Le théorème de Fermat-Wiles
et le critère d'irréductibilité d'Eisenstein

Ahmed Idrissi Bouyahyaoui

<<<>>>

Le théorème de Fermat-Wiles :

L'égalité $z^n = x^n + y^n$, x, y, z et n des nombres entiers, est impossible pour n>2 .

<<<>>>

Essai de démonstration
utilisant le critère d'irréductibilité d'Eisenstein
pour n=p premier impair

Abstract :

Setting m = x+y-z, we obtain :

x = (x+y-z)+z-y = m+u , u=z-y ;

y = (x+y-z)+z-x = m+v , v=z-x ;

z = (x+y-z)+(z-y)+(z-x) = m+u+v = m+w, w=u+v .

Setting x=m+u, y=m+v and z=m+w in equation

(1) $x^p + y^p - z^p = 0$, we obtain :

(2) $(m+u)^p - ((m+w)^p - (m+v)^p) = (m+u)^p - u(\sum_{i=1}^{p} (m+u+v)^{p-i}(m+v)^{i-1}) = 0$,
with gcd(u,pv)=1, $u=u_0^p$, gcd(v,p)= ap (a=0 or 1), $v=p^\beta v_0^n$ ($\beta\geq 0$ and $\gcd(v_0,p)=1$), $m=m_0u_0$ ($\gcd(m_0,u_0)=1$), $m=m_1v_0$ ($\gcd(m_1,v_0)=1$) .

After dividing equation (2) by $u=u_0^p$, we obtain :

(3) $(m_0+ u_0^{p-1})^p - \sum_{i=1}^{p} (m_0u_0+ u_0^p +v)^{p-i}(m_0u_0+v)^{i-1} = 0$.

Let P(X) the polynomial associated to equation (3) expanded into a sum of monomials, its reduction modulo k prime$|u_0$ with k<p and pv^{p-1} [k] >1 or k prime$|v_0$ with k<p and $p*p^\beta u^{p-1}$ [k] >1 ($\beta\geq 0$) gives :

(4) $R(X) = P(X)\ [k] = X^p - c$, $c = p*v^{p-1}$ [k] or $p*p^\beta u^{p-1}$ [k] .

Let q^γ a prime factor of c, then $1 < q^\gamma < k < p$, $\gamma < p$ and $\gcd(\gamma,p)=1$, and so $R(X) = X^p - c$ is irreducible in $Z_k[X]$.

R(X)=P(X) [k] being irreducible in $Z_k[X]$, P(X) is irreducible in Z[X] and, therefore, hasn't integer roots .

Therefore, the equation $x^p+y^p-z^p=0$ hasn't nonzero integer solutions for all odd prime p .

<<<>>>

Résumé :

En posant m = x+y-z, on obtient :
x = (x+y-z)+z-y = m+u , u=z-y ;
y = (x+y-z)+z-x = m+v , v=z-x ;
z = (x+y-z)+(z-y)+(z-x) = m+u+v = m+w, w=u+v .
En posant x=m+u, y=m+v et z=m+w dans l'équation
(1) $x^p + y^p - z^p = 0$, on obtient :
(2) $(m+u)^p - ((m+w)^p - (m+v)^p) = (m+u)^p - u(\sum_{i=1}^{p} (m+u+v)^{p-i}(m+v)^{i-1}) = 0$,
avec pgcd(u,pv)=1, $u=u_0^p$, pgcd(v,p)= ap (a=0 ou 1), $v=p^\beta v_0^n$ ($\beta \geq 0$ et pgcd(v_0,p)=1), $m=m_0u_0$ (pgcd(m_0,u_0)=1), $m=m_1v_0$ (pgcd(m_1,v_0)=1) .
Après division de l'équation (2) par $u=u_0^p$, on obtient l'équation :
(3) $(m_0+ u_0^{p-1})^p - \sum_{i=1}^{p} (m_0u_0+ u_0^p +v)^{p-i}(m_0u_0+v)^{i-1} = 0$.
Soit P(X) le polynôme associé à l'équation (3) développée en une somme de monômes, sa réduction modulo k premier$|u_0$ avec k<p et pv^{p-1} [k] >1 ou k premier$|v_0$ avec k<p et $p*p^\beta u^{p-1}$ [k] >1 donne :
(4) $R(X) = P(X)\ [k] = X^p - c$, $c = pv^{p-1}$ [k] ou $p*p^\beta u^{p-1}$ [k] .
Soit q^γ un facteur premier de c, alors $1 < q^\gamma < k < p$, $\gamma < p$ et pgcd(γ,p)=1, et ainsi $R(X) = X^p - c$ est irréductible dans $Z_k[X]$.

