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 .

<<<>>>

Démonstration utilisant le critère d'irréductibilité d'Eisenstein pour n=p un nombre 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 pgcd(u,pv)=1, $u=u_0^p$, $v=p^\beta v_0^p$ ($\beta \geq 0$ and pgcd(v_0,p)=1), $m=m'p^\alpha$ ($\alpha \geq 1$ and pgcd(m',p)=1), $m=m_0u_0$ (pgcd(m_0,u_0)=1), $m=m_1v_0$ (pgcd(m_1,v_0)=1) .

After dividing equation (2) by $u=u_0^p$ (u>1), 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$|u_0$ gives :

(4) $R(X) = P(X)\ [k] = X^p - pv^{p-1}$

If gcd(v,p)=1 then $R(X) = X^p - pv^{p-1}$ is irreducible

else $p^{\alpha p} = p*p^\beta$, $R(X)= X^p - p(p^\beta v_0^p)^{p-1} = X^p - p^{(\alpha p-1)(p-1)+1}v_0^{p(p-1)}$ is irreducible .

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

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

<<<>>>

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, $u=u_0^p$, $v=p^\beta v_0^p$ ($\beta \geq 0$ et pgcd(v_0,p)=1), $m=m'p^\alpha$ ($\alpha \geq 1$ et pgcd(m',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 $u=u_0^p$ (u>1), 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 donne :

(4) $R(X) = P(X)\ [k] = X^p - pv^{p-1}$

Si pgcd(v,p)=1 alors $R(X) = X^p - pv^{p-1}$ est irréductible
sinon $p^{\alpha p} = p*p^\beta$, $R(X)= X^p - p(p^\beta v_0^p)^{p-1} = X^p - p^{(\alpha p-1)(p-1)+1} v_0^{p(p-1)}$ est irréductible .
R(X)=P(X) [k] étant irréductible, P(X) est irréductible 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 un nombre premier impair .

<<<>>>

Théorèmes utilisés :

*Petit théorème de Fermat : $x^p \equiv x$ [p], x et p des entiers et p premier.

*La réduction modulo k et l'irréductibilité :
Soit P(X) un polynôme de coefficients entiers, si le polynôme R(X)=P(X) [k], k étant un premier, est irréductible alors le polynôme P(X) est irréductible .

*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^k ne divise pas a_n ,
- 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 $x^n+y^n-z^n=0$, où x, y, z, n sont des entiers positifs et n>2, on peut supposer z>y>x et, sans perte de généralité, n est un nombre premier impair ou égal à 4 et x, y, z sont premiers entre eux .
Dans la suite, c'est le cas n= p un nombre premier impair qui est traité .

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 est 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) $(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+v)^{i-1}) \equiv \sum_{i=1}^{p} v^{p-i} v^{i-1} \equiv p\, v^{p-1}$ [k] .

Comme pgcd(u,pv)=1, les facteurs u et $(\sum_{i=1}^{n} (m+u+v)^{n-i} (m+v)^{i-1})$, 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)' $(m+v)^p - v(\sum_{i=1}^{p} (m+u+v)^{p-i} (m+u)^{i-1}) = 0$.

Evaluation de β dans le cas où $v = p^\beta v_0^{\,p}$:

