

A la recherche de la démonstration de FERMAT

Search for Fermat's proof

Abstract :

Let $P_n(x)$ the associated polynomial to the equation $X^n + Y^n = Z^n$.

$P_n(x) = (x+u)^n + (x+v)^n - (x+w)^n$, $x = X+Y-Z$, $X = x+Z-Y = x+u$, $Y = x+Z-X = x+v$, $Z = X+Y-x = x+w$,
 $u, v, w = u+v$ and $n \in \mathbb{N}^*$, $n > 2$; $nP_{n-1}(x) = P_n'(x)$, $(n+1)P_n(x) = P_{n+1}'(x)$.

$n \pm 1 \in \mathbb{Z}$ [4], $P_{n \pm 1}(a) = 0$: a is the single positive root (Descartes' rule of signs).

$n \pm 1 \in \mathbb{Z}$ [4], $P_{n \pm 1}(a) = 0 \implies a$ is an irrational number (Fermat's theorem).

$uv \in \mathbb{N}^*$, $P_{n \pm 1}(a) \equiv a^2 - 2uv = 0$ [3] $\implies a^2$ is a rational number.

a^2 is a rational number $\implies P_{n \pm 1}(a) = A + Ba \neq 0$, $B \neq 0$, $(0 \neq 0) = \text{False}$.

By contraposition :

$n \pm 1 \in \mathbb{Z}$ [4], $P_{n \pm 1}(a) = 0 \implies a^2$ and $uv = (Z-Y)(Z-X)$ are irrational numbers.

uv is an irrational number \implies the equality $P_n(m) = (m+u)^n + (m+v)^n - (m+w)^n = 0$,
 with $m, u, v, w = u+v$ and n positive integers, is impossible for $n > 2$.

Résumé :

Soit $P_n(x)$ le polynôme associé à l'équation $X^n + Y^n = Z^n$.

$P_n(x) = (x+u)^n + (x+v)^n - (x+w)^n$, $x = X+Y-Z$, $X = x+Z-Y = x+u$, $Y = x+Z-X = x+v$, $Z = X+Y-x = x+w$,
 $u, v, w = u+v$ et $n \in \mathbb{N}^*$, $n > 2$; $nP_{n-1}(x) = P_n'(x)$, $(n+1)P_n(x) = P_{n+1}'(x)$.

$n \pm 1 \in \mathbb{Z}$ [4], $P_{n \pm 1}(a) = 0$: a est l'unique racine positive
 (règle des signes de Descartes).

$n \pm 1 \in \mathbb{Z}$ [4], $P_{n \pm 1}(a) = 0 \implies a$ est un nombre irrationnel (théorème de Fermat).

$uv \in \mathbb{N}^*$, $P_{n \pm 1}(a) \equiv a^2 - 2uv = 0$ [3] $\implies a^2$ est un nombre rationnel.

a^2 est un nombre rationnel $\implies P_{n \pm 1}(a) = A + Ba \neq 0$, $B \neq 0$, $(0 \neq 0) = \text{Faux}$.

Par contraposition :

$n \pm 1 \in \mathbb{Z}$ [4], $P_{n \pm 1}(a) = 0 \implies a^2$ et $uv = (Z-Y)(Z-X)$ sont des nombres irrationnels.

uv est un nombre irrationnel \implies l'égalité $P_n(m) = (m+u)^n + (m+v)^n - (m+w)^n = 0$,
 où $m, u, v, w = u+v$ et n sont des entiers positifs, est impossible pour $n > 2$.

A la recherche de la démonstration de FERMAT

$$X^n + Y^n \neq Z^n, n > 2$$

Théorème de Fermat-Wiles :

L'équation $X^n + Y^n = Z^n$, où X, Y, Z, n sont des entiers positifs, n'a pas de solution pour $n > 2$.

Fermat a formulé par écrit la preuve pour $n=4$ et affirmé avoir découvert celle du cas général.

La preuve, présentée dans cet article, s'appuie sur celle donnée pour $n=4$.

Démonstration :

En posant $x = X + Y - Z$ ($x > 0$), on a $X = x + Z - Y = x + u$, $Y = x + Z - X = x + v$, $Z = X + Y - x = x + w$, $w = u + v$; u et v sont des entiers positifs.

Par substitution dans l'équation $X^n + Y^n = Z^n$, on obtient le polynôme associé :
 $P_n(x) = (x+u)^n + (x+v)^n - (x+w)^n$.

Les nombres u et v sont communs aux polynômes $P_{n-1}(x)$, $P_n(x)$ et $P_{n+1}(x)$ puisque $nP_{n-1}(x) = P_n'(x)$, $(n+1)P_n(x) = P_{n+1}'(x)$.

Pour tout $n > 2$, on a $n \in \mathbb{O} [4]$, et le problème est résolu par le théorème de Fermat, ou $n \pm 1 \in \mathbb{O} [4]$ ou $n = 2k$ avec k un nombre impair et l'on a $k \pm 1 \in \mathbb{O} [4]$ et n retenu est toujours impair.

Le polynôme $P_{n \pm 1}(x)$ possède une seule racine positive (règle des signes de Descartes).

Soit a cette racine.

Pour $n \pm 1 \in \mathbb{O} [4]$, $P_{n \pm 1}(a) = (a+u)^{n \pm 1} + (a+v)^{n \pm 1} - (a+w)^{n \pm 1} = 0$ et, d'une part, a est un irrationnel d'après le théorème de Fermat car $n \pm 1 \in \mathbb{O} [4]$, et d'autre part, $0 = P_{n \pm 1}(a) = (a+u)^{n \pm 1} + (a+v)^{n \pm 1} - (a+w)^{n \pm 1} \equiv (a+u)^2 + (a+v)^2 - (a+w)^2 [3]$.

Ce qui donne $P_{n \pm 1}(a) \equiv a^2 - 2uv = 0 [3]$.

Par hypothèse uv étant un entier, a^2 est alors un rationnel.

Le développement de l'égalité $P_{n\pm 1}(a) = (a+u)^{n\pm 1} + (a+v)^{n\pm 1} - (a+w)^{n\pm 1} = 0$ donne :

$$0 = P_{n\pm 1}(a) = \sum_{i=0}^{n\pm 1} C_{n\pm 1}^i (u^i + v^i - w^i) a^{n\pm 1-i} \quad \text{où } w = u+v, \quad u^i + v^i - w^i < 0 \text{ pour } i > 1.$$

Si a^2 est un rationnel alors $P_{n\pm 1}(a)$ est de la forme $A + Ba$ où A et B sont des rationnels avec $B \neq 0$.

Comme a est un irrationnel, $P_{n\pm 1}(a) = A + Ba \neq 0$, ce qui implique $(0 \neq 0) = \text{Faux}$.

Donc, par contraposition, a^2 est un irrationnel et le produit $uv = (Z-Y)(Z-X)$ l'est aussi puisque $a^2 - 2uv = 0$ [3], et par suite, l'égalité

$$P_n(m) = (m+u)^n + (m+v)^n - (m+w)^n = 0,$$

où $m, u, v, w = u+v$ et n sont des entiers positifs, est impossible pour $n > 2$.

Ahmed Idrissi Bouyahyaoui

ahmed.idrissi@laposte.net