Elementary proof of Fermat-Wiles' Theorem

by Ahmed Idrissi Bouyahyaoui

***

Fermat-Wiles' Theorem :

(1) « the equality $x^n+y^n=z^n$, with $n, x, y, z \in N^+$, is impossible for $n>2$. »

***

Abstract :

In the Euclidean division of $x^n = z^n - y^n$ by $x^{n-1} = az^{n-1} - by^{n-1}$ with $(a,b) \in Z^2$, remainder must be zero implying the equality $b^2 y^{n-2} = a^2 z^{n-2}$ which is impossible for $n>2$ since $x^{n-1} = az^{n-1} - by^{n-1}$ and x, y, z are coprim numbers.

***

We suppose x, y and z are coprim numbers.

Given gcd(y,z)=1 and the corollary of the Bachet's theorem (1624), it exists two relative integers a and b such that :

(2) $x^{n-1} = az^{n-1} - by^{n-1}$

In the Euclidean division $(z^n - y^n) : (az^{n-1} - by^{n-1})$ $(= x^n : x^{n-1} = x)$ remainder must be zero.

Let us put the Euclidean division :

$z^n - y^n$ | $az^{n-1} - by^{n-1}$

$- z^n + (b/a)zy^{n-1}$ x = $z/a + y/b$

$- z/a - y/b$

$- y^n + (b/a)zy^{n-1}$

$+ y^n - (a/b)yz^{n-1}$

$R_1 = (b/a)zy^{n-1} - (a/b)yz^{n-1}$

$- (b/a)zy^{n-1} + z^n$

$R_2 = z^n - (a/b)yz^{n-1}$

$+ (a/b)yz^{n-1} - y^n$

$R_3 = z^n - y^n \neq 0$, $x, y, z \in N^+$ and gcd(y,z)=1

If the remainder R_2 is zero then the quotient $x = z/a + y/b - z/a = y/b$, so $bx = y$, which is impossible since gcd(x,y)=1. Therefore only the remainder R_1 must be equal to zero :

(3) $R_1 = (b/a)zy^{n-1} - (a/b)yz^{n-1} = ((b/a)y^{n-2} - (a/b)z^{n-2})yz = 0$

So $(b/a)y^{n-2} - (a/b)z^{n-2} = 0$ which implies the equality :

(4) $b^2 y^{n-2} = a^2 z^{n-2}$

where, for $n>2$, as gcd(y,z)=1, y divides a^2 and z divides b^2, and then, according to the equality $x^{n-1} = az^{n-1} - by^{n-1}$, gcd(x,y) >1 and gcd(x,z) >1, but gcd(x,y)= gcd(x,z)=1 (hypothesis). Therefore, the equalities $b^2y^{n-2} - a^2z^{n-2} = 0$ (R), $x^{n-1} = az^{n-1} - by^{n-1}$ (d), $x^n = z^n - y^n$ (D) are impossible for $n>2$.

ahmed.idrissi@free.fr INPI - Paris (France)