International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

An Elementary Proof of Fermat-Wiles Theorem and Generalization to Beal Conjecture

Jamel Ghanouchi

RIME Department of Mathematics, Marsa, Tunisie

Abstract: ***A proof of Fermat theorem is presented and a generalization to Beal conjecture is proposed. For this, we begin with Fermat and Fermat-Catalan equations and solve them.***

Keywords: Diophantine; Fermat; Fermat-Catalan; Resolution

1. The Fermat Equation

Fermat equation is $y^n = x^n \pm z^n = x^n + az^n$

Let $x^{n-2}y^2 - y^{n-2}x^2 = Aa$

If $A = 0 \Rightarrow x^{n-4} = y^{n-4}$ but $GCD(x,y) = 1 \Rightarrow n = 4$ impossible, there is no solution and

If $A^2 = z^{2n}; n \geq 3 \Rightarrow x^{n-3}y - y^{n-2} = \dfrac{Aaz^n}{x} \in Z$ impossible $\Rightarrow n = 2$

We have

$$(x^{n-2}y^2 - y^{n-2}x^2)z^n = Aaz^n = Ay^{n-2}y^2 - Ax^{n-2}x^2$$

$$\Rightarrow (x^{n-2}z^n - Ay^{n-2})y^2 = (y^{n-2}z^n - Ax^{n-2})x^2$$

$$(y^2z^n + Ax^2)x^{n-2} = (x^2z^n + Ay^2)y^{n-2}$$

But GCD(x,y)=1

We have then four cases:

$$x^2 = u(-x^{n-2}z^n + Ay^{n-2}); y^2 = u(-y^{n-2}z^n + Ax^{n-2})$$

$$x^{n-2} = v(x^2z^n + Ay^2); y^{n-2} = v(y^2z^n + Ax^2)$$

or

$$ux^2 = -x^{n-2}z^n + Ay^{n-2}; uy^2 = -y^{n-2}z^n + Ax^{n-2}$$

$$vx^{n-2} = x^2z^n + Ay^2; vy^{n-2} = y^2z^n + Ax^2$$

or

$$x^2 = u(-x^{n-2}z^n + Ay^{n-2}); y^2 = u(-y^{n-2}z^n + Ax^{n-2})$$

$$vx^{n-2} = x^2z^n + Ay^2; vy^{n-2} = y^2z^n + Ax^2$$

or

$$ux^2 = -x^{n-2}z^n + Ay^{n-2}; uy^2 = -y^{n-2}z^n + Ax^{n-2}$$

$$x^{n-2} = v(x^2z^n + Ay^2); y^{n-2} = v(y^2z^n + Ax^2)$$

with $u, v \in Z$

First case

$$x^2 = u(-x^{n-2}z^n + Ay^{n-2}); y^2 = u(-y^{n-2}z^n + Ax^{n-2})$$

$$x^{n-2} = v(x^2z^n + Ay^2); y^{n-2} = v(y^2z^n + Ax^2)$$

We have

$$y^n = uv(-y^nz^{2n} + A^2x^n - Az^n(x^2y^{n-2} - y^2x^{n-2})) = uv(-y^nz^{2n} + A^2x^n + A^2az^n) = uv(A^2 - z^{2n})y^n$$

$$uv(A^2 - z^{2n}) = 1$$

Impossible because A, u, v are integers

Second case

or

$$ux^2 = -x^{n-2}z^n + Ay^{n-2}; uy^2 = -y^{n-2}z^n + Ax^{n-2}$$

$$vx^{n-2} = x^2z^n + Ay^2; vy^{n-2} = y^2z^n + Ax^2$$

We have

$$uvy^n = -y^nz^{2n} + A^2x^n - Az^n(x^2y^{n-2} - y^2x^{n-2}) = -y^nz^{2n} + A^2x^n + A^2az^n = (A^2 - z^{2n})y^n$$

$$uv = A^2 - z^{2n}$$

But

$$uv(y^2x^{n-2} - x^2y^{n-2}) = auvA = v(-y^{2n-4} + x^{2n-4})A = u(y^4 - x^4)A$$

