

L'irréductibilité de polynômes et le théorème de Fermat-Wiles.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere : cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

Démonstration du Théorème de Fermat-Wiles par l'irréductibilité de polynômes.

Résumé :

Etant donnée l'équation de Fermat $x^n + y^n - z^n = 0$, où $(x, y, z, n) \in \mathbb{N}^{*4}$, $n > 2$ et p premier > 2 , le polynôme $P(X)$ associé à l'équation $x^p + y^p - z^p = 0$ et le polynôme $Q(X)$ associé à l'équation $x^4 + y^4 - z^4 = 0$ n'ont pas de racines entières et, par conséquent, la marge $m = x + y - z$ n'est pas un entier, ce qui est contradictoire.

Et par suite, l'égalité $z^n = x^n + y^n$, où $(x, y, z, n) \in \mathbb{N}^{*4}$ et $n > 2$, est impossible.

Preuve :

Théorèmes de référence :

Th. 1 - : Soit $P(X) \in \mathbb{Z}[X]$. Si $P(X) = 0$ admet une racine $X \in \mathbb{Z}$ alors $P(X) \equiv 0 [p]$ admet des solutions quelque soit p premier.

Ce théorème a pour contraposée : Soit $P(X) \in \mathbb{Z}[X]$. Si $P(X) \equiv 0 [p]$, p premier, n'admet aucune solution entière alors $P(X) = 0$ n'admet aucune racine $X \in \mathbb{Z}$.

Th. 2 - : Soit $P(X) \in \mathbb{Z}[X]$. Si $P(X) [p]$, p premier, est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Th. 3 - : Soit $P(X) \in \mathbb{Z}[X]$ et $a \in \mathbb{Q}$ alors $P(X)$ est irréductible dans $\mathbb{Q}[X]$ si et seulement si le polynôme $P(X+a)$ est irréductible dans $\mathbb{Q}[X]$.

Soit l'équation $x^n + y^n - z^n = 0$, où $(x, y, z, n) \in \mathbb{N}^{*4}$ et $n > 2$.

En posant $m = x + y - z$, on peut écrire :

$$x = (x+y-z)+z-y = m+u, \text{ avec } u=z-y$$

$$y = (x+y-z)+z-x = m+v, \text{ avec } v=z-x$$

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

Remarques :

- m est indépendant de u, v, w puisque $w=u+v$ et $m= x+y-z$.

- Dans une équation m est une variable entière et dans une égalité m est un nombre entier. Dans tous les cas, u, v, w et n sont des constantes entières.

- Les polynômes examinés sont unitaires et, par conséquence, primitifs.

En posant $x=m+u$, $y=m+v$ et $z=m+w$ dans $x^n+y^n-z^n=0$, on obtient l'équation:

$$(1) \quad (m+u)^n + (m+v)^n - (m+w)^n = 0, \text{ avec } w=u+v.$$

Equation polynômiale de second membre nul et qui a pour indéterminée m, indépendante des constantes entières u, v et w puisque $w=u+v$ et $m=x+y-z$, et pour degré un entier $n > 2$.

Soit $P(M) = (M+u)^n + (M+v)^n - (M+w)^n$, le polynôme associé à l'équation (1), les racines de (1) sont aussi des racines de $P(M)=0$.

Si le polynôme $P(M)$ de degré n n'admet pas de racines entières, alors l'équation (1) n'admet pas de racines entières non plus.

Puisque $n > 2$, n est multiple de 4 ou d'un nombre premier $p > 2$, il suffit de considérer le cas $n=p$ et le cas $n=4$.

A – L'équation (1) n'a pas de racines entières :

Pour $n=p$, l'équation (1) peut s'écrire :

$$(2) \quad ((m-2)+(u+2))^p + ((m-2)+(v+2))^p - ((m-2)+(w+2))^p = 0, \text{ avec } w=u+v.$$

Soit $P(X)$ le polynôme associé à (2) :

$$(3) \quad P(X) = (X+(u+2))^p + (X+(v+2))^p - (X+(w+2))^p,$$

avec $X=m-2$ (changement de variable par translation).

