

Une demonstration du theoreme de Fermat-Wiles

Jamel Ghanouchi
e-mail:ghanouchi.jamel@planet.tn

Resume

(MSC=11) Le theoreme est le suivant

$$\forall U > 0, X > 0, Y > 0, n > 2, PGCD(X, Y) = 1$$

entiers

$$U^n \neq X^n + Y^n$$

La presente demonstration commence par un changement dans les donnees du probleme. Au lieu d'une seule equation, la traditionnelle $X > 0, Y > 0, U > 0, n > 2, PGCD(X, Y) = 1$ entiers

$$X^n = U^n - Y^n$$

qui est (a), nous en definissons deux autres, equivalentes

$$x = u - y$$

qui est (1) et

$$\frac{1}{z} = \frac{1}{x} + \frac{1}{y}$$

qui est (2). x, y, z, u entiers. Ce qui permet de construire des suites convergentes. Nous les etudions rapidement. Un calcul de convergence de series permet de conclure qu'il n'y a pas de solution.

La demonstration

Notre but est de prouver que si $U > 0, X > 0, Y > 0, n > 2, PGCD(X, Y) = 1$, sont des entiers, ils ne verifient jamais l'equation qui suit (a)

$$X^n = U^n - Y^n$$

Notre demonstration s'appuie sur un raisonnement par l'absurde. Nous supposons que

$$\exists U > 0, X > 0, Y > 0, n > 2$$

entiers et que $PGCD(X, Y) = 1$, et qu'ils verifient (a). Si nous choisissons u, x, y, z entiers comme suit. Soit

$$u = U^{2n}$$

$$x = U^n X^n$$

$$y = U^n Y^n$$

$$z = X^n Y^n$$

alors,

$$u = U^{2n} = U^n(X^n + Y^n) = x + y$$

c'est (1) et

$$\frac{1}{z} = \frac{1}{X^n Y^n} = \frac{U^{2n}}{U^n X^n U^n Y^n} = \frac{u}{xy} = \frac{x+y}{xy} = \frac{1}{x} + \frac{1}{y}$$

c'est (2). Si U, X, Y sont des entiers verifiant (a), alors u, x, y, z comme definis plus haut verifient simultanement (1) et (2) qui suivent

LEMME 1 (1)

$$u = x + y$$

et (2)

$$\frac{1}{z} = \frac{1}{x} + \frac{1}{y}$$

Fin du lemme 1 Donc

$$z = X^n Y^n$$

$$u = (X^n + Y^n)^2$$

$$x = X^n(X^n + Y^n)$$

$$y = Y^n(X^n + Y^n)$$

Maintenant, nous savons qu'il existe des solutions pour $n \leq 2$, nous supposerons donc dans ce qui suit : $n > 2$. Posons

$$x_1 = x$$

et

$$y_1 = y$$

$\forall x_1, y_1$ entier, $\exists z_1$ verifiant

$$\frac{1}{z_1} = \frac{1}{x_1} + \frac{1}{y_1}$$

et

$$z_1 = \frac{xy}{x+y} = z$$

et

$$(x_1 + y_1)z_1 = x_1y_1$$

soit

$$x_1(y_1 - z_1) = z_1y_1$$

posons

$$y_2 = y_1 - z_1 = \frac{z_1y_1}{x_1}$$

et

$$y_1(x_1 - z_1) = z_1x_1$$

posons

$$x_2 = x_1 - z_1 = \frac{z_1x_1}{y_1}$$

et

$$x_2y_2 = z_1^2$$

alors

$$x_1 = x_2 + z_1 = x_2 + \sqrt{x_2y_2}$$

et

$$y_1 = y_2 + z_1 = y_2 + \sqrt{x_2y_2}$$

et

$$u_1 = u = (x_1 + y_1) = (\sqrt{x_2} + \sqrt{y_2})^2 > x_2 + y_2 > 1$$

$(x_1 + y_1)$ entier

$$x_1 = \sqrt{x_2}(\sqrt{x_2} + \sqrt{y_2}) > x_2 > 0$$

x_1 entier

$$y_1 = \sqrt{y_2}(\sqrt{x_2} + \sqrt{y_2}) > y_2 > 0$$

y_1 entier

$$z_1 = \frac{x_1 y_1}{x_1 + y_1} = X^a Y^b = \sqrt{x_2 y_2} > z_2 = \frac{x_2 y_2}{x_2 + y_2} > 0$$

