

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

CONFIRMATION OF THE FERMAT LAST THEOREM BY AN ELEMENTARY SHORT PROOF

Mohammed Ghanim*

* Ecole Nationale de Commerce et de Gestion B.P 1255 Tanger Maroc

DOI: 10.5281/zenodo.2222392

ABSTRACT

I give a short elementary proof of the Fermat's last theorem. Recall that the hard problem of finding an elementary proof of this famous conjecture (called Fermat last theorem), which says that the Diophante equation $x^n + y^n = z^n$ has, for $n \geq 3$, no natural integer solutions x, y, z such that: $0 < x < y < z$, is open since 1665 (the extinction date of the French Mathematician Pierre de Fermat (1601-1665)). Recall also that the 1994 proof of the English Mathematician Andrew Wiles (Born in 1953) [13] is not elementary because it uses powerful tools of number theory and is not short because it takes 100 pages. My proof, taking 13 pages, is based essentially on the intermediate value theorem, the B. Bolzano (1781-1848)-K. Weierstrass (1815-1897) theorem and the L. Euler (1707-1783)-J.C.F. Gauss (1777-1855) theorem. My proof uses also some techniques of my previous papers [5], [6] published by the GJAETS.

KEYWORDS: Fermat last theorem, Intermediate value theorem, Bolzano-Weierstrass theorem, Euler-Gauss theorem.

2010 Mathematics Subject Classification: 11 A xx (Elementary Number theory)

INTRODUCTION

Definition: We call « Fermat last theorem », the following statement: « It does not exist natural integers x, y and z such that: $0 < x < y < z$ and $x^n + y^n = z^n$, for n a natural integer ≥ 3 ».

History: *This problem has appeared about the fourth century with the Greek mathematician Diophante (325-410) in his work « Arithmetica » [1] (the problem II.VIII, page 85), but the problem $x^2 + y^2 = z^2$, has appeared and was resolved by Euclid, about 300 before J.C, in his famous "Elements" (The Book X)[2]

*About 1621, the French mathematician Pierre Simon de Fermat (1601-1665) wrote in the margin of the page 85 of his copy of [1] nears the statement of the famous problem, the following: « J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir ». This we can translate as: "I have discovered a truly remarkable proof which this margin is too small to contain". But it seems that Fermat has never published his proof. In any case we don't know now this proof.

*In 1670, the proof of the case $n=4$, by Fermat, was published by his son Samuel.

*On 4 August 1753, L. Euler wrote to Goldbach claiming to prove the Fermat last theorem for $n=3$, but his proof, published in his book "Algebra" (1770) is incomplete.

*In 1816, the Paris Sciences Academy devoted a gold medal and 3000 F for who can give a proof of the Fermat last theorem. This offer was retaken in 1850.

*In 1825, Dirichlet (1805-1859) and Legendre (1752-1833) proved the case $n=5$.

*Searching a solution to the Fermat last theorem, Marie-Sophie Germain (1776-1831) discovered his "Sophie Germain theorem"[10] which says that at least one of the positive integers x, y, z such that $x^p + y^p = z^p$, for $p \geq 3$ a prime integer, must be divisible by p^2 if we can find an auxiliary prime q such that:

- 1) Two none zero consecutive classes modulo q cannot be simultaneously be p -powers
- 2) p itself cannot be a p -power modulo q

*In 1832, Dirichlet proved the case $n=14$.

*In 1839, Lame proved the case $n=7$

*In 1863, the proof of the case $n=3$, by Gauss, was published.

*In 1908, The Gottingen University and the Wolfskehl Foundation devoted a price of 100.000 Marks for who can give a proof of the Fermat last theorem before 2008.

*In 1952, Harry Vandiver used a Swac Computer to show that the Fermat last theorem is true for $n \leq 2000$

*Between 1964 and 1994, Jean-Pierre Sere, Yves Hellegouarch and Robert Langlands have given some development to the problem by working on the representation of the elliptic curves with the modular functions.

* This problem, then, remained open for more than 370 years, (Although many attempts of the more eminent mathematicians), when in 1994 the English mathematician Andrew Wiles [13] proved it—by a relatively long proof that has occupied about 100 pages- using powerful tools of number theory, such the Shimura-Taniyama-Weil conjecture, the modular forms, the Galoisian representations...

So the problem of finding a short elementary proof of the Fermat last theorem remained open up to now.

*For More and detailed History see on Wikipedia the articles on the Fermat last theorem specially [9] with their references and the Simon Singh good book “Le dernier théorème de Fermat” [8].