L'application de la réduction modulo p à $P(X)$, avec $u^p+v^p-w^p \equiv u+v-w=0 \pmod{p}$ et $2^p \equiv 2 \pmod{p}$, donne : $P(X) \pmod{p} = X^p+2$.

Puisque le nombre $2^{1/p}$ est irrationnel, le polynôme $P(X) \pmod{p}$ n'a pas de racines entières et, par suite, $P(X)$ n'a pas de racines entières et, par équivalence, l'équation (2) n'a pas de solutions entières pour m , ce qui est contradictoire.

Et par suite, l'égalité $x^p + y^p - z^p = 0$, où $(x,y,z) \in \mathbb{N}^{*3}$ et p premier >2 , est impossible.

Pour $n=4$, l'équation (1) peut s'écrire :

$$(4) \quad ((m-1)+(u+1))^4 + ((m-1)+(v+1))^4 - ((m-1)+(w+1))^4 = 0, \text{ avec } w=u+v.$$

Soit $P(X)$ le polynôme associé à (4) :

$$(5) \quad P(X) = (X+(u+1))^4 + (X+(v+1))^4 - (X+(w+1))^4, \text{ avec } X=m-1.$$

L'application de la réduction modulo 2 à $P(X)$, avec $w^4-u^4-v^4 \equiv w-u-v=0 \pmod{2}$, donne : $P(X) \pmod{2} = X^4+1$, polynôme qui, par le changement de variable $Y=X^2$, devient le polynôme équivalent : $Q(Y)=Y^2+1$, polynôme de degré 2 et de discriminant négatif. Donc il n'a pas de racines entières, et par suite le polynôme $P(X)$ n'a pas de racines entières et, par équivalence, l'équation (4) n'a pas de solutions entières pour m , ce qui est contradictoire.

Et par suite, l'égalité $x^4 + y^4 - z^4 = 0$, où $(x,y,z) \in \mathbb{N}^{*3}$, est impossible.

B – Le polynôme associé à l'équation (1) est irréductible :

Pour $n=p$, le polynôme $P(X) \pmod{p} = X^p+2$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ (critère d'irréductibilité d'Eisenstein) et par suite $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Pour $n=4$, l'équation (1) peut s'écrire :

$$(4) \quad ((m'-4)+(u'+4))^4 + ((m'-4)+(v'+4))^4 - ((m'-4)+(w'+4))^4 = 0, \text{ avec } w'=u'+v',$$

où $u'=5u$, $v'=5v$, $w'=5w$, $m'=5m$.

Soit $P(X)$ le polynôme associé à (4) :

$$(5) \quad P(X)=(X+(u'+4))^4+(X+(v'+4))^4-(X+(w'+4))^4, \text{ avec } w'=u'+v' \text{ et } X=m'-4.$$

Comme $u \equiv 0, v \equiv 0, w \equiv 0 \pmod{5}$ implique $u^k \equiv 0, v^k \equiv 0, w^k \equiv 0 \pmod{5}$ et, en général, $4 \not\equiv 4^k \pmod{5}$, on a les réductions à partir de (5):

$$P(X) \equiv (X+4)^4 + (X+4)^4 - (X+4)^4 = (X+4)^4 \pmod{5}$$

$$P(X) \equiv X^4 + (4^2)X^3 + 6(4^2)X^2 + (4^4)X + 4^4 \pmod{5}$$

Et finalement, on obtient :

$$(6) \quad Q(X) = P(X) \pmod{5} = X^4 + X^3 + X^2 + X + 1$$

Le polynôme $Q(X)$, étant un polynôme cyclotomique, est irréductible dans $\mathbb{Z}/5\mathbb{Z}[X]$ et, par suite, le polynôme $P(X)$ est irréductible dans $\mathbb{Z}[X]$.

Remarque :

Comme $Q(0)$ et $Q(1)$ sont des nombres impairs, $Q(X)$ n'a pas de racines entières et, par suite, $P(X)$ n'a pas de racines entières et, par équivalence, l'équation (4) n'a pas de solutions entières pour m , ce qui est contradictoire.

Ainsi, l'égalité $z^n = x^n + y^n$, où $(x, y, z, n) \in \mathbb{N}^{*4}$ et $n > 2$, est impossible.

Ahmed Idrissi Bouyahyaoui

Inpi - Paris