1

Direct Proof of Fermat's Last Theorem

by Roberto Iannone

Abstract

In 1994 the mathematician Andrews Wiles proved, using concepts of modern mathematics, namely the Modular Elliptic Curves, the Fermat's Last Theorem. That demonstration is long and it is understandable to mathematic specialists, moreover, these mathematical concepts were not known at the time when Fermat lived, so he could not prove it throug this road. I thought that there might be another simpler proof which would use the properties of algebraic equations and inequalities. These mathematical concepts were known at the time in which Fermat lived and which, therefore, could apply for the proof of the theorem of which he wrote, in the margin of a page of the book of Arithmetica of Diophantus he was reading, to have found a demonstration "wonderful," but that he had not could to write to the narrowness of the margin itself. I propose, therefore, the following demonstration that directly uses the mathematical properties of algebraic equations and inequalities that are understood by all those who study algebra.

T h e o r e m

It is possible to divide a power, with an integer base of degree n, into the sum of two integer powers, of the same degree, only if n is equal to 2.

Demonstration

1) - $X^n + Y^n = Z^n$

X,Y,Z,n are integers such that **X<Y<Z** that is **X+Y > Z**, why $(X+Y)^n = X^n + Y^n + R$ (R sum of the products of Newton's binomial), thus $(X+Y)^n > X^n + Y^n = Z^n$, therefore $(X+Y)^n > Z^n$ and extracting the nth root we have that **X + Y > Z** . We also have that

2) - $\frac{X^n + Y^n}{Z^n} = 1$ and more

3) - $\frac{X^n}{Z^n} > 0 < \frac{1}{2}$ and also .

4) - $\frac{Y^n}{Z^n} > 0 > \frac{1}{2}$ we raising to **1/n, 3)** and **4),** we have

5) - $\frac{X}{Z} > 0 < \left(\frac{1}{2}\right)^{1/n}$ and yet

6) - $\frac{Y}{Z} > 0 > \left(\frac{1}{2}\right)^{1/n}$ and so adding the **5)** and the **6)** we have

7) - $\frac{X+Y}{Z} > 1 < 2\left(\frac{1}{2}\right)^{1/n}$ and simplifying **second term** we have

$$\frac{X+Y}{Z} > 1 < \left(2^{n-1}\right)^{1/n}$$

the value of the second member **of the inequality, forany value of** n**,is always** < 2**,** furthermore, being $X+Y > Z$ and $X < Y < Z$ **,** as indicated in number **1), the second member, equally, is always** < 2**,** therefore we can write also that

8) - $\frac{X+Y}{Z} > 1 < 2^{1/n}$ being the first members of the inequalities **7)** and **8), equal,** there must also have **equality** of the **second members** and thus we must find the value of n **that satisfies both,** so we can write that

9)-$<\left(2^{n-1}\right)^{1/n} = <2^{1/n}$ we **raise** the members to n that are $<\left[\left(2^{n-1}\right)^{1/n}\right]^n = <\left(2^{1/n}\right)^n$ and we obtain $<2^{n-1} = <2$ **if we put** to the exponent $n = 2$ we develop and obtain the **equality** $< 2 = < 2$**,**therefore the exponent $n=2$ satisfies the **equality** and it is the only exponent that satisfies her. Any other value of $n > 2$ does not satisfy **equality,** in fact there would be increasing values and therefore greater than **2.**

We have therefore found also the exponent **2** that satisfies the inequalities **7).** From what has been said above, let's now check and proceed with the substituting the exponent **n** with **2** on the second member of inequality **7)** and then we raise the first and second members to the exponent **2** and we have

10) - $\left(\frac{X + Y}{Z} \right)^2 > 1 < \left[\left(2^{2-1} \right)^{1/2} \right]^2$ we develop and we obtain

11) - $\frac{X^2 + Y^2 + 2*X*Y}{Z^2} > 1 < 2$ the numerator of the first member of the inequality **is the square of a binomial** of which: $X^2 + Y^2$ are the two powers, of the same degree, and that are equal to the first member of the equation **1)** and **2 *X*Y** is the product relating to the **binomial.** We delop and obtain the equation **2)** **from which it is clear that**

12) - $\frac{X^2 + Y^2}{Z^2} = 1$ and $\frac{2*X*Y}{Z^2} < 1$ **that is to say**

it is possible to divide a power, with an integer base of degree n, into the sum of two integer powers, of the same degree, only if n is equal to $\underline{2.}$ Therefore we can write the equation **1)**, with integers:

13) - $X^2 + Y^2 = Z^2$

Q. E. D.

References

[1] A. Wiles - Modular elliptic curves and Fermat's Last Theorem
http://math.stanford.edu/~lekheng/flt/wiles.pdf

[2] Simon Singh, L'ultimo teorema di Fermat, Milano, Rizzoli, 1999

[3] Wikipedia: Fermat's Last Theorem