The note: The present short note gives an elementary short proof of the Fermat’s last theorem. Indeed, using the intermediate value theorem, the Bolzano-Weierstrass theorem and the Euler-Gauss theorem (which shows the veracity of the Fermat last theorem for the case: $n = 3$), I show that: $\forall n$ an integer $\geq 3 \forall x, y, z$ integers such: $0 < x < y < z$, we have: $|x^n + y^n - z^n| > 0$.

The paper is organized as follows. The §1 is an introduction giving the necessary definition and some history. The § 2 gives the ingredients of the proof. The §3 gives the proof of the Fermat last theorem. The §4 gives the references of the paper for further reading.

THE INGREDIENTS OF THE PROOF OF FERMAT LAST THEOREM

We will need the following results:

Proposition1: (Euclid (300 before J.C) theorem) ([2], book X) we have:

*for $n = 1$: the equation $x+y=z$ has an infinite number of solutions.

*for $n = 2$: $(x, y, z) = (3, 4, 5)$ is a solution of $x^2 + y^2 = z^2$, and we can show easily that: $\begin{cases} x = 2abc \\ y = a(b^2 - c^2) \\ z = a(b^2 + c^2) \end{cases}$, with

$a, b, c \in \mathbb{N}$, three natural integers of different parity such that: $b > c$, are the solutions of: $x^2 + y^2 = z^2$

Proposition2: (L.Euler (1707-1783) [3] – J.C.F. Gauss (1777-1855) [4] theorem) (See [7] for a proof).

$\forall x, y, z \in \mathbb{N}$ Such that: $0 < x < y < z$, we have: $|x^3 + y^3 - z^3| > 0$

I.e.: for $n = 3$, the Diophante equation $x^3 + y^3 = z^3$ das not have trivial natural integer solutions x, y, z such $0 < x < y < z$.

Proposition 3 : (Intermediate value theorem [12]) let $\varphi: [a, b] \rightarrow \mathbb{R}$ (With: $a < b$) a continuous function. Then:

$$\varphi(a)\varphi(b) < 0 \Rightarrow \exists c \in]a, b[\text{ such that } \varphi(c) = 0$$

Proposition4: (B. Bolzano-K. Weierstrass theorem [11]) any below and above bounded real sequence $(t_n)_n \subset [a, b]$ has a convergent subsequence denoted also $(t_n)_n$, such that: $\lim_{n \rightarrow +\infty} t_n = t \in [a, b]$

Proposition5: we have : (1) $\lim_{t \rightarrow 0^+} t \ln(t) = 0$

(2) So, we can extend, by continuity at 0, the function: $f(t) = t^t$. The extension is defined by $F(t) = \begin{cases} t^t & \text{if } t > 0 \\ 1 & \text{if } t = 0 \end{cases}$

Proof: (of the assertion (2) of proposition6)

The result follows because, by using the assertion (1) of proposition5, we have:

$$\lim_{t \rightarrow 0^+} t^t = \lim_{t \rightarrow 0^+} e^{t \ln(t)} = e^{\lim_{t \rightarrow 0^+} t \ln(t)} = e^0 = 1$$

Proposition6: let A a real subset.

- (1) A is bounded above, if: $\exists M \in \mathbb{R}$ such that: $\forall a \in A: a \leq M$
 (2) A is not bounded above, if: $\exists (a_n)$ a sequence of element of A such that:

$$\lim_{n \rightarrow +\infty} a_n = +\infty$$

Proof: (of the assertion (2) of proposition6)

*The negation of the assertion (1) of proposition6 is " $\forall M \in \mathbb{R} \exists a_M \in A$ such that: $a_M > M$ ". So, in particular: " $\forall n \in \mathbb{N} \exists a_n \in A$ such that: $a_n > n$ ".

*The result follows by tending $n \rightarrow +\infty$.

Proposition7: any none empty, bounded above, part A of \mathbb{N} has a maximal element $a = \max(A)$ characterized by:

- (i) $a \in A$
 (ii) $\forall x \in A \ x \leq a$
 (iii) $a + 1 \notin A$

Proposition8: any none empty part B of \mathbb{N} has a minimal element $b = \min(B)$ characterized by:

- (i) $b \in B$
 (ii) $\forall x \in B \ b \leq x$
 (iii) $b = 0$ or $b - 1 \notin B$

Proposition9: We have:

- (i) For $a > 0, a \neq 1$: the derivative of $f(t) = a^t$ is $f'(t) = a^t \ln(a)$
 (ii) $0 < a < 1 \Leftrightarrow \ln(a) < 0$

