Preuve élémentaire du Théorème de Fermat-Wiles

par Ahmed Idrissi Bouyahyaoui

Théorème de Fermat-Wiles :

(1) « L'égalité $x^n + y^n = z^n$, où $n, x, y, z \in N^*$, est impossible pour $n > 2$. »

**

Résumé de la preuve :

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

Dans la division euclidienne de $ab(z^n - y^n)$ par $az^{n-1} - by^{n-1}$, il existe un seul reste qui peut être nul et valide et ainsi impliquer l'égalité $b^2 y^{n-2} = a^2 z^{n-2}$ qui est impossible pour $n > 2$ puisque $x^{n-1} = az^{n-1} - by^{n-1}$ et x, y, z sont des nombres entiers premiers entre eux.

**

L'équivalence dans la division euclidienne :

On suppose x, y et z sont des nombres premiers entre eux.

Etant donnés pgcd(y, z) = 1 et le corollaire du théorème de Bachet (1624), il existe deux entiers relatifs a et b tel que :

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

On a la division :

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

normalisée pour être une division euclidienne :

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

Comme $(z^n - y^n) = (az^{n-1} - by^{n-1})x$, la division entière est possible dans (4).

Dans la division euclidienne D = dq + r, on a l'<u>équivalence</u> :

(5) D = dq (division entière) $\Leftrightarrow$ r = 0 (reste nul)

Donc, pour que la division :

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

soit entière, il suffit que le reste soit nul.

En appliquant <u>l'équivalence euclidienne</u> (5) :

(7) $b^2zy^{n-1} - a^2yz^{n-1} = 0 \quad \Leftrightarrow \quad ab(z^n - y^n) = (az^{n-1} - by^{n-1})abx$ (dq)

$abx = bz + ay$ (q)

on obtient l'égalité :

(8) $b^2y^{n-2} = a^2z^{n-2}$ qui est impossible pour $n > 2$ puisque $x^{n-1} = az^{n-1} - by^{n-1}$ et x, y, z sont des nombres premiers entre eux.

Pour $n = 2$, on a $a^2 = b^2$.

Par conséquent, les égalités :

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

tel que $D = dx$ sont impossibles pour $n > 2$.

***

Pose de la division euclidienne :

On suppose x, y et z sont des nombres premiers entre eux.

Etant donnés pgcd(y, z) = 1 et le corollaire du théorème de Bachet (1624), il existe deux entiers relatifs a et b tel que :

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

On a la division

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

qui doit avoir un seul reste nul valide.

Posons la division et effectuons les opérations jusqu'à l'obtention d'un reste déjà obtenu (fin du cycle des opérations) et ainsi obtenir les restes candidats à être nuls. Pour cela, on doit appliquer une méthode de réduction de la puissance n qui consiste à éliminer les monômes comportant la puissance n de sorte à n'avoir que des monômes comportant au plus la puissance n – 1.

Cette méthode optimise la recherche (dans l'arbre de la division) du seul reste pouvant être nul en écartant des restes nuls sans suite ou non valides.

Pose de la division euclidienne :

	$ab * z^n - y^n$	
(D)	$abz^n - aby^n$	$\vert az^{n-1} - by^{n-1}$ (d)

	$- abz^n + b^2zy^{n-1}$	$bz + ay - bz + bz$
	--------------------	<u>Evaluation des restes et des quotients partiels :</u>
$R_{1=}$	$- aby^n + b^2 zy^{n-1}$	$R_1 = 0 \Rightarrow q_1 = abx = bz \Rightarrow$ **ax = z** $\Rightarrow R_1 \neq 0$
	$aby^n - a^2yz^{n-1}$	pgcd(x, z) = 1

$R_2=$	$\mathbf{b^2zy^{n-1} - a^2yz^{n-1}}$	$R_2 = 0 \Rightarrow b^2y^{n-2} - a^2 z^{n-2} = 0 \Rightarrow q_2 = abx = bz + ay$
	$- b^2zy^{n-1} + abz^n$	pgcd(y, a) >1, pgcd(z, b) >1 et $x^{n-1} = az^{n-1} - by^{n-1}$
		==> pgcd(x, y) > 1, pgcd(x, z) > 1 pour n > 2.

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

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

$\mathbf{b^2zy^{n-1} - a^2yz^{n-1}}$ fin du cycle des opérations.

**

L'évaluation des restes et des quotients partiels a permis de déterminer le reste, qui peut être nul, obtenu par déduction : deux restes sur les trois obtenus ne peuvent pas être nuls.

Ainsi, seul le reste R_2 dans la division euclidienne ci-dessus peut être nul :

(3) $\quad R_2 = b^2zy^{n-1} - a^2yz^{n-1} = 0$ implique l'égalité

(4) $\quad b^2 y^{n-2} = a^2 z^{n-2}$ qui est impossible pour $n > 2$ puisque $x^{n-1} = az^{n-1} - by^{n-1}$ et x, y, z sont des nombres premiers entre eux.

Pour $n = 2$, on a $a^2 = b^2$.

Par conséquent, les égalités :

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

tel que D = dx sont impossibles pour $n > 2$.

***

***

Remarque :

Soit le système :

(1) $\quad a^x + b^y = c^z$, $(a, b, c, x, y, z) \in N^{*6}$ et a, b, c premiers entre eux.

(2) $\quad a^x = c^z - b^y$

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

Comme décrit ci-dessus pour la division $(z^n - y^n)$: $(az^{n-1} - by^{n-1})$, le reste de la division $(c^z - b^y)$: $(uc^{z-1} - vb^{y-1})$ qui peut être nul, implique l'égalité :

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

égalité impossible pour (y > 2 ou z > 2), et par symétrie, ou pour (x > 2 ou z > 2), ou pour (x > 2 ou y > 2).