An elementary proof of Fermat-Wiles theorem.

Jamel Ghannouchi

An elementary proof of Fermat-Wiles theorem

Jamel Ghanouchi
Ecole Supérieure des Sciences et Techniques de Tunis
jamel.ghanouchi@live.com

Abstract

(MSC=11D04) We begin with Fermat equation $Y^n = X^n + Z^n$ and solve it.

(Keywords : Diophantine equations, Fermat equation ; Approach)

Resolution of Fermat equation

Let Fermat equation :

$$Y^n = X^n + Z^n$$

We have

$$X^{n-2}Y^2 - Y^{n-2}X^2 = AZ^n$$

And

$$Y^{n-2}Y^2 - X^{n-2}X^2 = Y^n - X^n = Z^n$$

If $A = 0$ then $X^{n-4} = Y^{n-4}$ leads, as $GCD(X, Y) = 1$, to $n = 4$. This case has been studied by Fermat, it has no solution. Thus $A \neq 0$.
And if $A = \pm 1$ then it means that both
$X^{n-3}Y^2 = \pm\frac{Z^n}{X} + XY^{n-2}$ and
$Y^{n-3}X^2 = \mp\frac{Z^n}{X} + X^{n-3}Y^2$ are rationals

it means that $n = 2$.
We have

$$\frac{X^{n-2}}{A}Y^2 - \frac{Y^{n-2}}{A}X^2 = Z^n = Y^{n-2}Y^2 - X^{n-2}X^2$$

And we have simultaneously

$$(Y^{n-2} - \frac{X^{n-2}}{A})Y^2 = (X^{n-2} - \frac{Y^{n-2}}{A})X^2$$

Or

$$(AY^{n-2} - X^{n-2})Y^2 = (AX^{n-2} - Y^{p-2})X^2$$

And

$$(Y^2 + \frac{X^2}{A})Y^{n-2} = (X^2 + \frac{Y^2}{A})X^{n-2}$$

Or

$$(AY^2 + X^2)Y^{p-2} = (AX^2 + Y^2)X^{n-2}$$

We have four cases with u and v integers

$$\frac{Y^2}{A} = u(X^{n-2} - \frac{Y^{n-2}}{A}); \quad \frac{X^2}{A} = u(-\frac{X^{n-2}}{A} + Y^{p-2})$$

$$\frac{Y^{n-2}}{A} = v(X^2 + \frac{Y^2}{A}); \quad \frac{X^{n-2}}{A} = v(\frac{X^2}{A} + Y^2)$$

Or

$$u\frac{Y^2}{A} = X^{n-2} - \frac{Y^{n-2}}{A}; \quad u\frac{X^2}{A} = -\frac{X^{n-2}}{A} + Y^{n-2}$$

$$v\frac{Y^{n-2}}{A} = X^2 + \frac{Y^2}{A}; \quad v\frac{X^{n-2}}{A} = \frac{X^2}{A} + Y^2$$

Or

$$\frac{Y^2}{A} = u(X^{n-2} - \frac{Y^{n-2}}{A}); \quad \frac{X^2}{A} = u(-\frac{X^{n-2}}{A} + Y^{n-2})$$

$$v\frac{Y^{n-2}}{A} = X^2 + \frac{Y^2}{A}; \quad v\frac{X^{n-2}}{A} = \frac{X^2}{A} + Y^2$$

Or

$$u\frac{Y^2}{A} = X^{n-2} - \frac{Y^{n-2}}{A}; \quad u\frac{X^2}{A} = -\frac{X^{n-2}}{A} + Y^{n-2}$$

$$\frac{Y^{n-2}}{A} = v(X^2 + \frac{Y^2}{A}); \quad \frac{X^{n-3}}{A} = v(\frac{X^2}{A} + Y^2)$$

First case

$$Y^n = uv(A^2X^n - Y^n + A(Y^2X^{n-2} - Y^{n-2}X^2))$$

$$= uv(A^2X^n - Y^n + A(AZ^n)) = uv(A^2X^n + A^2A^n - Y^n) = uv(A^2Y^n - Y^n)$$

Thus

$$uv = \frac{1}{A^2 - 1}$$

As uv is integer, it means that it is impossible thus $u = 0$ and $A^2 = 1$ or $A = \pm -1$
(A is an integer and can not equal to $\sqrt{2}$)
it means that $q = 3$ and $p = 2$.
Second case

$$uv\frac{Y^n}{A^2} = X^n - \frac{Y^n}{A^2} + \frac{Y^2X^{n-2} - Y^{n-2}X^2}{A}$$

$$= X^n - \frac{Y^n}{A^2} + Z^n = X^n + Z^n - \frac{Y^n}{A^2} = (\frac{A^2 - 1}{A^2})Y^n$$