Comme par hypothèse $x^p+y^p-z^p=0$ avec pgcd(x,y,z)=1 et $v = z-x = p^\beta v_0^{\,p}$ avec β≥1 , on a : $z=x+ p^\beta v_0^{\,p}$,
$z^p=y^p+x^p=(x+ p^\beta v_0^{\,p})^p= x^p + p*p^\beta v_0^{\,p} x^{p-1}+C_p^{\,2}(p^\beta v_0^{\,p})^2 x^{p-2}+ \ldots. +(p^\beta v_0^{\,p})^p$,
$y^p = p*p^\beta v_0^{\,p} x^{p-1}+((p-1)/2)p(p^\beta v_0^{\,p})^2 x^{p-2}+ \ldots. +(p^\beta v_0^{\,p})^p$.
Comme p est premier, les coefficients du binôme $C_p^{\,i}$ sont divisibles par p pour i=1, 2, ….. , p-1 et l'on a la mise en facteur de $p*p^\beta v_0^{\,p}$:
(9) $y^p = (m+v)^p = p*p^\beta v_0^{\,p} [x^{p-1}+((p-1)/2)(p^\beta v_0^{\,p}) x^{p-2}+ \ldots. +(1/p)(p^\beta v_0^{\,p})^{p-1}]$. (p≥3)
Comme pgcd(x=m+u,p)=1, p ne divise pas le facteur $[x^{p-1}+(p-1)/2 *(p^\beta v_0^{\,p}) x^{p-2}+\ldots]$ et, par suite, p^α étant un facteur premier de m, on a :
$(m' p^\alpha + p^\beta v_0^{\,p})^p = p*p^\beta v_0^{\,p} [x^{p-1}+((p-1)/2)(p^\beta v_0^{\,p}) x^{p-2}+\ldots.+(1/p)(p^\beta v_0^{\,p})^{p-1}]$ et, comme le facteur $p*p^\beta$ ne peut être égal à $p^{\beta p}$ puisque β≥1 et p≥3, $p*p^\beta = p^{\alpha p}$, β=αp-1 et
(10) $v = p^{\alpha p-1} v_0^{\,p}$.

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

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 .
La réduction modulo k premier|u_0 appliquée à ce polynôme donne :
(13) $R(X) = P(X)\ [k] = X^p - \sum_{i=1}^{p} v^{p-i} v^{i-1} = X^p - p*v^{p-1}$.

Application du critère d'irréductibilité d'Eisenstein :

a) pgcd(v,p)=1, $v= v_0^p$, $R(X) = X^p - p*v^{p-1}$ est irréductible .
Si u=1, on prend l'équation (7)' avec v_0^p comme pivot, d'où
$R(X) = X^p - p*u^{p-1} = X^p - p$ est irréductible .

b) pgcd(v,p)=p, $v= p^{\alpha p-1}v_0^p$, pgcd(v_0,p)=1 et u>1 .
$R(X) = X^p - p*v^{(p-1)} = X^p - p(p^{\alpha p-1} v_0^p)^{p-1} = X^p - p^{(\alpha p-1)(p-1)+1}*v_0^{p(p-1)}$.
Comme pgcd((αp-1)(p-1)+1,p)=1, R(X) est irréductible .

c) pgcd(v,p)=p, $v= p^{\alpha p-1}v_0^p$, pgcd(v_0,p)=1 et u=z-y=1 .
En posant z=y+1, x=y-v+1=y+(1-v) dans l'équation $z^P = x^P + y^P$, on obtient :
$(y+1)^P = (y+(1-v))^P + y^P = y^P + \sum_{i=1}^{p} C_p^i((1-v)^i - 1)*y^{P-I} = 0$,
équation d'indéterminée y et de polynôme associé :
$P(Y) = Y^P + \sum_{i=1}^{p} C_p^i((1-v)^i - 1)*Y^{P-I}$.
Comme p|v, v≥p>2 et pgcd(1-v,p)=1, soit k premier|1-v, k≠p et k ne divise pas tous les C_p^i pour i=1,2, …. ,p-1 .
L'application de la réduction modulo k au polynôme P(Y) donne :
$R(Y) = P(Y)\ [k] = Y^P - \sum_{i=1}^{p} C_p^i*Y^{P-I} = 2*Y^P - (Y+1)^P$
et après changement de variable en posant Y=X – 1 :
$R(X) = 2(X-1)^P - X^P = X^P - 2\sum_{i=1}^{p} C_p^i (-1)^{i-1}*X^{p-I}$ est irréductible .

Le polynôme R(X) = P(X) [k] étant irréductible, le polynôme P(X) est irréductible 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 entiers, est impossible pour tout p un nombre premier impair .

Ahmed Idrissi Bouyahyaoui INPI
ahmed.idrissi@laposte.net