$$\Rightarrow au = -y^{2n-4} + x^{2n-4}; av = y^4 - x^4$$

$$x < y$$

$$a(A - z^n) = (y^2 + x^2)(x^{n-2} - y^{n-2}) < 0$$

$$a(A + z^n) = y^2x^{n-2} - x^2y^{n-2} + y^n - x^n = (y^2 - x^2)(x^{n-2} + y^{n-2}) > 0$$

$$uv = A^2 - z^{2n} < 0$$

$$a > 0$$

$$A = a(y^2x^{n-2} - x^2y^{n-2}) < 0$$

$$v = a(y^4 - x^4) > 0$$

$$0 < auvA = v(x^{2n-4} - y^{2n-4}) < 0$$

and if

$$x > y$$

$$a(A - z^n) = (y^2 + x^2)(x^{n-2} - y^{n-2}) > 0$$

$$a(A + z^n) = y^2x^{n-2} - x^2y^{n-2} + y^n - x^n = (y^2 - x^2)(x^{n-2} + y^{n-2}) < 0$$

$$uv = A^2 - z^{2n} < 0$$

$$a < 0$$

$$A = a(y^2x^{n-2} - x^2y^{n-2}) < 0$$

$$v = a(y^4 - x^4) > 0$$

$$0 < auvA = v(x^{2n-4} - y^{2n-4}) < 0$$

It is impossible because $\Rightarrow n = 2$

Third case

or

$$x^2 = u(-x^{n-2}z^n + Ay^{n-2}); y^2 = u(-y^{n-2}z^n + Ax^{n-2})$$

$$vx^{n-2} = x^2z^n + Ay^2; vy^{n-2} = y^2z^n + Ax^2$$

We have

$$vy^n = u(-y^nz^{2n} + A^2x^n - Az^n(x^2y^{n-2} - y^2x^{n-2})) = u(-y^nz^{2n} + A^2x^n + A^2az^n) = u(A^2 - z^{2n})y^n$$

$$v = u(A^2 - z^{2n})$$

And

$$v(y^2x^{n-2} - x^2y^{n-2}) = vA = uv(-y^{2n-4} + x^{2n-4})A = (y^4 - x^4)A$$

$$\Rightarrow u(-y^{2n-4} + x^{2n-4}) = 1 \Rightarrow u = \infty; n = 2$$

Impossible because u, A are integers

Fourth case

$$ux^2 = -x^{n-2}z^n + Ay^{n-2}; uy^2 = -y^{n-2}z^n + Ax^{n-2}$$

$$x^{n-2} = v(x^2z^n + Ay^2); y^{n-2} = v(y^2z^n + Ax^2)$$

We have

$$uy^n = v(-y^n z^{2n} + A^2 x^n - Az^n(x^2 y^{n-2} - y^2 x^{n-2})) = v(-y^n z^{2n} + A^2 x^n + A^2 az^n) = v(A^2 - z^{2n})y^n$$

$$u = v(A^2 - z^{2n})$$

And

$$u(y^2 x^{n-2} - x^2 y^{n-2}) = uA = (-y^{2n-4} + x^{2n-4})A = uv(y^4 - x^4)A$$

$$\Rightarrow v(x^4 - y^4) = 1 \Rightarrow v = 1; x^4 = y^4 + 1$$

Impossible! Because v, A are integers !
The only solution is A=1 and n=2

2. The Fermat-Catalan equation

The equation now is $y^p = x^q \pm z^c = x^q + az^c$

Let $x^{q-w} y^2 - y^{p-2} x^w = aA$

If

$$A = 0 \Rightarrow x^{q-2w} = y^{p-4}$$

$$GCD(x,y) = 1 \Rightarrow p = 4$$

It means that p=2 is the prime solution!
And

$$A^2 = z^{2c}; p \geq 3 \Rightarrow x^{q-w} y - y^{p-3} x^w = \frac{\pm z^c}{y} \in Z$$