z_2 rationnel

car

$\forall x_2, y_2$ entiers, $\exists z_2$ rationnel verifiant l'equation suivante

$$\frac{1}{z_2} = \frac{1}{x_2} + \frac{1}{y_2}$$

jusqu'a l'infini. A l'ordre i

$$(x_i + y_i) = (\sqrt{x_{i+1}} + \sqrt{y_{i+1}})^2 > x_{i+1} + y_{i+1} > 1$$

et $x_i + y_i$ rationnel pour $i > 2$

$$x_i = \sqrt{x_{i+1}}(\sqrt{x_{i+1}} + \sqrt{y_{i+1}}) > x_{i+1} > 0$$

x_i rationnel pour $i > 2$

$$y_i = \sqrt{y_{i+1}}(\sqrt{x_{i+1}} + \sqrt{y_{i+1}}) > y_{i+1} > 0$$

y_i rationnel pour $i > 2$

$$z_i = \frac{x_i y_i}{x_i + y_i} = \sqrt{x_{i+1} y_{i+1}} > z_{i+1} = \frac{x_{i+1} y_{i+1}}{x_{i+1} + y_{i+1}} > 0$$

z_i rationnel pour $i > 1$ et

$$\frac{1}{z_{i+1}} = \frac{1}{x_{i+1}} + \frac{1}{y_{i+1}}$$

avec cette recurrence

$$(x_i + y_i) = (\sqrt{x_{i+1}} + \sqrt{y_{i+1}})^2$$

LEMME 2 x_i et y_i ont pour expression

$$x_i = x^{2^{i-1}} \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})^{-1}$$

qui est (H)

$$y_i = y^{2^{i-1}} \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})^{-1}$$

qui est (H')

Fin du lemme 2

Preuve du lemme 2 nous allons prouver le lemme 2 comme suit

$$x = \sqrt{x_2}(\sqrt{x_2} + \sqrt{y_2}) = \sqrt{x_2}(x + y)^{\frac{1}{2}}$$

$$x_2 = \frac{x^2}{x + y}$$

de meme

$$y_2 = \frac{y^2}{x + y}$$

c'est verifie pour $i = 2$. Nous supposons (H) et (H') vraies a l'ordre i et nous en deduirons qu'elles sont vraies a l'ordre $i + 1$

$$x_i = \sqrt{x_{i+1}}(\sqrt{x_{i+1}} + \sqrt{y_{i+1}}) = \sqrt{x_{i+1}}(x_i + y_i)^{\frac{1}{2}}$$

soit

$$x_{i+1} = x_i^2 (x_i + y_i)^{-1}$$

or (H) et (H'), donc

$$x_{i+1} = x^{2^i} \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})^{-2} (x^{2^{i-1}} + y^{2^{i-1}})^{-1} \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})$$

$$= x^{2^i} \prod_{j=0}^{j=i-1} (x^{2^j} + y^{2^j})^{-1}$$

et c'est vrai a l'ordre $i + 1$, de meme pour y_i

Fin de la preuve du lemme 2 donc

$$x_i = x^{2^{i-1}} \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})^{-1}$$

de meme pour y_i

$$y_i = y^{2^{i-1}} \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})^{-1}$$

$$\forall i > 1$$

Or, $\forall a, b$

$$a - b = (a^{2^{i-1}} - b^{2^{i-1}}) \prod_{j=0}^{j=i-2} (a^{2^j} + b^{2^j})^{-1}$$

c'est (E). Donc

$$x - y = (x^{2^{i-1}} - y^{2^{i-1}}) \prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j})^{-1}$$

c'est (E')

$$\prod_{j=0}^{j=i-2} (x^{2^j} + y^{2^j}) = \frac{(x^{2^{i-1}} - y^{2^{i-1}})}{x - y}$$

nous en concluons avec

$$x \neq y$$

donc avec

$$x_i \neq y_i$$

le lemme 3 suivant

LEMME 3

$$x_i = \frac{x^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}} (x - y) = U^n \frac{X^{n2^{i-1}}}{X^{n2^{i-1}} - Y^{n2^{i-1}}} (X^n - Y^n)$$

et

$$y_i = \frac{y^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}} (x - y) = U^n \frac{Y^{n2^{i-1}}}{X^{n2^{i-1}} - Y^{n2^{i-1}}} (X^n - Y^n)$$

$$u_i = x_i + y_i = U^n \frac{X^{n2^{i-1}} + Y^{n2^{i-1}}}{X^{n2^{i-1}} - Y^{n2^{i-1}}} (X^n - Y^n)$$