Proposition10: $\forall m \in \mathbb{N}^* \forall a, b \in \mathbb{R}: a^m - b^m = (a - b) \sum_{k=0}^{m-1} a^k b^{m-1-k}$

THE ELEMENTARY SHORT PROOF OF THE FERMAT LAST THEOREM

Theorem: (Fermat last theorem)

$\forall n \in \mathbb{N}^* - \{1,2\} \forall x, y, z \in \mathbb{N}$ satisfying $0 < x < y < z$, we have: $|x^n + y^n - z^n| > 0$

Proof: (of the theorem)

Let $A = \{n \in \mathbb{N}^* \text{ such that: } \exists x, y, z \in \mathbb{N} \text{ satisfying } \begin{cases} 0 < x < y < z \\ (\frac{x}{z})^n + (\frac{y}{z})^n = 1 \end{cases}\}$

$B = \{n \in \mathbb{N}^* \text{ such that: } \forall x, y, z \in \mathbb{N} \text{ satisfying } 0 < x < y < z, \text{ we have: } |x^n + y^n - z^n| > 0\}$

It is clear that the theorem is proved if we show that $A = \{1,2\}$

Lemma1: The function $f(s) = (\frac{x}{z})^s + (\frac{y}{z})^s$ is strictly decreasing on the interval $[0, +\infty[$.

Where: x, y, z are integers such that $0 < x < y < z$

Proof: (of lemma1)

*By the assertion (i) of proposition 9, we have:

$$f'(s) = (\frac{x}{z})^s \ln(\frac{x}{z}) + (\frac{y}{z})^s \ln(\frac{y}{z})$$

*By the assertion (ii) of lemma9, we have:

$$0 < \frac{x}{z} < \frac{y}{z} < 1 \Rightarrow \ln(\frac{x}{z}) < \ln(\frac{y}{z}) < 0$$

*So: $f'(s) < 0$.

*That is f is strictly decreasing on $[0, +\infty[$.

Lemma2: $A \neq \emptyset$

Proof: (of lemma2)

By the Euclid theorem (proposition1): $\{1,2\} \subset A$, so: $A \neq \emptyset$

Lemma3: $B \neq \emptyset$

Proof: (of lemma3)

By the Euler-Gauss theorem (proposition2) we have: $3 \in B$, so: $B \neq \emptyset$

Lemma4: We have: (1) $B = \mathbb{P} - A = \{n \in \mathbb{P}, n \notin A\}$ (2) $A \cap B = \emptyset$

Proof: (of lemma4)

The result follows by definition of the sets A and B

Lemma5: We have:

$\forall n \in A \exists x(n), y(n), z(n)$ integers such that $0 < x(n) < y(n) < z(n) \exists m(n)$ an integer $> n$ Such that: $z(n)^{m(n)-1} \geq y(n)^{m(n)} > x(n)^{m(n)}$

Proof: (of lemma5)

*Suppose contrarily that: $\exists n \in A$ such that $\forall 0 < x < y < z \quad \forall m > n: z^{m-1} < y^m$

*We have: $\forall m > n: z^{m-1} < y^m \Leftrightarrow (m-1) \ln(z) < m \ln(y) \Leftrightarrow \frac{\ln(z)}{\ln(y)} < \frac{m}{m-1}$

*So, tending: $m \rightarrow +\infty$, we have: $\lim_{m \rightarrow +\infty} \frac{\ln(z)}{\ln(y)} = \frac{\ln(z)}{\ln(y)} \leq \lim_{m \rightarrow +\infty} \frac{m}{m-1} = 1$

*That is: $\ln(z) \leq \ln(y)$ i.e.: $z \leq y$

*This contradicting our hypothesis “ $z > y$ ”, lemma5 is proved

Lemma6: The set A is bounded above.

Proof: (of lemma6)

*Suppose that A is not bounded.

*So, by the assertion (2) of proposition 6: $\exists q_k \in A$ such that: $\lim_{k \rightarrow +\infty} q_k = +\infty$

*Let: $0 < x(q_k) < y(q_k) < z(q_k)$ integers such that: $(x(q_k))^{q_k} + (y(q_k))^{q_k} = (z(q_k))^{q_k}$

Claim1: We have: $z(q_k) > y(q_k) > x(q_k) > q_k$

Proof: (of claim1)

*By proposition 10, we have:

$$(x(q_k))^{q_k} = (z(q_k))^{q_k} - (y(q_k))^{q_k} = (z(q_k) - y(q_k)) \sum_{i=0}^{q_k-1} (y(q_k))^i (z(q_k))^{q_k-1-i}$$

$$> \sum_{i=0}^{q_k-1} (x(q_k))^i (x(q_k))^{q_k-1-i} = q_k (x(q_k))^{q_k-1}$$

*That is: $x(q_k) > q_k$

*The result follows.

