

THE SOLUTION OF FERMAT EQUATION IN THE RATIONAL POINTS OF THE UNITARY CIRCUMFERENCE

B. Martín Cerna Maguiña

Department of Mathematics

National University of “Santiago Antúnez de Mayolo”
Campus Shancayan, Av. Centenario 200, Huaraz, PERÚ

Abstract: In this work we resolve the Fermat equation over rational points in the unitary circumference. For this we take a point (p_0, q_0) in the unitary circumference $x^2 + y^2 = 1$, where $p_0, q_0 \in \mathbb{Q}$ or $q_0 \in \mathbb{I}$ and $p_0 \in \mathbb{I}$. Then the straight line $y = q_0$ intersects the curve $x^d + y^d = 1$, in the point (p_1, q_0) we demonstrated that p_1 is an irrational number.

AMS Subject Classification: 11A41, 11D41

Key Words: primes, Fermat’s equations, Diophantine equations

1. Introduction

We know that Fermat’s equation is $a^n + b^n = c^n$, this doesn’t have different integer solution of the trivial for $a, b, c, n \in \mathbb{Z}^+$ and $n \geq 3$, it was solved for the English Mathematician Andrew Wile in 1996; I listened that this only was possible using a technique of extremely difficult for its comprehension. Motivated by these comments, I took the decision investigate, so I discovered a simple technique that can help solve the general case.

The used technique, consist in the following, We took a point in the Cartesian plane whose coordinates are (p_0, q_0) in the unitary circumference, where $p_0, q_0 \in \mathbb{Q}$ or $q_0 \in \mathbb{Q}$ and $p_0 \in \mathbb{I}$, then we get $p_0^2 + q_0^2 = 1$, these points are known as

$$p_0 = \frac{2t_0}{1+t_0^2}, \quad q_0 = \frac{1-t_0^2}{1+t_0^2},$$

here note that $p_0, q_0 \in \mathbb{Q}^+$ if and only if $t_0 \in \mathbb{Q}^+, t_0 \in [0, 1]$, if $q_0 \in \mathbb{Q}^+$ and $p_0 \in \mathbb{I}^+$ then $t_0^2 \in \mathbb{Q}^+$.

The straight line $y = q_0$, in the first quadrant intersects the curve $x^d + y^d = 1$ in the point (p_1, q_0) , then we have the following equation $p_1^d + q_0^d = 1$.

From the last equation we demonstrate that p_1 never is a rational number. So it is important to note that (p_0, q_0) also can be written as:

$$q_0 = \frac{2t_1}{1+t_1^2}, \quad p_0 = \frac{1-t_1^2}{1+t_1^2}$$

where the relation between t_0, t_1 is $t_0 = \frac{1-t_1}{1+t_1}$.

Let us introduce the notations used in this work: \mathbb{Z}^+ represents the set of positive integer numbers, \mathbb{Q} represents the set rational numbers, \mathbb{I} represents the set of irrational numbers.

2. Fermat Had Reason

Theorem 1. *Let $a, b, c, d \in \mathbb{Z}^+$ the equation $a^d + b^d = c^d$ does not have integer solution different of the trivial.*

Proof. This theorem is equivalent to prove the following $p^d + q^d = 1$ it does not have rational solution para $p, q \in \mathbb{Q} \cap [0, 1]$. So we take (p_0, q_0) a point in the unitary circumference. Then following cases happens:

I) $p_0, q_0 \in \mathbb{Q}$ and satisfies the equation $p_0^2 + q_0^2 = 1$, where

$$p_0 = \frac{2t_0}{1+t_0^2} = \frac{1-t_1^2}{1+t_1^2} \text{ and } q_0 = \frac{1-t_0^2}{1+t_0^2} = \frac{2t_1}{1+t_1^2} \quad (1)$$

Clearly $t_0, t_1 \in \mathbb{Q}$ and t_0, t_1 are related by the following equation

$$t_0 = \frac{1-t_1}{1+t_1} \quad (2)$$

Let $t_0 = \frac{m}{n}, t_1 = \frac{m_1}{n_1}$, where $m, n, m_1, n_1 \in \mathbb{Z}^+$ and m, n are relative primes.

The same way m_1, n_1 are relative primes and satisfies the relation $m < n, m_1 < n_1$.