Fin du lemme 3

LEMME 4 Il y a des constantes

$$x - y = x_i - y_i$$

Fin du lemme 4 Le lemme 4 est evident. D'autre part, x_i est solution de

$$x_i^2 - x_{i+1}x_i - x_{i+1}y_i = 0$$

et y_i est solution de

$$y_i^2 - y_{i+1}y_i - y_{i+1}x_i = 0$$

LEMME 5 La solution de ces equations est

$$x_i = y_i = 2x_{i+1} = 2y_{i+1}$$

soit

$$u = x = y$$

et

$$U = X = Y = 0$$

car

$$PGCD(X, Y) = 1$$

Fin du lemme 5

Demonstration du lemme 5

$$(x_{i+1}y_i = x_i^2 - x_{i+1}x_i) \Rightarrow (x_i = \frac{x_{i+1} + \sqrt{x_{i+1}^2 + 4y_ix_{i+1}}}{2})$$

$$\Rightarrow ((y_i - y_{i+1})x_{i+1} = x_i^2 - x_{i+1}x_i - x_{i+1}y_{i+1})$$

$$= (x_i - x_{i+1})x_{i+1} = x_ix_{i+1} - x_{i+1}^2$$

$$\Rightarrow (x_i^2 - 2x_ix_{i+1} + x_{i+1}(x - y) = 0) \Rightarrow (x_i = x_{i+1} + \sqrt{x_{i+1}^2 - x_{i+1}(x - y)})$$

de meme

$$(y_{i+1}y_i = y_i^2 - y_{i+1}x_i) \Rightarrow (y_i = \frac{y_{i+1} + \sqrt{y_{i+1}^2 + 4x_iy_{i+1}}}{2})$$

$$\Rightarrow ((y_i - y_{i+1})y_{i+1} = y_i^2 - y_{i+1}x_i - y_{i+1}^2)$$

$$\begin{aligned}
&= (x_i - x_{i+1})y_{i+1} = x_i y_{i+1} - x_{i+1} y_{i+1} \\
\Rightarrow (y_i^2 - 2x_i y_{i+1} + y_{i+1}(x - y) = 0) &\Rightarrow (y_i^2 - 2y_i y_{i+1} + y_{i+1}(x - y) - 2x_i y_{i+1} + 2y_i y_{i+1}) \\
&= y_i^2 - 2y_i y_{i+1} - y_{i+1}(x - y) = 0 \Rightarrow (y_i = y_{i+1} + \sqrt{y_{i+1}^2 + y_{i+1}(x - y)})
\end{aligned}$$

donc

$$x - y = \frac{x_i(2x_{i+1} - x_i)}{x_{i+1}} = \frac{y_i(-2y_{i+1} + y_i)}{y_{i+1}}$$

donc

$$x - y = 0 \Leftrightarrow (x_i = y_i = 2x_{i+1} = 2y_{i+1})$$

or

$$\begin{aligned}
x_i - x_{i+1} &= \sqrt{x_{i+1}y_{i+1}} \\
x_{i-1} - x_i &= \sqrt{x_i y_i}
\end{aligned}$$

...

$$x_1 - x_2 = x - x_2 = \sqrt{x_2 y_2}$$

ce qui implique

$$\sum_{j=2}^{j=i+1} (\sqrt{x_j y_j}) = x - x_2 + x_2 - x_3 + \dots + x_i - x_{i+1} = x - x_{i+1}$$

donc

$$\sum_{j=2}^{j=\infty} (\sqrt{x_j y_j}) = \lim_{i \rightarrow \infty} (x - x_{i+1})$$

mais si

$$\begin{aligned}
&x > y \\
\lim_{i \rightarrow \infty} (y_i) &= \lim_{i \rightarrow \infty} \left(\frac{y^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}} (x - y) \right) = 0
\end{aligned}$$

et

$$\lim_{i \rightarrow \infty} (x_i) = \lim_{i \rightarrow \infty} \left(\frac{x^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}} (x - y) \right) = x - y$$

donc

$$\sum_{j=2}^{j=\infty} (\sqrt{x_j y_j}) = \lim_{i \rightarrow \infty} (x - x_{i+1}) = x - (x - y) = y$$

et

$$\begin{aligned}
\sqrt{x_2 y_2} &= x - x_2 \\
-\sqrt{x_3 y_3} &= x_3 - x_2 \\
\sqrt{x_4 y_4} &= x_3 - x_4
\end{aligned}$$

