [F]$$

About Fermat's equation

Fermat's equation is the most famous diophantine equation. A diophantine equation is an equation in which only constants and integer variables appear. In the case of [F], there are no constants and the variables (x, y, z, n) represent positive integers.

We can assume that the triples (x, y, z) are primitive, i.e., that they have no common factor, i.e., $gcd(x, y, z) = 1$. If they did, then the initial equation could be reduced to one without that common factor.

Proof

In equation [F], dividing x^n and y^n by z, we have:

$$x^n = c_1 z + r_1$$
$$y^n = c_2 z + r_2$$

with c_i being the integer quotients and r_i being the remainders. Therefore, $0 \leq r_i < z$.

Adding both equations, and calling $c = c_1 + c_2$ and $r = r_1 + r_2$, we have:

$$\boxed{z^n = cz + r} \quad [G]$$

In this way, we have reduced the initial expression into a simpler, linear one, where the values c and r depend on x, y, z and n.

If either of the two remainders (r_1 or r_2) is zero, for example r_1, we have:

$$x^n = c_1 z, \quad y^n = c_2 z + r_2$$
$$z^n = c_1 z + c_2 z + r_2$$
$$z^n = cz + r_2$$

For the latter equation to be satisfied, r_2 must necessarily be a multiple of z, but $r_2 < z$. Therefore, it is impossible.

If $r = 0$, then:

$$r_1 = r_2 = 0$$
$$x^n = c_1 z, \quad y^n = c_2 z$$
$$z^n = c_1 z + c_2 z = cz$$

And x^n, y^n and z^n have a common factor, z, contrary to assumption. Therefore, r cannot be zero: $r > 0$.

For equation [G] to be satisfied, r must be a multiple of z. Since $0 < r < 2z$, it follows that $r = z$. The expressions x^n and y^n are linked because their remainders when divided by z are complementary to z. In this link lies the essence of the proof.

The above expression is now even simpler:

$$\boxed{z^n = cz + z} \quad [Z]$$

On both sides of this equation there is a common factor (z) for all $n \geq 2$.

Let's analyze the equation resulting from eliminating the common factor z. Then [Z] becomes

$$\boxed{z^{n-1} = c + 1} \quad [R]$$

Equation [R] reveals the true structure of equation [F], its internal structure, the link $r_1 + r_2 = z$, which must exist for [F] to be fulfilled.

Equations [F] and [R] are algebraically equivalent, but the exponents of the three expressions have changed.

We know the exponents of z ($n - 1$) and 1 (1). Regarding c, we do not know its degree as a power, so we will call its exponent k, being $k \geq 1$.

Since it is a necessary (but not sufficient) condition that the three exponents are equal, we have:

$$n - 1 = k = 1$$

Therefore, $\boxed{n = 2}$.

But this condition is also sufficient, because for this value of n, Fermat's equation has a geometrical interpretation: the Pythagorean ternaries.

With this result the theorem is proved: n cannot be greater than 2.

The new formula for Pythagorean triples

The Pythagorean triples fulfill the traditional equation [T]:

$$\boxed{z^2 = x^2 + y^2} \quad [T]$$

The integer division between two positive integers, n_1 and n_2, will be represented as $[n_1/n_2]$. Therefore, $c_1 = [x^n/z]$ and $c_2 = [y^n/z]$.

For $n = 2$, the equation [R] is reduced to $z = c + 1$, i.e,

$$\boxed{z = [x^2/z] + [y^2/z] + 1} \quad [P]$$

This equation is an alternative expression to the traditional one [T] without the common factor z. For example, for the triple (3, 4, 5) it holds:

$$[3^2/5] + [4^2/5] + 1 = 1 + 3 + 1 = 5.$$

Andrew Wiles' proof

Since Pierre de Fermat posed his conjecture in 1637, all the great mathematicians have tried to prove it, without success. There have been proofs for certain particular cases of n, but not for the general case. Fermat himself proved it for $n = 4$.

Finally, the Englishman Andrew Wiles presented a proof in 1993, which failed in the first instance, but was corrected by Wiles himself with the help of a mathematician friend named Richard Taylor and finally published in 1995 [3, 5, 6]. The proof took 109 pages and required the use of advanced and sophisticated mathematical techniques, not at all intuitive and difficult to understand, even for professional mathematicians. Moreover, Wiles did not prove the theorem directly. He proved it as a corollary of another more general theorem, the Taniyama-Shimura theorem. The FLT is one of the great theorems in the history of mathematics.

Wiles spent many years working on the problem. With his feat, Wiles achieved worldwide fame, receiving numerous awards, including the Abel Prize, considered the Nobel Prize in Mathematics.

Fermat's "marvelous proof"?

Perhaps the simple proof of this article is the "marvelous proof" that Fermat claimed to have and that did not fit in the margin of the copy of the book "Arithmetica", by Diophantus of Alexandria [1, 4].

But, because of the complexity of Wiles' proof, most mathematicians believe that Fermat was mistaken in believing he had such a marvelous proof.

So the so-called "most difficult theorem in the world" [2] is, paradoxically, one of the easiest. Sometimes the simplest thing is the hardest thing to discover.

The proof in a margin

We do not know if this proof is the one Fermat claimed to have, but we can be sure that if it was, it would have fit in the margin of the book he was reading:

$x^n + y^n = z^n$
Dividing x^n and y^n by z,
$x^n = c_1 z + r_1 \quad 0 \leq r_1 < z$
$y^n = c_2 z + r_2 \quad 0 \leq r_2 < z$
$c = c_1 + c_2 \quad r = r_1 + r_2$
$0 < r < 2z \rightarrow r = z$ (r cannot be 0)
$z^n = cz + z$
$z^{n-1} = c + 1$
We do not know the degree of c as a power.
Let's call k the exponent.
Equalizing the three exponents,
$n - 1 = k = 1 \rightarrow n = 2$

Bibliography

[1] Aczel, Amir D. (1998). Fermat's Last Theorem. Unlocking the Secret of an Ancient Mathematical Problem. Delta.

[2] Areán Alvárez, Luis Fernando (2012).El Teorema de Fermat, El Problema más difícil del Mundo. (Fermat's Theorem. The most difficult problem in the world). RBA Coleccionables.

[3] Bell, Eric T. (1998). The Last Problem. New York: The Mathematical Association of America. ISBN 978-0-88385-451-8.

[4] Singh, Simon (1998). Fermat's Enigma. The Epic Quest to Solve the World's Greatest Mathematical Problem. Anchor Books.

[5] Stevens, Glenn (1997). "An Overview of the Proof of Fermat's Last Theorem". Modular Forms and Fermat's Last Theorem. New York: Springer. pp. 1-16. ISBN 0-387-94609-8.

[6] Wiles, Andrew (1995). Modular Elliptic Curves and Fermat's Last Theorem. Annals of Mathematics, Second Series, vol. 141 (1995), pp. 443-551 (109 pages). Mathematics Department, Princeton University, https://doi.org/10.2307/2118559