# 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 Euclidean-division of $ab(z^n - y^n)$ by $az^{n-1} - by^{n-1}$, it exists one and only one remainder which can be equal to zero and valid, and which 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 Euclidean-division :

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 remainders equal to zero and not interesting or not valid.

Setting of the Euclidean-division :

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

$ab * z^n - y^n$

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

---

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

---

Evaluation of remainders and partial quotients :

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

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

---

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

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

$\Rightarrow$ pgcd(x, y) > 1, pgcd(x, z) > 1 for n > 2.

---

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

$b^2zy^{n-1} - abz^n$ 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 equal to zero and 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) $b^2y^{n-2} = a^2z^{n-2}$ 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 $n > 2$.

# 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 $ab(z^n - y^n) = (az^{n-1} - by^{n-1})(bz + ay) + b^2zy^{n-1} – a^2yz^{n-1}$, the term $b^2zy^{n-1} – a^2yz^{n-1}$ must be zero according to the tree of the Euclidean-division.

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

**

## The direct division :

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

normalized into the Euclidean-division:

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

(According to the tree of the Euclidean-division, remainder is zero.)

If it exists a couple (a, b) $\in Z^2$ such that :

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

$abx = bz + ay$ (Problem not resolved.)

then remainder $b^2zy^{n-1} – a^2yz^{n-1} = 0$.

What implies the equality :

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

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

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

Remark :

Let the system :

(6) $a^x + b^y = c^z$, (a, b, c, x, y, z) $\in N^{*6}$ and a, b, c are coprim integers.

(7) $a^x = c^z - b^y$

(10) $a^{x-1} = uc^{z-1} - vb^{y-1}$ , $(u, v) \in Z^2$

As described above for the division $(z^n-y^n) : (az^{n-1}-by^{n-1})$, the remainder of the division $(c^z-b^y) : (uc^{z-1} - vb^{y-1})$ which can be zero implies the equality :

(11) $v^2b^{y-2} = u^2c^{z-2}$ ,

which is impossible for (y > 2 or z > 2) or, by symmetry, for (x > 2 or z > 2), or (for x > 2 or y > 2).