Impossible because GCD(y,z)=1, thus p=2
We have

$$(x^{q-w} y^2 - y^{p-2} x^w) z^c = aAz^c = Ay^{p-2} y^2 - Ax^{q-w} x^w$$

$$\Rightarrow (x^{q-w} z^c - Ay^{p-2}) y^2 = (y^{p-2} z^c - Ax^{q-w}) x^w$$

$$(y^2 z^c + Ax^w) x^{q-w} = (x^w z^c + Ay^2) y^{p-2}$$

$$GCD(x,y) = 1$$

We have then four cases:
First case

$$x^w = u(-x^{q-w} z^c + Ay^{p-2}); y^2 = u(-y^{p-2} z^c + Ax^{q-w})$$

$$x^{q-w} = v(x^w z^c + Ay^2); y^{p-2} = v(y^2 z^c + Ax^w)$$

We have

$$y^p = uv(-y^p z^{2c} + A^2 x^q - Az^c(x^w y^{p-2} - y^2 x^{q-w})) = uv(-y^p z^{2c} + A^2 x^q + A^2 az^c) = uv(A^2 - z^{2c})y^p$$

$$uv(A^2 - z^{2c}) = 1$$

Impossible because A,u,v are integers
Second case

$$ux^w = -x^{q-w} z^c + Ay^{p-2}; uy^2 = -y^{p-2} z^c + Ax^{q-w}$$

$$vx^{q-w} = x^w z^c + Ay^2; vy^{p-2} = y^2 z^c + Ax^w$$

We have

$$uvy^p = -y^p z^{2c} + A^2 x^q - Az^c(x^w y^{p-2} - y^2 x^{q-w}) = -y^p z^{2c} + A^2 x^q + A^2 az^c) = (A^2 - z^{2c})y^p$$

$$uv = A^2 - z^{2c}$$

And if a>0 and the proof is the same for a<0, we have

$$A = y^2x^{a-w} - x^w y^{p-2} = (x^a + z^c)(\frac{x^{a-w}}{y^{p-2}} - \frac{x^w}{y^2})$$

$$A < 0 \Rightarrow \frac{x^{a-w}}{y^{p-2}} - \frac{x^w}{y^2} < 0$$

$$x^{a-w} < y^{b-2}; x^w > y^2 \Rightarrow x^{a-w}y^2 < y^b = x^a + z^c < x^w y^{b-2}$$

$$x^w x^{a-w} = x^a = y^b - z^c > y^2 x^{a-w}$$

$$0 < y^2(y^{b-2} - x^{a-w}) < x^a + z^c - x^a = z^c = y^b - x^a$$

$$\Rightarrow y^2 x^{a-w} > x^a \Rightarrow x^w < y^2 < x^w$$

It is impossible !

And if

$$x^w < y^2 \Rightarrow x^{a-w} < y^{b-2} \Rightarrow x^{a-w}y^2 < y^b = x^a + z^c \Rightarrow 1 \le y^2 - x^w < z^c x^{w-a}$$

Thus if $x^a > z^c$ it is impossible ! And if

$$x^{a-w} > y^{b-2} \Rightarrow x^w > y^2 \Rightarrow x^{a-w}y^2 > y^b = x^a + z^c \Rightarrow 0 > y^2 - x^w > z^c x^{w-a} > 0$$

It is impossible ! Let us suppose now

$$A > 0 \Rightarrow \frac{x^{a-w}}{y^{p-2}} - \frac{x^w}{y^2} > 0$$

If

$$x^{a-w} > y^{b-2}; x^w < y^2 \Rightarrow y^{b-2}y^2 = y^b = x^a + z^c > x^w y^{b-2}$$

$$x^w x^{a-w} = x^a = y^b - z^c < y^2 x^{a-w}$$

$$0 > y^2(y^{b-2} - x^{a-w}) > y^b - x^a = z^c > 0$$

Impossible ! And if

$$x^w > y^2 \Rightarrow x^{a-w} > y^{b-2} \Rightarrow x^{a-w}y^2 > y^b = x^a + z^c \Rightarrow 0 > y^2 - x^w > z^c x^{w-a} > 0$$

Impossible ! And if

$$x^{a-w} < y^{b-2} \Rightarrow x^w < y^2 \Rightarrow x^{a-w}y^2 < y^b = x^a + z^c \Rightarrow 1 \le y^2 - x^w < z^c x^{w-a}$$

