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 of proof :

Let $x^n = z^n - y^n$ and $x^{n-1} = az^{n-1} - by^{n-1}$, $(a, b) \in Z^2$.

In the division with zero remainder of $ab(z^n - y^n)$ by $az^{n-1} - by^{n-1}$, it exists one and only one remainder equal to zero and valid, and then implies 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 integers.

**

The tree of the division with zero remainder :

We suppose x, y and z are coprim integers.

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

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

We have the division

(2) $ab(z^n - y^n) : (az^{n-1} - by^{n-1})$

which must have only one remainder equal to zero and valid.

Research of the optimal branch of the division :

Let us put the division and carry out the operations until obtaining a remainder already obtained (end of the operations cycle) and then obtain the candidate remainders to be equal to zero and valid. For that, we must carry out a method of reduction of the power n which is to remove the monomials with the power n such that to have only monomials with power (n-1) or less.

This method optimizes the research of the unique remainder which can be equal to zero and valid by discarding the zero remainders not valid.

Setting of the division with zero remainder :

$z^n - y^n = (az^{n-1} – by^{n-1})x$, $q = x$

ab * $z^n - y^n$

$abz^n - aby^n$ (D_1) $|az^{n-1} – by^{n-1}$ (d)

$- abz^n + b^2zy^{n-1}$ $bz + ay –bz + bz$

------------------- Evaluation of remainders and partial quotients :

$R_{1=}$ $- aby^n + b^2 zy^{n-1}$ $R_1 = 0$ => $q_1 = abx = bz$ => $\mathbf{ax = z}$ => $R_1 \neq 0$

$aby^n - a^2yz^{n-1}$ pgcd(x, z) = 1

$R_2 =$ $\mathbf{b^2zy^{n-1} - a^2yz^{n-1}}$ $R_2 = 0$ => $b^2y^{n-2} - a^2 z^{n-2} = 0$ => $q_2 = abx = bz + ay$

$- b^2zy^{n-1} + abz^n$ pgcd(y, a) >1, pgcd(z, b) >1 and $x^{n-1} = az^{n-1} - by^{n-1}$

==> pgcd(x, y) > 1, pgcd(x, z) > 1 for n > 2.

$R_3 =$ $abz^n - a^2yz^{n-1}$ $R_3 = 0$ => $q_3 = abx = bz + ay –bz$ => $\mathbf{bx = y}$ => $R_3 \neq 0$

$b^2zy^{n-1} - abz^n$ pgcd(x, y) = 1

$\mathbf{b^2zy^{n-1} - a^2yz^{n-1}}$ end of the operations cycle.

**

The evaluation of remainders and partial quotients allowed obtaining the remainder which can be zero and valid obtained by deduction : two remainders out of the three obtained cannot be equal to zero.

So, only the remainder R_2 obtained in the division above can be equal to zero :

(3) $R_2 = b^2zy^{n-1} - a^2yz^{n-1} = 0$ implies the equality

(4) $b^2 y^{n-2} = a^2 z^{n-2}$ which is impossible for n > 2 since $x^{n-1} = az^{n-1} - by^{n-1}$
and x, y, z are coprim integers.

Therefore, the equalities

(5) $b^2y^{n-2} - a^2z^{n-2} = 0$ (R), $x^{n-1} = az^{n-1} - by^{n-1}$ (d), $x^n = z^n - y^n$ (D)

such that D = xd are impossible for n > 2.

Another formulation of elementary proof :

application of the equivalence in the direct division.

We have the direct division :

(1) $ab(z^n - y^n) = (az^{n-1} - by^{n-1})(bz + ay) + b^2zy^{n-1} – a^2yz^{n-1}$

and the quivalence

(2) $D = d*q \Leftrightarrow r = 0$

(D) dividend = (d) divisor * (q) quotient + (r) remainder.

$abx = bz + ay \quad \Leftrightarrow \quad b^2zy^{n-1} – a^2yz^{n-1} = 0$

$x^{n-1} = az^{n-1} - by^{n-1}$

As $ab(z^n - y^n) = (az^{n-1} - by^{n-1})abx$ (integer division) since $x^{n-1} = az^{n-1} - by^{n-1}$, the remainder $b^2zy^{n-1} – a^2yz^{n-1}$ can be zero in application of the equivalence (2) :

(3) $b^2zy^{n-1} – a^2yz^{n-1} = 0 \implies b^2y^{n-2} = a^2z^{n-2}$,

impossible equality for $n > 2$ since $x^{n-1} = az^{n-1} - by^{n-1}$ and x, y, z are coprim integers.