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. »

**

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.

**

L'arbre de la division de reste nul :

On suppose x, y et z sont des nombres entiers 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) $ab(z^n - y^n) : (az^{n-1} - by^{n-1})$

qui doit avoir un seul reste nul valide.

Recherche de la branche optimale de l'arbre de la division :

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 du seul reste pouvant être nul et valide en écartant des restes nuls non valides.

Pose de la division de reste nul :

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

$ab * (z^n - y^n)$

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

$R_3=$	$abz^n - a^2yz^{n-1}$	$R_3 = 0 \Rightarrow q_3 = abx = bz + ay - bz \Rightarrow$ $\mathbf{bx = y}$ $\Rightarrow R_3 \neq 0$
	$b^2zy^{n-1} - abz^n$	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 (division entière) et valide, <u>obtenu par déduction</u> : deux restes sur les trois obtenus ne peuvent pas être nuls.

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

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

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

Par conséquent, les égalités :

(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)

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

Autre formulation de preuve élémentaire :

Application de l'équivalence dans la division directe.

On a la division directe :

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

et l'équivalence

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

(D) dividende = (d) diviseur * (q) quotient + (r) reste.

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

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

Comme $ab(z^n - y^n) = (az^{n-1} - by^{n-1})abx$ est une division de reste nul , le reste $b^2zy^{n-1} - a^2yz^{n-1}$ peut être nul dans l'application de l'équivalence (2) :

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

égalité 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.