An elementary proof of Catalan-Mihailescu theorem

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

Abstract

(MSC=11D04) We begin with Catalan equation $Y^p = X^q + 1$ and solve it.

(Keywords : Diophantine equations, Catalan equation ; Approach)

Resolution of Catalan equation

Let Catalan equation :

$$Y^p = X^q + 1$$

We have

$$X^{q-3}Y^2 - Y^{p-2}X^3 = A$$

And

$$Y^{p-2}Y^2 - X^{q-3}X^3 = Y^p - X^q = 1$$

If $A = 0$ then $X^{q-6} = Y^{p-4}$ leads, as $GCD(X, Y) = 1$, to $p = 4$ and $q = 6$. This case has been studied by Lebesgue in the XIX century, it has no solution. Thus $A \neq 0$.

And if $A = \pm 1$ then it means that both
$X^{q-4}Y^2 = \pm\frac{1}{X} + X^2Y^{p-2}$ and
$Y^{p-3}X^3 = \mp\frac{1}{X} + X^{q-3}Y$ are rationals

it means that $q = 3$ and $p = 2$.
We have

$$\frac{X^{q-3}}{A}Y^2 - \frac{Y^{p-2}}{A}X^3 = 1 = Y^{p-2}Y^2 - X^{q-3}X^3$$

And we have simultaneously

$$(Y^{p-2} - \frac{X^{q-3}}{A})Y^2 = (X^{q-3} - \frac{Y^{p-2}}{A})X^3$$

Or

$$(AY^{p-2} - X^{q-3})Y^2 = (AX^{q-3} - Y^{p-2})X^3$$

And

$$(Y^2 + \frac{X^3}{A})Y^{p-2} = (X^3 + \frac{Y^2}{A})X^{q-3}$$

Or

$$(AY^2 + X^3)Y^{p-2} = (AX^3 + Y^2)X^{q-3}$$

We have four cases with u and v integers

$$\frac{Y^2}{A} = u(X^{q-3} - \frac{Y^{p-2}}{A}); \quad \frac{X^3}{A} = u(-\frac{X^{q-3}}{A} + Y^{p-2})$$

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

Or

$$u\frac{Y^2}{A} = X^{q-3} - \frac{Y^{p-2}}{A}; \quad u\frac{X^3}{A} = -\frac{X^{q-3}}{A} + Y^{p-2}$$

$$v\frac{Y^{p-2}}{A} = X^3 + \frac{Y^2}{A}; \quad v\frac{X^{q-3}}{A} = \frac{X^3}{A} + Y^2$$

Or

$$\frac{Y^2}{A} = u(X^{q-3} - \frac{Y^{p-2}}{A}); \quad \frac{X^3}{A} = u(-\frac{X^{q-3}}{A} + Y^{p-2})$$

$$v\frac{Y^{p-2}}{A} = X^3 + \frac{Y^2}{A}; \quad v\frac{X^{q-3}}{A} = \frac{X^3}{A} + Y^2$$

Or

$$u\frac{Y^2}{A} = X^{q-3} - \frac{Y^{p-2}}{A}; \quad u\frac{X^3}{A} = -\frac{X^{q-3}}{A} + Y^{p-2}$$

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

First case

$$Y^p = uv(AX^q - Y^p + A(Y^2X^{q-3} - Y^{p-2}X^3))$$

$$= uv(A^2X^q - Y^p + A(A)) = uv(A^2X^q + A^2 - Y^p) = uv(A^2Y^p - Y^p)$$

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

$$uv\frac{Y^p}{A^2} = X^q - \frac{Y^p}{A^2} + \frac{Y^2X^{q-3} - Y^{p-2}X^3}{A}$$

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

Thus

$$uv = A^2 - 1$$

And

$$uv(Y^2X^{q-3} - X^3Y^{p-2}) = uvA = u(X^{2q-6} - Y^{2p-4})A = v(X^6 - Y^4)A$$

Thus

$$u = X^6 - Y^4; \quad v = X^{2q-6} - Y^{2p-4}$$

$$uv = A^2 - 1 = (X^6 - Y^4)(X^{2q-6} - Y^{2p-4})$$

$$= (Y^2X^{q-3} - X^3Y^{p-2})^2 - 1 = X^{2q} + Y^{2p} - Y^4X^{2q-6} - X^6Y^{2p-4}$$
$$= Y^4X^{2q-6} + X^6Y^{2p-4} - 2X^qY^p - 1$$

And

$$X^{2q} + Y^{2p} + 2X^qY^p = 2Y^4X^{2q-6} + 2Y^{2p-4}X^6 - 1$$
$$= (Y^p + X^q)^2 = (2Y^p - 1)^2 = 4Y^{2p} - 4Y^p + 1$$

If $p \geq 3$ then

$$\frac{1}{Y} = Y^3X^{2q-6} + Y^{2p-5}X^6 - 2Y^{2p-1} + 2Y^{p-1} \in \mathbb{Z}$$

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

$$Y^2 = u(AX^{q-3} - Y^{p-2}); \quad X^3 = u(-X^{q-3} + AY^{p-2})$$
$$vY^{p-2} = AX^3 + Y^2; \quad vX^{q-3} = X^3 + AY^2$$

And

$$vY^p = u(A^2X^q - Y^p + A^2) = u(A^2 - 1)Y^p$$
$$v = u(A^2 - 1)$$
$$v(Y^2X^{q-3} - X^3Y^{p-2}) = vA = uvA(X^{2q-6} - Y^{2p-4}) = A(X^6 - Y^4)$$
$$= u^2A(X^{2q-6} - Y^{2p-4})^2 = v^2A$$

Thus

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

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

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

We have here

$$uY^2 = AX^{q-3} - Y^{p-2}; \quad uX^3 - AY^{p-2} = -X^{q-3}$$

And

$$Y^{p-2} = AX^{q-3} - uY^2 = (Y^2X^{q-3} - X^3Y^{p-2})X^{q-3} - uY^2$$

Hence

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

Thus

$$u = v(A^2 - 1)$$
$$u(Y^2X^{q-3} - X^3Y^{p-2}) = uA = A(X^{2q-6} - Y^{2p-4}) = uv(X^6 - Y^4)A$$
$$u = X^{2q-6} - Y^{2p-4} = v(X^6 - Y^4) = uv(X^6 - Y^4)$$

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 $p = 2$ and $q = 3$.
And $Y^2 = X^3{+}1$ whose solution is $(X, Y) = (2, \pm 3)$.

Conclusion

Catalan equation $Y^p = X^q + 1$ has solutions only for $q = 3$ and $p = 2$. 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).