From (2) we have

$$t_0 = \frac{m}{n} = \frac{n_1 - m_1}{n_1 + m_1} \tag{3}$$

The line $y = q_0$ intersects the curve $x^d + y^d = 1$ in the point (p_1, q_0) , therefore this point satisfies the following :

$$p_1^d + q_0^d = 1 \tag{4}$$

From the relation (1) ,(3) and (4) we have:

$$p_1 = \frac{\sqrt[d]{(m^2 + n^2)^d - (n^2 - m^2)^d}}{n^2 + m^2} = \frac{\sqrt[d]{(n_1^2 + m_1^2)^d - (2n_1m_1)^d}}{n_1^2 + m_1^2} \tag{5}$$

Supposing that $p_1 \in \mathbb{Q}$ from the relation (4) and (5) we have the equation

$$A^d + (2n_1m_1)^d = (n_1^2 + m_1^2)^d \tag{6}$$

If $A = n_1^2 + m_1^2 - j, j = 1, 2, \dots, n_1^2 + m_1^2 - 1$, we have

$$(n_1^2 + m_1^2 - j)^d + (2n_1m_1)^d = (n_1^2 + m_1^2)^d$$

don't have a solution, for all $n_1, m_1, d \in \mathbb{N}$ and $\forall j$ odd number.

Therefore

$$(n_1^2 + m_1^2 - j)^d + (2n_1m_1)^d > (n_1^2 + m_1^2)^d \tag{7}$$

or

$$(n_1^2 + m_1^2 - j)^d + (2n_1m_1)^d < (n_1^2 + m_1^2)^d \tag{8}$$

Then We supposing that exists j_0 even number such that (6) have a solution

$$(n_1^2 + m_1^2 - j_0)^d + (2n_1m_1)^d = (n_1^2 + m_1^2)^d \tag{9}$$

From the relation (9) and (7) we have

$$(n_1^2 + m_1^2 - j)^d > (n_1^2 + m_1^2 - j_0)^d,$$

if d is an odd number we have

$$-j > -j_0 \Rightarrow j_0 > j, \forall j \text{ odd number.}$$

Then $j_0 = n_1^2 + m_1^2 - 1$, if n_1 is an odd number and m_1 is an even number or viceversa. This relation and (9) is

$$1^d + (2n_1m_1)^d = (n_1^2 + m_1^2)^d$$

which don't have an integer solution.

From the relation (8) and (9), we have

$$(n_1^2 + m_1^2 - j)^d < (n_1^2 + m_1^2 - j_0)^d,$$

therefore, if d is an odd number

$$j_0 < j, \forall j \text{ odd number,}$$

for $j = 1$, we have that j_0 doesn't exist.

When d is a even number the analysis is the same

II) If $q_0 \in \mathbb{Q}$ and $p_0 \in \mathbb{I}$. We have

$$p_0^d + (n - m)^d = (n + m)^d,$$

for $B = n + m - j, j = 1, 2, \dots, n + m - 1$, we have

$$(n + m - j)^d + (n - m)^d = (n + m)^d, \quad (10)$$

for $j = n + m - k$ on (10), we have

$$k^d + (n - m)^d = (n + m)^d \quad (11)$$

If k is an odd number, then (11) don't have a solution for every $n, m \in \mathbb{N}$ and $\forall k$ odd number. by analogy with the item (I), We have that (11) only has a solution if

$$(n + m - 1)^d + (n - m)^d = (n + m)^d \quad (12)$$

where n is odd and m is even number.

□

Theorem 2. For $d = 4$ the equation (12) doesn't solution

Proof. Suppose that (12) have a solution

$$(n + m - 1)^4 = (n + m)^4 - (n - m)^4$$

$$(n + m - 1)^4 = 8nm(n^2 + m^2); n \text{ is odd and } m \text{ is even} \quad (13)$$

We have $n^2 + m^2 = c^2, c \in \mathbb{N}$ then

$$n = u^2 - v^2, m = 2uv, c = u^2 + v^2 \quad (14)$$

Therefore u and v have a square root exact. Furthermore n has a square root exact and $n = (u - v)(u + v)$ then $u = A^2, v = B^2; A, B \in \mathbb{N}$. Hence

$$\begin{cases} A^2 - B^2 = \tau^2, \tau \in \mathbb{N} \\ A^2 + B^2 = \lambda^2, \lambda \in \mathbb{N} \end{cases} \quad (15)$$

Then (15) don't have an integer solution □

Acknowledgments

The author thanks Victor Pocoy Y. for the reading the manuscript.

References

- [1] Pierre Samuel, *Thorie Algbrique des Nombres*, Hermann Editeurs Des Sciences Et Des Arts. Francia (1921).