Claim2: We have:

(1) $\lim_{k \rightarrow +\infty} z(q_k) = +\infty$

(2) $\lim_{k \rightarrow +\infty} \left(\frac{x(q_k)}{z(q_k)}\right)^{m(q_k)} = \lim_{k \rightarrow +\infty} \left(\frac{y(q_k)}{z(q_k)}\right)^{m(q_k)} = 0$, $m(q_k) > q_k$ given by lemma5.

Proof: (of claim2)

(1) The result follows by claim1.

(2) *By lemma5, we have: $\exists m(q_k) > q_k$ such that

$$\frac{1}{z(q_k)} \geq \left(\frac{y(q_k)}{z(q_k)}\right)^{m(q_k)} > \left(\frac{x(q_k)}{z(q_k)}\right)^{m(q_k)} > 0$$

* The assertion (1) of claim2, gives the result by tending $k \rightarrow +\infty$

Claim3: $\forall k, r \in \mathbb{N}^* \exists \gamma(q_k, r) \in]0, 1[$ such that:

$$\left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k, r)} \gamma(q_k, r)^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} + \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k, r)} \gamma(q_k, r)^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} = 1$$

Proof: (of claim3)

*Consider on $[0, 1]$ the continuous function:

$$\varphi(t) = \left(\frac{x(q_k)}{z(q_k)}\right)^t t^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} + \left(\frac{y(q_k)}{z(q_k)}\right)^t t^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} - 1$$

*We have:

** $\varphi(0) = \left(\frac{x(q_k)}{z(q_k)}\right)^{(0)} \gamma(q_k, r)^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} + \left(\frac{y(q_k)}{z(q_k)}\right)^{(0)} \gamma(q_k, r)^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} - 1 = 1 + 1 - 1 = 1 > 0$

** $m(q_k) > q_k$ and lemma1 \Rightarrow

$$\varphi(1) = \left(\frac{y(q_k)}{z(q_k)}\right)^{m(q_k)} + \left(\frac{x(q_k)}{z(q_k)}\right)^{m(q_k)} - 1 < \left(\frac{y(q_k)}{z(q_k)}\right)^{q_k} + \left(\frac{x(q_k)}{z(q_k)}\right)^{q_k} - 1 = 1 - 1 = 0$$

*So, by the intermediate value theorem (proposition 3), we have:

$$\varphi(0)\varphi(1) < 0 \Rightarrow \exists \gamma(q_k, r) \in]0, 1[\text{ Such that: } \varphi(\gamma(q_k, r)) = 0$$

That is: $\forall k, r \in \mathbb{N}^: \left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k, r)} \gamma(q_k, r)^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} + \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k, r)} \gamma(q_k, r)^{\gamma(q_k, r) + \frac{1}{r} m(q_k)} = 1$

Claim4: (1) We can suppose: $\lim_{r \rightarrow +\infty} \gamma(q_k, r) = \gamma(q_k) \in [0, 1]$

(2) We can suppose: $\lim_{k \rightarrow +\infty} \gamma(q_k) = \gamma \in [0, 1]$

(3) $\forall k \in \mathbb{N}^*: \left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k)} \gamma(q_k)^{\gamma(q_k) + \frac{1}{r} m(q_k)} + \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k)} \gamma(q_k)^{\gamma(q_k) + \frac{1}{r} m(q_k)} = 1$

(4) $\forall k \in \mathbb{N}^*: \gamma(q_k) \in]0, 1[$

(5) If: $\gamma = 0$, then: $\lim_{k \rightarrow +\infty} (\gamma(q_k))^{\gamma(q_k)} = 1$

(6) If: $\gamma \neq 0$, then: $\lim_{k \rightarrow +\infty} (\gamma(q_k))^{\gamma(q_k)} = \gamma^\gamma \neq 0$

(7) $\lim_{k \rightarrow +\infty} \left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(q_k) = \lim_{k \rightarrow +\infty} \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(q_k) = 0$

Proof: (of claim4)

(1) By the Bolzano-Weierstrass theorem (proposition 4), because $(\gamma(q_k, r))_r \subset]0,1[$, this sequence has a convergent subsequence denoted also $(\gamma(q_k, r))_r$ such that: $\lim_{r \rightarrow +\infty} \gamma(q_k, r) = \gamma(q_k) \in [0,1]$

(2) The result is obtained as the assertion (1) of claim4

(3) The result is obtained by tending $r \rightarrow +\infty$ in the relation of claim3