R(X)=P(X) [k] étant irréductible dans $Z_k[X]$, P(X) est irréductible dans Z[X] et, par suite, n'admet pas de racines entières .
Ainsi, l'équation $x^p + y^p - z^p = 0$ n'admet pas de solutions entières non nulles pour tout p premier impair .

<<<>>>

Théorèmes utilisés :

*Petit théorème de Fermat : $x^p \equiv x$ [p], x et p des entiers et p premier.
*La réduction modulo p et l'irréductibilité :
Soit le polynôme $P(X) \in Z[X]$, si le polynôme R(X)=P(X)[p], p étant un premier et pgcd(p,a_n)=1, est irréductible dans $Z_p[X]$ alors P(X) est irréductible dans Z[X] .
*Le critère d'irréductibilité d'Eisenstein généralisé :
Soit P(X) le polynôme de coefficients entiers :
$P(X)=a_nX^n + a_{n-1}X^{n-1} + \ldots\ldots + a_1X + a_0$.
S'il existe un nombre premier p et un entier k positif tels que :
- p ne divise pas a_n , $a_na_0 \neq 0$
- p^k divise a_{n-1} , a_{n-2} , ……. a_1 , a_0 ,
- p^{k+1} ne divise pas a_0 ,
- pgcd(k,n)=1 ,

alors le polynôme P(X) est irréductible .

<<<>>>

Dans l'équation $x^p+y^p-z^p=0$, où x, y, z, p sont des entiers positifs et p est un nombre premier impair, on peut supposer, sans perte de généralité, z>y>x et x, y, z premiers entre eux .
En posant m = x+y-z, on obtient :
$x = (x+y-z)+z-y = m+u$, $u=z-y$,
$y = (x+y-z)+z-x = m+v$, $v=z-x$,
$z = (x+y-z)+(z-y)+(z-x) = m+u+v = m+w$, $w=u+v$,
$0 = x^p + y^p - z^p \equiv x+y-z = m \ [p]$.
m = x+y-z étant divisible par p, soit p^α un facteur premier de m .

En posant x=m+u, y=m+v et z=m+w dans l'équation
(5) $x^p + y^p - z^p = 0$,
en supposant u et v (w=u+v) donnés, on obtient l'équation d'indéterminée m :
(6) $(m+u)^p + (m+v)^p - (m+w)^p = 0$
L'équation (6) peut s'écrire :
(7) $(m+u)^p - ((m+w)^p - (m+v)^p) = (m+u)^p - u(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+v)^{i-1}) = 0$.
L'équation (7) montre que si k premier divise u alors k divise m+u et, par suite, k divise m et pgcd(u,v)=1 puisque pgcd(x=m+u,y=m+v)=1 .
Supposons pgcd(u,p)=1 et soit k un nombre premier quelconque tel que k divise u, donc k divise m, on a :
(8) $(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+v)^{i-1}) \equiv \sum_{i=1}^{p} v^{p-i} v^{i-1} \equiv pv^{p-1} \ [k]$.

Comme pgcd(u,pv)=1, les facteurs u et $(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+v)^{i-1})$, de produit égal à $(m+u)^p$, sont premiers entre eux et, par suite, chacun d'eux est une puissance pième .
Donc u est de la forme $u = u_0^p$ et, par symétrie, si pgcd(v,p)=1 v est de la forme $v = v_0^p$, sinon v est de la forme $v = p^\beta v_0^p$.
Pour v, on a l'équation symétrique à (7) :
(7)' $(m+v)^p - v(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+u)^{i-1}) = 0$.

