



HAL
open science

An elementary proof of Catalan-Mihailescu theorem

Jamel Ghannouchi

► **To cite this version:**

| Jamel Ghannouchi. An elementary proof of Catalan-Mihailescu theorem. 2011. hal-00677731v1

HAL Id: hal-00677731

<https://hal.science/hal-00677731v1>

Preprint submitted on 9 Mar 2012 (v1), last revised 25 Oct 2014 (v35)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

An elementary proof of Catalan-Mihailescu theorem

Jamel Ghanouchi

jamel.ghanouchi@topnet.tn

Abstract

(MSC=11D04) More than one century after its formulation by the Belgian mathematician Eugene Catalan, Preda Mihailescu has solved the open problem. But, is it all? Mihailescu's solution utilizes computation on machines, we propose here not really a proof as it is intended classically, but a resolution of an equation like the resolution of the polynomial equations of third and fourth degrees. This solution is totally algebraic and does not utilize, of course, computers or any kind of calculation.

(Keywords : Diophantine equations, Catalan equation ; Algebraic resolution)

Introduction

Catalan theorem has been proved in 2002 by Preda Mihailescu. In 2004, it became officially Catalan-Mihailescu theorem. This theorem stipulates that there are not consecutive pure powers. There do not exist integers strictly greater than 1, $X > 1$ and $Y > 1$, for which with exponents strictly greater than 1, $p > 1$ and $q > 1$,

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

but for $(X, Y, p, q) = (2, 3, 2, 3)$. We can verify that

$$3^2 = 2^3 + 1$$

Euler has proved that the equation $X^3 + 1 = Y^2$ has this only solution. We propose in this study a general solution. The particular cases already solved concern $p = 2$, solved by Ko Chao in 1965, and $q = 3$ which has been solved in 2002. The case $q = 2$ has been solved by Lebesgue in 1850. We solve here the equation for the general case.

The approach

Let

$$c = \frac{X^p - 1}{Y^{\frac{p}{2}}}, \quad c' = \frac{7 - X^p}{Y^{\frac{p}{2}}}$$

And

$$b = \frac{X^p - 1}{Y^{q-p}}, \quad b' = \frac{7 - X^p}{Y^{q-p}}$$

If

$$c' = 1 \Rightarrow (7 - X^p)^2 = X^q + 1$$

If we suppose $p > q$

$$48 - 14X^p + X^{2p} = X^q$$

Thus

$$\frac{48}{X^q} = 1 + 14X^{p-q} - X^{2p-q}$$

is an integer, hence X^q divides 48, three solutions

$$X^q = 4 \Rightarrow X^q + 1 = 5 \neq Y^p$$

And

$$X^q = 16 \Rightarrow X^q + 1 = 17 \neq Y^p$$

And

$$X^q = 8 \Rightarrow X^q + 1 = 9 = Y^p \Rightarrow q > p$$

And the hypothesis $p > q$ is impossible! Now let $q > p$

$$\frac{48}{X^p} = X^{q-p} + 14X^{q-p} - X^p$$

is an integer, hence X^p divides 48, three solutions

$$X^p = 8 \Rightarrow (7 - X^p)^2 = 1 \neq X^q + 1$$

And

$$X^p = 16 \Rightarrow (7 - X^p)^2 = 81 \neq X^q + 1$$

And

$$X^p = 4 \Rightarrow X = 2, \quad p = 2 \Rightarrow (7 - X^p)^2 = 9 = X^q + 1 = Y^2 \Rightarrow Y = \pm 3, \quad q = 3$$

Now, if $c = 1$, thus

$$(X^p - 1)^2 = X^q + 1$$

Thus

$$X^{2p} - 2X^p = X^q$$

As $X^q > X^p$, thus $q > p$ and

$$X^{q-p} = X^p - 2 \geq 2$$

We deduce

$$q - p > 0, \quad p > 1$$

if we divide by X

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

is an integer, thus

$$X = 2$$

and

$$2^{p-1} - 1 = 2^{q-p-1}$$

In the right, we have an even number and in the left, an odd one : this equality is possible if $p = 2$. We have

$$2 - 1 = 1 = X^{q-3} \Rightarrow q = 3 \Rightarrow Y^2 = 2^3 + 1 = 9 \Rightarrow Y = \pm 3$$