...

$$\begin{aligned}
\sqrt{x_{2k} y_{2k}} &= x_{2k-1} - x_{2k} \\
-\sqrt{x_{2k+1} y_{2k+1}} &= x_{2k+1} - x_{2k}
\end{aligned}$$

donc

$$\begin{aligned}
\sum_{j=2}^{j=2k+1} ((-1)^j \sqrt{x_j y_j}) &= x - 2x_2 + 2x_3 - 2x_4 + \dots + 2x_{2k-1} - 2x_{2k} + x_{2k+1} \\
&= x - 2((x_2 - x_3) + (x_4 - x_5) + \dots + (x_{2k-2} - x_{2k-1})) - 2x_{2k} + x_{2k+1} \\
&= x - 2(\sqrt{x_3 y_3} + \sqrt{x_5 y_5} + \dots + \sqrt{x_{2k-1} y_{2k-1}}) - 2x_{2k} + x_{2k+1}
\end{aligned}$$

mais

$$\sqrt{x_{2k-1} y_{2k-1}} > \sqrt{x_{2k} y_{2k}}$$

et

$$0 < \sum_{j=2}^{j=2k+1} ((-1)^j \sqrt{x_j y_j}) < x - \sqrt{x_3 y_3} - \sqrt{x_4 y_4} - \dots - \sqrt{x_{2k} y_{2k}} - \sqrt{x_{2k+1} y_{2k+1}} - x_{2k}$$

soit

$$0 < \sum_{j=2}^{j=\infty} ((-1)^j \sqrt{x_j y_j}) < x + \sqrt{x_2 y_2} - \sum_{j=2}^{j=\infty} (\sqrt{x_j y_j}) - (x - y) = \sqrt{x_2 y_2}$$

et

$$\sum_{j=2}^{j=\infty} ((-1)^j \sqrt{x_j y_j})$$

est convergente,

$$\sum_{j=2}^{j=\infty} (\sqrt{x_j y_j})$$

est convergente donc

$$y - 2 \sum_{j=2}^{j=\infty} ((-1)^j x_j) = \sum_{j=2}^{j=\infty} ((-1)^j \sqrt{x_j y_j})$$

est convergente, ce qui veut dire que

$$\sum_{j=2}^{j=\infty} ((-1)^j x_j) = S$$

$$\lim_{i \rightarrow \infty} (x_i) = S - S = 0$$

or

$$\lim_{i \rightarrow \infty} (x_i) = x - y$$

soit

$$x - y = 0 \Rightarrow (x_i = y_i = 2x_{i+1} = 2y_{i+1})$$

et si

$$x < y$$

$$\lim_{i \rightarrow \infty} (y_i) = \lim_{i \rightarrow \infty} \left(\frac{y^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}} (x - y) \right) = y - x$$

et

$$\lim_{i \rightarrow \infty} (x_i) = \lim_{i \rightarrow \infty} \left(\frac{x^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}} (x - y) \right) = 0$$

alors

$$\sum_{j=2}^{j=\infty} (\sqrt{x_j y_j}) = \lim_{i \rightarrow \infty} (x - x_{i+1}) = x$$

et

$$\begin{aligned}\sqrt{x_2 y_2} &= y - y_2 \\ -\sqrt{x_3 y_3} &= y_3 - y_2 \\ \sqrt{x_4 y_4} &= y_3 - y_4\end{aligned}$$

...