(4) *If: $\exists k \in \mathbb{N}^*$ such that: $\gamma(q_k) = 0$ or $\gamma(q_k) = 1$, we have: $(\gamma(q_k))^{\gamma(q_k)} = 1$

* So, replacing this value in the relation (2) of claim 4, we have:

$$m(p_k) > p_k \Rightarrow \left(\frac{x(p_k)}{z(p_k)}\right)^{m(p_k)} + \left(\frac{y(p_k)}{z(p_k)}\right)^{m(p_k)} = 1 < \left(\frac{x(p_k)}{z(p_k)}\right)^{p_k} + \left(\frac{y(p_k)}{z(p_k)}\right)^{p_k} = 1$$

*This being impossible, the result follows

(5) (6) are evident.

(7) *The result is obtained by combination of the assertion (2) of claim2 and the assertions (5), (6) of claim 4.

*Indeed:

$$\lim_{k \rightarrow +\infty} \gamma(q_k)^{\gamma(q_k)} = \gamma^\gamma \neq 0 \text{ and } \lim_{k \rightarrow +\infty} \left(\frac{x(q_k)}{z(q_k)}\right)^{m(q_k)} = \lim_{k \rightarrow +\infty} \left(\frac{y(q_k)}{z(q_k)}\right)^{m(q_k)} = 0$$

$$\Rightarrow \lim_{k \rightarrow +\infty} \left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(p_k) = \lim_{k \rightarrow +\infty} \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(p_k) = 0 \gamma^\gamma = 0$$

RETURN TO THE PROOF OF LEMMA6

*Tending $k \rightarrow +\infty$ in the relation (3) of claim 4, with use of the assertion (7) of claim4, we obtain successively:

$$\lim_{k \rightarrow +\infty} \left(\left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(q_k) + \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(q_k)\right) = 1 = \lim_{k \rightarrow +\infty} \left(\frac{x(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(q_k) +$$

$$\lim_{k \rightarrow +\infty} \left(\frac{y(q_k)}{z(q_k)}\right)^{\gamma(q_k)} (\gamma(q_k))^{\gamma(q_k)} m(q_k) = 0 + 0 = 0$$

*This being impossible, lemma6 is proved.

Lemma 7: (1) the set A has a maximal element $\max(A) = m \in \mathbb{N}^* - \{1\}$

(2) $A \subset \{1,2, \dots, m\} = \{n \in \mathbb{N}^*, 1 \leq n \leq m\}$

(3) $\{m + 1, m + 2, \dots\} = \{n \in \mathbb{N}, n \geq m + 1\} \subset B$

Proof: (of lemma7)

(1) The result is obtained by combination of proposition 8, lemma2 and lemma6.

(2) The result follows by use of the assertion (1) of lemma7.

(3) The result follows by taking the complementary in the relation (2) of lemma7.

Lemma8: We have: $m = 2$

Proof: (of lemma8)

The proof of lemma8 will be deduced from the claims below.

Claim5: $\forall n \in \mathbb{N}^* \forall x, y, z, a, b, c$ integers such that $0 < x < y < z$ and $0 < a < b < c$, $\forall k \in \mathbb{N}^* \forall p \in \mathbb{N}^*$ $\exists \delta(p, k) \in]0,1[$ such that:

$$(\delta(p, k))^{\delta(p,k)+\frac{1}{p}} (|a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k}) = (1 - \delta(p, k))^{1-\delta(p,k)+\frac{1}{p}} (|x^n + y^n - z^n| + \frac{1}{k})$$

Proof: (of claim5)

*Consider, on $[0, 1]$, the continuous function ψ defined by:

$$\psi(t) = t^{t+\frac{1}{p}} (|a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k}) - (1 - t)^{1-t+\frac{1}{p}} (|x^n + y^n - z^n| + \frac{1}{k})$$

*We have:

$$**\psi(0) = 0^{\frac{1}{p}} (|a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k}) - 1^{1+\frac{1}{p}} (|x^n + y^n - z^n| + \frac{1}{k}) = -(|x^n + y^n - z^n| + \frac{1}{k}) < 0$$

$$**\psi(1) = 1^{1+\frac{1}{p}} (|a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k}) - 0^{\frac{1}{p}} (|x^n + y^n - z^n| + \frac{1}{k}) = |a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k} > 0$$

