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 :

Dans la division de $x^n = z^n - y^n$ par $x^{n-1} = az^{n-1} - by^{n-1}$, (a,b) $\in Z^2$, le reste doit être égal à zéro impliquant l'égalité $b^2y^{n-2} = a^2z^{n-2}$ 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.

L'application du schéma de la procédure de la division euclidienne jusqu'au reste égal à $z^n- y^n$, puis l'évaluation des restes et des quotients partiels permettent d'obtenir l'unique reste qui peut et doit être nul.

***

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

La division $(z^n - y^n) : (az^{n-1} - by^{n-1})$ $(x = x^n : x^{n-1})$ doit avoir un reste nul.

Posons la division et effectuons les opérations jusqu'à apparition du reste égal au dividende $z^n - y^n$ et obtenir ainsi les restes candidats à être nuls :

	$x^n = z^n - y^n$ (D_0)	$\mid x^{n-1} = az^{n-1} - by^{n-1}$ (d)	

	$- z^n + (b/a)zy^{n-1}$	$z/a + y/b - z/a - y/b$	
	---	Evaluation des restes :	
$D_1 = R_0 =$	$- y^n + (b/a)zy^{n-1}$	$R_0 = 0 \Rightarrow (q)=x= z/a \Rightarrow$ **ax=z** $\Rightarrow R_0 \neq 0$	
	$+ y^n - (a/b)yz^{n-1}$		

$D_2 = R_1 =$	$(b/a)zy^{n-1} - (a/b)yz^{n-1}$	$R_1 =0 \Rightarrow b^2y^{n-2}-a^2z^{n-2}=0 \Rightarrow (q)=x=z/a+y/b$	
	$- (b/a)zy^{n-1} + z^n$		

$D_3 = R_2 =$	$z^n - (a/b)yz^{n-1}$	$R_2=0 \Rightarrow (q)=x=z/a+y/b -z/a \Rightarrow$ **bx=y** $\Rightarrow R_2\neq 0$	
	$+ (a/b)yz^{n-1} - y^n$		

$R_3 =$	$z^n - y^n \neq 0$;	fin du cycle des opérations.	

ahmed.idrissi@free.fr INPI - Paris

Evaluation des restes et des quotients partiels :
Si le reste R_0 est nul alors le quotient est x = z/a, soit ax=z, égalité impossible puisque pgcd(x,z)=1.
Si le reste R_2 est nul alors le quotient est x = z/a + y/b - z/a = y/b, soit bx = y, égalité impossible puisque pgcd(x,y)=1.
$R_3 = z^n - y^n \neq 0$; $y, z \in N^*$ et pgcd(y,z)=1.

L'application du schéma de la procédure de la division euclidienne a permis d'obtenir les restes et le reste qui peut et doit être nul est unique et obtenu par déduction : trois restes sur les quatre obtenus ne peuvent pas être nuls.
Donc le problème d'existence du reste nul ne se pose pas.

Ainsi seul le reste R_1 peut et doit être nul :

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

Soit $(b/a)y^{n-2} - (a/b)z^{n-2} = 0$ ce qui implique l'égalité :

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

où, pour n>2, comme pgcd(y,z)=1, y divise a^2 et z divise b^2, soient pgcd(a,y) >1 et pgcd(b,z) >1.
Par suite, d'après l'égalité $x^{n-1}=az^{n-1}-by^{n-1}$ (2), pgcd(a,y) >1 implique pgcd(x,y) >1 et pgcd(b,z) >1 implique pgcd(x,z) >1 mais pgcd(x,y) = pgcd(x,z) =1 (hypothèse).

Par conséquent, les égalités $b^2y^{n-2}-a^2z^{n-2}=0$ (R), $x^{n-1}=az^{n-1}-by^{n-1}$ (d), $x^n = z^n - y^n$ (D) sont impossibles pour n>2.
***

ahmed.idrissi@free.fr INPI - Paris

Division avec des nombres entiers :

$a * z^n - y^n$ (D_0) | $az^{n-1} - by^{n-1}$ (q)

$=> az^n - ay^n$ $z + ay - bz + bz$

$-az^n + bzy^{n-1}$ Comme on a multiplié D_0 par a, puis D_1 par b, on a $z/a + ay/ab - bz/ab + bz/ab$

Evaluation des restes et des quotients partiels :

$b * bzy^{n-1} - ay^n$ (D_1) $R_0 = 0 => (q)= x = z/a$ => **ax = z** => $R_0 \neq 0$

$D_1=R_0=$ $=> b^2zy^{n-1} - aby^n$

$-a^2yz^{n-1} + aby^n$

>>>>$R_1=$ $b^2zy^{n-1} - a^2yz^{n-1}$ (D_2) $R_1=0 => b^2y^{n-2}-a^2z^{n-2}=0$ => $(q)= x = z/a + y/b$

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

$D_3=R_2=$ $abz^n - a^2yz^{n-1}$ (D_3) $R_2=0 =>(q)= x= z/a+y/b -z/a$ => **bx = y** => $R_2\neq0$

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

R_1 <<<< $b^2zy^{n-1} - a^2yz^{n-1}$ fin du cycle des opérations.

***

Remarque :

Soit le système :

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

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

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

En appliquant l'algorithme décrit ci-dessus à la division de $c^z - b^y$ par $uc^{z-1} - vb^{y-1}$, le reste, qui peut et doit être nul, implique l'égalité :

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

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

ahmed.idrissi@free.fr INPI - Paris