$$\begin{aligned}\sqrt{x_{2k} y_{2k}} &= y_{2k-1} - y_{2k} \\ -\sqrt{x_{2k+1} y_{2k+1}} &= y_{2k+1} - y_{2k}\end{aligned}$$

donc

$$\begin{aligned}\sum_{j=2}^{j=2k+1} ((-1)^j \sqrt{x_j y_j}) &= y - 2y_2 + 2y_3 - 2y_4 + \dots + 2y_{2k-1} - 2y_{2k} + y_{2k+1} \\ &= y - 2((y_2 - y_3) + (y_4 - y_5) + \dots + (y_{2k-2} - y_{2k-1})) - 2y_{2k} + y_{2k+1} \\ &= y - 2(\sqrt{x_3 y_3} + \sqrt{x_5 y_5} + \dots + \sqrt{x_{2k-1} y_{2k-1}}) - 2y_{2k} + y_{2k+1}\end{aligned}$$

or

$$\sqrt{x_{2k-1} y_{2k-1}} > \sqrt{x_{2k} y_{2k}}$$

et

$$0 < \sum_{j=2}^{j=2k+1} ((-1)^j \sqrt{x_j y_j}) < y - \sqrt{x_3 y_3} - \sqrt{x_4 y_4} - \dots - \sqrt{x_{2k} y_{2k}} - \sqrt{x_{2k+1} y_{2k+1}} - y_{2k}$$

soit

$$0 < \sum_{j=2}^{j=\infty} ((-1)^j \sqrt{x_j y_j}) < y + \sqrt{x_2 y_2} - \sum_{j=2}^{j=\infty} (\sqrt{x_j y_j}) - (y - x) = \sqrt{x_2 y_2}$$

et

$$\sum_{j=2}^{j=\infty} ((-1)^j \sqrt{x_j y_j})$$

est convergente,

$$\sum_{j=2}^{j=\infty} (\sqrt{x_j y_j})$$

est convergente donc

$$x - 2 \sum_{j=2}^{j=\infty} ((-1)^j y_j) = \sum_{j=2}^{j=\infty} ((-1)^j \sqrt{x_j y_j})$$

est convergente, ce qui signifie que

$$\begin{aligned}\sum_{j=2}^{j=\infty} ((-1)^j y_j) &= S' \\ \lim_{i \rightarrow \infty} (y_i) &= S' - S' = 0\end{aligned}$$

mais

$$\lim_{i \rightarrow \infty} (y_i) = y - x$$

donc

$$y - x = 0 \Rightarrow (x_i = y_i = 2x_{i+1} = 2y_{i+1})$$

Fin de la demonstration du lemme 5 Le lemme 5 est demontre et, par suite, le theoreme est demontre ! La question qui se pose maintenant est : pourquoi $n = 2$ est-il un cas particulier ? Pour repondre, nous utiliserons les formules. D'abord, il est important de noter que pour $n = 1$, il y a trivialement une infinite de solutions. Or, pour $n = 1$, nous avons le le LEMME 3

$$\begin{aligned} x_i &= \frac{x^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}}(x - y) = U \frac{X^{2^{i-1}}}{X^{2^{i-1}} - Y^{2^{i-1}}}(X - Y) \\ &= U \frac{X^{2^{2^{i-2}}}}{X^{2^{2^{i-2}}} - Y^{2^{2^{i-2}}}}(X - Y) \end{aligned}$$

et

$$\begin{aligned} y_i &= \frac{y^{2^{i-1}}}{x^{2^{i-1}} - y^{2^{i-1}}}(x - y) = U \frac{Y^{2^{i-1}}}{X^{2^{i-1}} - Y^{2^{i-1}}}(X - Y) \\ &= U \frac{Y^{2^{2^{i-2}}}}{X^{2^{2^{i-2}}} - Y^{2^{2^{i-2}}}}(X - Y) \end{aligned}$$

$$u_i = x_i + y_i = U \frac{X^{2^{2^{i-2}}} + Y^{2^{2^{i-2}}}}{X^{2^{2^{i-2}}} - Y^{2^{2^{i-2}}}}(X - Y) = \frac{X^{2^{2^{i-2}}} + Y^{2^{2^{i-2}}}}{X^{2^{2^{i-2}}} - Y^{2^{2^{i-2}}}}(X^2 - Y^2)$$

soit a U^2 pres l'expression de u'_{i-1} , le u_{i-1} de l'exposant 2. Le cas $n = 2$ est donc equivalent au cas $n = 1$ et il y aura une infinite de solutions !

Conclusion

Nous avons demontre que pour tout $X, Y, U, n > 2$ entiers

$$U^n \neq X^n + Y^n$$

Et, si c'est vrai pour des entiers, cela l'est egalement pour des rationnels.