*So, by the intermediate value theorem (proposition3), we have: $\exists \delta(p, k) \in]0,1[$ such that:

$$\psi(\delta(p, k)) = 0$$

*That is: $\exists \delta(p, k) \in]0,1[$ such that:

$$\delta(p, k)^{\delta(p,k)+\frac{1}{p}} (|x^{n+1} + y^{n+1} - z^{n+1}| + \frac{1}{k}) = (1 - \delta(p, k))^{1-\delta(p,k)+\frac{1}{p}} (|x^n + y^n - z^n| + \frac{1}{k})$$

Claim6: We have: $\exists \delta(k) \in [0,1]$ such that:

$$\delta(k)^{\delta(k)}(|a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k}) = (1 - \delta(k))^{1-\delta(k)}(|x^n + y^n - z^n| + \frac{1}{k})$$

Proof: (of claim5)

*By the Bolzano-Weierstrass theorem (proposition4), we have: the sequence $(\delta(p, k))_p$ (for fixed k and variable p), being bounded, has a convergent sub-sequence denoted also $(\delta(p, k))_p$ such that:

$$\lim_{p \rightarrow +\infty} \delta(p, k) = \delta(k) \in [0,1]$$

*So, tending $p \rightarrow +\infty$, in the relation of claim5, we have:

$$(\delta(k))^{\delta(k)}(|a^{n+1} + b^{n+1} - c^{n+1}| + \frac{1}{k}) = (1 - \delta(k))^{1-\delta(k)}(|x^n + y^n - z^n| + \frac{1}{k})$$

Claim7: We have:

$$(1) \exists \delta \in [0,1] \text{ Such that: } \delta^\delta(|a^{n+1} + b^{n+1} - c^{n+1}|) = (1 - \delta)^{1-\delta}(|x^n + y^n - z^n|)$$

$$(2) \delta \in [0,1] \Rightarrow \delta^\delta \neq 0 \text{ and } (1 - \delta)^{1-\delta} \neq 0$$

Proof: (of claim7)

(1)*By the Bolzano-Weierstrass theorem (proposition 4), we have: the sequence $(\delta(k))_k$, being bounded, has a convergent sub-sequence denoted also $(\delta(k))_k$ such that:

$$\lim_{k \rightarrow +\infty} \delta(k) = \delta \in [0,1]$$

*So, tending $k \rightarrow +\infty$, in the relation of claim6, we have:

$$F(\delta)(|a^{n+1} + b^{n+1} - c^{n+1}|) = F(1 - \delta)(|x^n + y^n - z^n|)$$

Where, with the notation of the assertion (2) of proposition6: $F(t) = \begin{cases} t^t & \text{if } t > 0 \\ 1 & \text{if } t = 0 \end{cases}$

(2)*Then:

$$** \delta = 0 \text{ or } \delta = 1 \Rightarrow F(\delta) = F(1 - \delta) = 1$$

$$** 0 < \delta < 1 \Rightarrow F(\delta) \neq 0 \text{ and } F(1 - \delta) \neq 0$$

Claim8: We have:

$$(1) n \in B \Rightarrow n + 1 \in B$$

$$(2) \forall n < m: n \in A \Rightarrow n + 1 \in A$$

Proof: (of claim8)

(1)*By the assertions (1) and (2) of claim7, we have:

$$\begin{cases} \delta^\delta(|a^{n+1} + b^{n+1} - c^{n+1}|) = (1 - \delta)^{1-\delta}(|x^n + y^n - z^n|) \\ \forall x, y, z \text{ integers such that: } 0 < x < y < z: |x^n + y^n - z^n| > 0 \\ \delta^\delta \neq 0 \text{ and } (1 - \delta)^{1-\delta} \neq 0 \end{cases}$$

$$\Rightarrow \forall a, b, c \text{ integers such that: } 0 < a < b < c, \text{ we have: } |a^{n+1} + b^{n+1} - c^{n+1}| > 0$$

*That is, by definition of : $n \in B \Rightarrow n + 1 \in B$

(2)* By definition of n , we have: $\forall n < m$

$$\begin{cases} \delta^\delta(|a^{n+1} + b^{n+1} - c^{n+1}|) = (1 - \delta)^{1-\delta}(|x^n + y^n - z^n|) \\ \exists x, y, z \text{ integers such that: } 0 < x < y < z: |x^n + y^n - z^n| = 0 \\ \delta^\delta \neq 0 \text{ and } (1 - \delta)^{1-\delta} \neq 0 \end{cases}$$

$$\Rightarrow \exists a, b, c \text{ integers such that: } 0 < a < b < c, \text{ we have: } |a^{n+1} + b^{n+1} - c^{n+1}| = 0$$

*That is, by definition of $A : \forall n < m: n \in A \Rightarrow n + 1 \in A$

RETURN TO THE PROOF OF LEMMAS

* We deduce, from claim 8, that: $A = \{n \in \mathbb{N}^*, 1 \leq n \leq m\} = \{1, 2, \dots, m\}$ and $B = \{n \in \mathbb{N}^*, n \geq m + 1\} = \{m + 1, m + 2, \dots\}$

*So, by the Euler-Gauss theorem: $3 \in B \Rightarrow 3 \geq m + 1 \Rightarrow m \leq 2$

*But, by the assertion (1) of lemma7: $m \geq 2$

*That is, finally: $m = 2$.