Thus

$$uv = A^2 - 1$$

And

$$uv(Y^2X^{n-2} - X^2Y^{n-2}) = uvAZ^n = u(X^{2n-4} - Y^{2n-4})A = v(X^4 - Y^4)A$$

Thus

$$uZ^n = X^4 - Y^4; \quad vZ^n = X^{2n-4} - Y^{2n-4}$$

$$uv = A^2 - 1 = (X^4 - Y^4)(X^{2n-4} - Y^{2n-4})$$

$$= (Y^2X^{n-2} - X^2Y^{n-2})^2 - 1 = X^{2n} + Y^{2n} - Y^4X^{2n-4} - X^4Y^{2n-4}$$
$$= Y^4X^{2n-4} + X^4Y^{2n-4} - 2X^nY^n - 1$$

And

$$X^{2n} + Y^{2n} + 2X^nY^n = 2Y^4X^{2n-4} + 2Y^{2n-4}X^4 - 1$$
$$= (Y^n + X^n)^2 = (2Y^n - Z^n)^2 = 4Y^{2n} - 4Z^nY^n + Z^{2n}$$

If $n \geq 3$ then

$$\frac{Z^{2n} + 1}{Y} = 2Y^3X^{2n-4} + Y^{2n-5}X^4 - 2Y^{2n-1} + 2Y^{n-1} \in \mathbb{Z}$$

And It is impossible ! It means that $n = 2$.
Third case :
We have here

$$Y^2 = u(AX^{n-2} - Y^{n-2}); \quad X^2 = u(-X^{n-2} + AY^{n-2})$$
$$vY^{n-2} = AX^2 + Y^2; \quad vX^{n-2} = X^2 + AY^2$$

And

$$vY^n = u(A^2X^n - Y^n + A^2Z^n) = u(A^2 - 1)Y^n$$
$$v = u(A^2 - 1)$$
$$v(Y^2X^{n-2} - X^2Y^{p-2}) = vA = uvA(X^{2n-4} - Y^{2n-4}) = A(X^4 - Y^4)$$
$$= u^2A(X^{2n-4} - Y^{2n-4})^2 = v^2A$$

Thus

$$v = 1 = u(A^2 - 1)$$

With u and $A^2 - 1$ integers, it means $A^2 = 2$: Impossible ! Fourth case :

$$u\frac{Y^2}{A} = X^{n-2} - \frac{Y^{n-2}}{A}; \quad u\frac{X^2}{A} = -\frac{X^{n-2}}{A} + Y^{n-2}$$
$$\frac{Y^{n-2}}{A} = v(X^2 + \frac{Y^2}{A}); \quad \frac{X^{n-2}}{A} = v(\frac{X^2}{A} + Y^2)$$

We have here

$$uY^2 = AX^{n-2} - Y^{n-2}; \quad uX^2 - AY^{n-2} = -X^{n-2}$$

And

$$Y^{n-2} = AX^{n-2} - uY^2 = (Y^2X^{n-2} - X^2Y^{n-2})X^{n-2} - uY^2$$

Hence

$$u\frac{Y^n}{A^2} = v(X^n - \frac{Y^p}{A^2} + Z^n) = v(1 - \frac{1}{A^2})Y^n$$

Thus

$$u = v(A^2 - 1)$$
$$u(Y^2X^{n-2} - X^2Y^{n-2}) = uA = A(X^{2n-4} - Y^{2n-4}) = uv(X^4 - Y^4)A$$
$$u = X^{2n-4} - Y^{2n-4} = v(X^4 - Y^4) = uv(X^4 - Y^4)$$

Thus $u = 1$ and $v(A^2 - 1) = 1$ with v and $A^2 - 1$ integers, it means $A^2 - 1 = 2$: Impossible !
The only solution, in all cases, in $n = 2$.
And there is of course the trivail $n = 1$

Conclusion

Fermat equation $Y^n = X^n + Z^n$ has solutions only for $n = 2$. We have shown a way to solve it.

Références

[1] Paolo Ribenboïm, The Catalan's conjecture *Academic press* , (1994).

[2] Robert Tijdeman, On the equation of Catalan *Acta Arith* , (1976).