If $(c^2 - 1)(c'^2 - 1) \neq 0$. Thus let

$$d = X^p - Y^{\frac{p}{2}}, \quad d' = Y^{\frac{p}{2}} + X^p$$

Or

$$X^p - d = d' - X^p \Rightarrow X^p = \frac{d + d'}{2} \Rightarrow Y^{\frac{p}{2}} = X^p - d = \frac{d' - d}{2}$$

But

$$\begin{aligned} cc'Y^{\frac{p}{2}} &= c'(X^p - 1) = c(7 - X^p) \Rightarrow X^p = \frac{7c + c'}{c + c'} \\ &\Rightarrow Y^{\frac{p}{2}} = \frac{X^p - 1}{c} = \frac{6}{c + c'} \end{aligned}$$

But

$$\frac{d + d'}{2} = \frac{7c + c'}{c + c'}, \quad \frac{d' - d}{2} = \frac{6}{c + c'}$$

Hence

$$d = \frac{7c + c' - 6}{c + c'}, \quad d' = \frac{7c + c' + 6}{c + c'}$$

We will give two proofs that $(c - 1)(c' - 1) = 0$. Let

$$Z = \frac{7c' + c}{c' + c}, \quad e = \frac{7c' + c - 6}{c + c'}, \quad e' = \frac{7c' + c + 6}{c' + c}$$

We have

$$(c - 1)Z = (c - 1)(8 - X^p) = 8(c - 1) - cd + 1 = c(8 - d) - 7 = ce' - 7$$

And

$$(c' - 1)Z = (c' - 1)(8 - X^p) = 8(c' - 1) - c'd' + 7 = c'(8 - d') - 1 = c'e - 1$$

We have

$$e = \frac{7c' + c - 6}{c + c'}, \quad e' = \frac{7c' + c + 6}{c + c'}$$

And let

$$d' = \alpha d, \quad e' = \beta e$$

But

$$d' - e' = d - e = \alpha d - \beta e$$

Thus

$$(\beta - 1)e = (\alpha - 1)d$$

And

$$\frac{\beta - 1}{\alpha - 1} = \frac{d}{e} = \frac{d'\beta}{e'\alpha}$$

Hence

$$\frac{\alpha\beta - \alpha}{\alpha\beta - \beta} = \frac{d'}{e'}$$

If we subtract 1

$$\begin{aligned} \frac{\beta - \alpha}{\alpha\beta - \beta} &= \frac{d' - e'}{e'} = \frac{6(c - c')}{7c' + c + 6} \\ \frac{\beta - \alpha}{\alpha - 1} &= \frac{d - e}{e} = \frac{6(c - c')}{7c' + c - 6} = \frac{6\beta(c - c')}{7c' + c + 6} \\ &= \frac{6(\beta - 1)(c - c')}{12} \\ 2(\beta - \alpha) &= (\alpha - 1)(\beta - 1)(c - c') \\ &= 2\left(\frac{e'}{e} - \frac{d'}{d}\right) = 2\left(\frac{e'd - ed'}{ed}\right) \\ &= 2\left(\frac{(7c' + c + 6)(7c + c' - 6) - (7c' + c - 6)(7c + c' + 6)}{ed}\right) \\ &= \frac{-24(7c' + c) + 24(7c + c')}{ed} = \frac{144(c - c')}{ed} \end{aligned}$$

Or

$$\begin{aligned} 144(c - c') &= (\alpha - 1)(\beta - 1)de(c - c') = (c - c')(d' - d)(e' - e) = 4Y^p(c - c') \\ 4Y^p &= 4(X^q + 1) \neq 144 \Rightarrow c = c' \end{aligned}$$

And

$$(c - 1)Y^{\frac{p}{2}} - (c' - 1)Y^{\frac{p}{2}} = d - 1 - (7 - d') = 0 = d + d' - 8 = 2X^p - 8$$

And $(X, p) = (2, 2)$ But

$$Y^p - 1 = Y^2 - 1 = 2^q$$

Y must be of the form $Y = \pm 2^\gamma(2k + 1)$ And

$$2^{2\gamma}(4k^2 + 4k + 1) - 1 = 2^q \Rightarrow (\gamma, k) = (0, 1) \Rightarrow 8 = 2^q \Rightarrow (Y, q) = (\pm 3, 3)$$