$u=u_0^p$ étant un facteur premier de $(m+u)^p=(m+u_0^p)^p$, m est de la forme $m=m_0u_0$.
En posant $m = m_0u_0$ et $u = u_0^p$ dans l'équation
(11) $(m+u)^p - u(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+v)^{i-1}) = 0$, on obtient
$(m_0u_0+ u_0^p)^p - u_0^p (\sum_{i=1}^{p} (m_0u_0+ u_0^p +v)^{p-i} (m_0u_0+v)^{i-1}) = 0$
et après division par u_0^p (pivot) :
(12) $(m_0+ u_0^{p-1})^p - \sum_{i=1}^{p} (m_0u_0+ u_0^p +v)^{p-i} (m_0u_0+v)^{i-1} = 0$.
Pour v, on a l'équation :
(12)' $(m_1+ v_0^{p-1})^p - p^\beta \sum_{i=1}^{p} (m_1v_0+ v_0^p +u)^{p-i} (m_1v_0+u)^{i-1} = 0$. ($\beta \geq 0$)

Soit P(X) le polynôme associé à l'équation (12) développée en une somme de monômes et d'indéterminée m_0 .
Toute racine entière de P(X) est une solution de (12) d'indéterminée m_0 .

HYPOTHESE :
On suppose l'existence de k un nombre premier facteur de u_0 tel que k<p et $p*v^{p-1}[k]>1$ ou facteur de v_0 tel que k<p et $p*p^{\beta}\,u^{p-1}[k]>1$, $\beta\geq 0$.
Si pour tout k premier tel que $k|u_0v_0$ on a k>p alors on suppose l'existence de k facteur de u_0 tel que $p*v^{p-1}[k]>1$ ou facteur de v_0 tel que $p*p^{\beta}\,u^{p-1}[k]>1$.
Et pour $c = p*v^{p-1}[k]$ ou $p*p^{\beta}\,u^{p-1}[k]$, on a q^{γ} un facteur premier de c tel que pgcd(γ,p)=1 .
Cette hypothèse de travail est à valider par des études approfondies .
Ce problème ne semble pas avoir été abordé par les spécialistes en la matière .

La réduction modulo k appliquée au polynôme P(X) donne :
pour le pivot u_0 (u>1) :
(13) $R(X) = P(X)\,[k] = X^p - \sum_{i=1}^{p} v^{p-i}\,v^{i-1} = X^p - p*v^{p-1}[k] = X^p - a$,
ou pour le pivot v_0 :
(13)' $R(X) = P(X)\,[k] = X^p - p^{\beta}\sum_{i=1}^{p} u^{p-i}\,u^{i-1} = X^p - p*p^{\beta}\,u^{p-1}[k] = X^p - b$; $\beta_i \geq 0$.

Soit c le résidu a ou le résidu b, on a :
(14) $R(X) = P(X)\,[k] = X^p - c$.

Soit q un nombre premier tel que q^{γ} est un facteur premier de c, alors, par hypothèse de travail, $q^{\gamma}<c<k<p$ et,par suite, pgcd(γ,p)=1 ou, si k>p, pgcd(γ,p)=1.

Application du critère d'irréductibilité d'Eisenstein :

Le polynôme $R(X) = X^p - c$ est irréductible dans $Z_k[X]$.
Car il remplit les conditions du critère d'irréductibilité d'Eisenstein généralisé :
q est un nombre premier, pgcd(γ,p)=1 et $q^{\gamma}|c$.

Le polynôme R(X)=P(X) [k] étant irréductible dans $Z_k[X]$, le polynôme P(X) est irréductible dans Z[X] et, par suite, n'admet pas de racines entières .

Ainsi, l'égalité $z^p = x^p + y^p$, où x, y, z et p sont des nombres entiers, est impossible pour tout p premier impair .

Ahmed Idrissi Bouyahyaoui INPI
ahmed.idrissi@laposte.net