Conclusion: we have showed that $A = \{1, 2\}$ and, so, that the last Fermat theorem is true.

Remark: I want here to give little amelioration to the references [5] and [6].

The reference [5]: replace in pp 7-8 the under-claim2 and its proof by the following new under-claim2 and its proof:

Under-claim2: Let $n \in \mathbb{N}^* - \{1\}$, $a, b \in \mathbb{P}_{2n}$, $p, q \in \mathbb{P}_{2(n+1)}$ and $k, r \in \mathbb{N}^*$

(1) $\exists \delta(r, k) \in]0, 1[$ Such that:

$$(\delta(r, k))^{\delta(r, k) + \frac{1}{r}}(|2(n + 1) - a - b| + \frac{1}{k}) = (1 - \delta(r, k))^{1 - \delta(r, k) + \frac{1}{r}}(|2n - p - q| + \frac{1}{k})$$

(2) $\exists \delta(k) \in [0,1]$ Such that:

$$\delta(k)^{\delta(k)}(|2(n+1) - a - b| + \frac{1}{k}) = (1 - \delta(k))^{1-\delta(k)}(|2n - p - q| + \frac{1}{k})$$

(3) $\exists \delta \in [0,1]$ Satisfying: $\delta^\delta \neq 0$ and $(1 - \delta)^{1-\delta} \neq 0$ such that:

$$\delta^\delta(|2(n+1) - a - b|) = (1 - \delta)^{1-\delta}(|2n - p - q|)$$

(4) $C = B$

Proof: (of the under-claim2)

(1) The result is obtained by applying the intermediate value theorem on $[0, 1]$ to the continuous function:

$$f(t) = t^{t+\frac{1}{r}}(|2(n+1) - a - b| + \frac{1}{k}) - (1-t)^{1-t+\frac{1}{r}}(|2n - p - q| + \frac{1}{k})$$

Having:

$$f(0) = -(|2n - p - q| + \frac{1}{k}) < 0 \text{ And } f(1) = (|2(n+1) - a - b| + \frac{1}{k}) > 0$$

(2) The result is obtained, using the Bolzano-Weierstrass theorem, by tending $r \rightarrow +\infty$ in the relation (1) of under-claim2.

(3)* The result is obtained, using the Bolzano-Weierstrass theorem, by tending $k \rightarrow +\infty$ in the relation (2) of under-claim2.

* $\delta \in [0,1] \Rightarrow \delta^\delta \neq 0$ and $(1 - \delta)^{1-\delta} \neq 0$ (because $0^0 = 1$)

(4)* By the assertion (3), we have:

$\forall n$ integer such that: $0 \leq n \leq m - 2: n \in C \Rightarrow n + 1 \in C$

*That is: $C = B$

The reference [6]: replace, in pp 39-40, the under-claim2 and its proof by the below new under-claim2 and its proof:

Under-claim2: Let $n \in \mathbb{N}, p, q \in \mathbb{P}$ and $k, r \in \mathbb{N}^*$

(1) $\exists \delta(r, k) \in]0,1[$ Such that:

$$(\delta(r, k))^{\delta(r, k)+\frac{1}{r}}(|n + 1 - [\sqrt{p}]| + \frac{1}{k}) = (1 - \delta(r, k))^{1-\delta(r, k)+\frac{1}{r}}(|n - [\sqrt{q}]| + \frac{1}{k})$$

(2) $\exists \delta(k) \in [0,1]$ Such that:

$$\delta(k)^{\delta(k)}(|n + 1 - [\sqrt{p}]| + \frac{1}{k}) = (1 - \delta(k))^{1-\delta(k)}(|n - [\sqrt{q}]| + \frac{1}{k})$$

(3) $\exists \delta \in [0,1]$ Satisfying: $\delta^\delta \neq 0$ and $(1 - \delta)^{1-\delta} \neq 0$ such that:

$$\delta^\delta(|n + 1 - [\sqrt{p}]|) = (1 - \delta)^{1-\delta}(|n - [\sqrt{q}]|)$$

(4) $C = B$

Proof: (of the under-claim2)

(1) The result is obtained by applying the intermediate value theorem on $[0,1]$ to the continuous function:

$$f(t) = t^{t+\frac{1}{r}}(|n + 1 - [\sqrt{p}]| + \frac{1}{k}) - (1-t)^{1-t+\frac{1}{r}}(|n - [\sqrt{q}]| + \frac{1}{k})$$

Having:

$$f(0) = -(|2n - p - q| + \frac{1}{k}) < 0 \text{ And } f(1) = (|2(n+1) - a - b| + \frac{1}{k}) > 0$$

(2) The result is obtained, using the Bolzano-Weierstrass theorem, by tending $r \rightarrow +\infty$ in the relation (1) of under-claim2.