And if $x^a > z^c$ it is impossible ! Another proof :

$$uv(y^2x^{q-w} - x^w y^{p-2}) = auvA = v(-y^{2p-4} + x^{2p-2w})A = u(y^4 - x^{2w})A$$

$$\Rightarrow au = -y^{2p-4} + x^{2q-2w}; av = y^4 - x^{2w}$$

$$1 < \frac{y^4}{x^{2w}} < \frac{y^p}{x^q}$$

$$a(A - z^c) = (y^2 + x^w)(x^{q-w} - y^{p-2}) < 0$$

$$a(A + z^c) = y^2x^{q-w} - x^w y^{p-2} + y^p - x^q = (y^2 - x^w)(x^{q-w} + y^{p-2}) > 0$$

$$uv = A^2 - z^{2c} < 0$$

$$y^p > x^q \Rightarrow a > 0$$

$$A = a(y^2x^{q-w} - x^w y^{p-2}) < 0$$

$$v = a(y^4 - x^{2w}) > 0$$

$$0 < auvA = v(x^{2q-2w} - y^{2p-4}) < 0$$

And if

$$1 > \frac{y^4}{x^{2w}} > \frac{y^p}{x^q}$$

$$a(A - z^c) = (y^2 + x^w)(x^{q-w} - y^{p-2}) > 0$$

$$a(A + z^c) = y^2 x^{q-w} - x^w y^{p-2} + y^p - x^q = (y^2 - x^w)(x^{q-w} + y^{p-2}) < 0$$

$$uv = A^2 - z^{2c} < 0$$

$$y^p < x^q \Rightarrow a < 0$$

$$A = a(y^2 x^{q-w} - x^w y^{p-2}) < 0$$

$$v = a(y^4 - x^{2w}) > 0$$

$$0 < auvA = v(x^{2q-2w} - y^{2p-4}) < 0$$

Impossible because : $\Rightarrow p = 2$

Third case

$$x^w = u(-x^{q-w} z^c + A y^{p-2}); y^2 = u(-y^{p-2} z^c + A x^{q-w})$$

$$v x^{q-w} = x^w z^c + A y^2; v y^{p-2} = y^2 z^c + A x^w$$

We have

$$v y^p = u(-y^p z^{2c} + A^2 x^q - A z^c (x^w y^{p-2} - y^2 x^{q-w})) = u(-y^p z^{2c} + A^2 x^q + A^2 a z^c) = u(A^2 - z^{2c}) y^p$$

$$v = u(A^2 - z^{2c})$$

And

$$v(y^2 x^{q-w} - x^w y^{p-2}) = vA = uv(-y^{2p-4} + x^{2q-2w})A = (y^4 - x^{2w})A$$

$$\Rightarrow u(-y^{2p-4} + x^{2q-2w}) = 1 \Rightarrow p = 2$$

Impossible because u, A are integers

Fourth case

$$u x^w = -x^{q-w} z^c + A y^{p-2}; u y^2 = -y^{p-2} z^c + A x^{q-w}$$

$$x^{q-w} = v(x^w z^c + A y^2); y^{p-2} = v(y^2 z^c + A x^w)$$

We have

$$u y^p = v(-y^p z^{2c} + A^2 x^q - A z^c (x^w y^{p-2} - y^2 x^{q-w})) = v(-y^p z^{2c} + A^2 x^q + A^2 a z^c) = v(A^2 - z^{2c}) y^p$$

$$u = v(A^2 - z^{2c})$$

And

$$u(y^2 x^{q-w} - x^w y^{p-2}) = uA = -y^{2p-4} + x^{2q-2w} A = uv(y^4 - x^{2w})A$$

$$\Rightarrow v(y^4 - x^{2w}) = 1$$

Impossible, because v,A are integers ! In the Fermat-Catalan equation, one of the exponents must be equal to 2 ! The Beal conjecture has been proved ! In fact, in the three precedent equations studied here, one of the exponent greater or equal to 2 must be minimum, which means that it must be 2 !

3. Conclusion

We have solved all three equations by the same method and proved two theorems and one conjecture.

References

[1] Paolo Ribenboïm, The Catalan’s conjecture, Academic Press, 1994
[2] Robert Tijdeman, On the equation of Catalan, ActaArith, 1976