Second proof : We have

$$cY^{\frac{p}{2}} = c(X^p - d) = X^p - 1 \Rightarrow X^p = \frac{cd - 1}{c - 1}$$

And

$$Y^p = (X^p - d)^2 = \frac{(d - 1)^2}{(c - 1)^2}$$

If we pose

$$c^2Y^{3p} = b^2Y^{2q}$$

We have

$$Y^q = \frac{c(d - 1)^3}{b(c - 1)^3}$$

And

$$\frac{b^2 - 1}{c^2 - 1} = \frac{c^2Y^{3p-2q} - 1}{b^2Y^{2q-3p} - 1}$$

$$= \left(\frac{Y^{-2q}}{Y^{-3p}}\right) \left(\frac{c^2 Y^{3p} - Y^{2q}}{b^2 Y^{2q} - Y^{3p}}\right) = \left(\frac{b^2}{c^2}\right) \left(\frac{c^2 Y^{3p} - Y^{2q}}{b^2 Y^{2q} - Y^{3p}}\right)$$

We deduce

$$\frac{b^2 c^2 - c^2}{b^2 c^2 - b^2} = \frac{c^2 Y^{3p} - Y^{2q}}{b^2 Y^{2q} - Y^{3p}}$$

Or

$$\frac{b^2 c^2 - c^2}{b^2 c^2 - b^2} - 1 = \frac{b^2 - c^2}{b^2(c^2 - 1)} = \frac{(c^2 + 1)Y^{3p} - (b^2 + 1)Y^{2q}}{b^2 Y^{2q} - Y^{3p}}$$

If we develop

$$b^2(c^2 - 1)((c^2 + 1)Y^{3p} - (b^2 + 1)Y^{2q}) = (b^2 - c^2)(b^2 Y^{2q} - Y^{3p})$$

Or

$$\begin{aligned} b^2 Y^{2q}(b^2 - c^2 + (c^2 - 1)(b^2 + 1)) &= Y^{3p}(b^2(c^4 - 1) + b^2 - c^2) \\ &= c^2 Y^{3p}(b^2 - c^2 + (c^2 - 1)(b^2 + 1)) = c^2 Y^{3p}(b^2 c^2 - 1) \end{aligned}$$

We deduce

$$b^2 - c^2 + (c^2 - 1)(b^2 + 1) = c^2 b^2 - 1$$

Also

$$\frac{b^2 c^2 - b^2}{b^2 c^2 - c^2} - 1 = \frac{c^2 - b^2}{c^2(b^2 - 1)} = \frac{(b^2 + 1)Y^{2q} - (c^2 + 1)Y^{3p}}{c^2 Y^{3p} - Y^{2q}}$$

If we develop

$$\begin{aligned} c^2 Y^{3p}(c^2 - b^2 + (b^2 - 1)(c^2 + 1)) &= Y^{2q}(c^2(b^4 - 1) + c^2 - b^2) \\ &= b^2 Y^{2q}(c^2 - b^2 + (b^2 - 1)(c^2 + 1)) = Y^{2q} b^2 (c^2 b^2 - 1) \end{aligned}$$

And we have

$$c^2 - b^2 + (b^2 - 1)(c^2 + 1) = b^2(c^2 b^2 - 1)$$

And

$$b^2 - c^2 + (c^2 - 1)(b^2 + 1) = c^2(c^2 b^2 - 1)$$

We add

$$\begin{aligned} (b^2 - 1)(c^2 + 1) + (c^2 - 1)(b^2 + 1) &= (b^2 + c^2)(c^2 b^2 - 1) \\ &= 2b^2 c^2 - 2 = (b^2 + c^2)(c^2 b^2 - 1) \end{aligned}$$

Consequently

$$(b^2 + c^2 - 2)(c^2 b^2 - 1) = 0$$

It means $b^2 + c^2 = 2$ or $b^2 c^2 = 1$. $c^2 - 1$ can not be different of zero! As we saw, the solution is

$$(c^2 - 1)(c'^2 - 1) = 0$$

Conclusion

Catalan equation implies a second one, and an original solution of Catalan equation exists. It seems that many problems of number theory can be solved like this. How? We showed an example.

Références

- [1] P. MIHAILESCU A class number free criterion for catalan's conjecture, *Journal of Number theory* , **99** (2003).