(3)* The result is obtained, using the Bolzano-Weierstrass theorem, by tending $k \rightarrow +\infty$ in the relation (2) of under-claim2.

* $\delta \in [0,1] \Rightarrow \delta^\delta \neq 0$ and $(1 - \delta)^{1-\delta} \neq 0$ (because $0^0 = 1$)

(4)* By the assertion (3), we have:

$\forall n$ integer such that: $0 \leq n \leq m - 2: n \in C \Rightarrow n + 1 \in C$

*That is: $C = B$

REFERENCES

- [1] Diophante d'Alexandrie (1621): Diophanti Alexandrini rarum arithmeticarum libri. Latin translation of the Diophante Grec work by Claude Gaspard Bachet De Méziriac. Available at: <https://gallica.bnf.fr/ak:/12148/bpt6k648679/> (Accessed on July 28, 2018)
- [2] Euclid (1966): les éléments T1 (livres I-VII), T2 (livres VIII-X), T3 (livres XI-XIII). In les œuvres d'Euclide. French Translation of the Euclid Grec work by F. Peyard. Blanchard. Paris. Available at: <https://archive.org/details/lesuvresd'euclide03eucl/> (Accessed on July 28, 2018)

- [3] Euler, L (1770): Vollständige Anlectung Zur Algebra. Available at: <https://rotichitropark.firebaseio.com/1421204266.pdf/> (Accessed on July 28, 2018)
- [4] Gauss, C.F: Neue theorie de zeregung der cuben; In C. F Gauss werke, Vol II, pp 383-390 Available at: archive.wikiwix.com/cache/?url=http%3A%2F%2Fgdz.sub.uni-goettingen.de%2Fdms%2Fload%2Fimg%2F%3FPPN%3DPPN23599524X%26DMDiD%3DDMDLOG_0057%26LOGRD... (Accessed on: July 28, 2018)
- [5] Ghanim, M (10/5/2018): Confirmation of the Goldbach binary conjecture. GJAETS. India, the 5(5) May 2018 issue Available at: <http://www.gjaets.com/> (Accessed on May 28, 2018)
- [6] Ghanim, M (10/8/2018): Confirmation of the Catalan and the Euler conjectures. GJAETS. India. The 5(8) August 2018 issue. Available at: <http://www.gjaets.com/> (Accessed on August 30, 2018)
- [7] Mehl, serge: grand theorem de Fermat, n=3. Available at: serge.mehl.free.fr/anx/th_fermat_gd3.html/ (Accessed on: July 28, 2018)
- [8] Singh, Simon (13/07/2011): Le dernier théorème de Fermat (En 312 pages). Collection Pluriel. Editions Pluriel, Paris. Available at: <https://www.Fayard.fr/pluriel/le-dernier-theoreme-de-fermat-9782818502037> (Accessed on October 29, 2018)
- [9] Wikipedia: Dernier théorème de Fermat. Available at: https://fr.wikipedia.org/wiki/Dernier_theoreme_de_Fermat/ (Accessed on October 29, 2018)
- [10] Wikipedia (2016): théorème de Sophie-Germain. Available at: https://fr.wikipedia.org/wiki/Theoreme_de_Sophie_Germain/ (Accessed on November 30, 2018)
- [11] Wikipedia (2018): théorème de Bolzano-Weierstrass. Available at: https://fr.wikipedia.org/wiki/Theoreme_de_Bolzano-Weierstrass/ (Accessed on November 30, 2018)
- [12] Wikipedia (2018): théorème des valeurs intermédiaires. Available at: https://fr.wikipedia.org/wiki/Theoreme_de_valeurs_intermediaires/ (Accessed on November 30, 2018)
- [13] Wiles, Andrew (1995): Modular elliptic curves and Fermat's last theorem, Annals of Mathematics, 142, 443-551. Available at: <http://math.stanford.edu/~lekheng/FLT/wiles.pdf> (Accessed on: July 28, 2018)