THE END OF FLT

Leszek W. Guła

Lublin-POLAND

yethi@wp.pl

29 – 30 May 2017

Abstract

1. The proper proof of The Fermat's Last Theorem (FLT).

2. The proof of the theorem - *For all* $n \in \{3,5,7,...\}$ *and for all* $z \in \{3,7,11,...\}$ *and for all natural numbers* u, v: $z^n \neq u^2 + v^2$.

MSC:

Primary: 11D41; Secondary: 11D45.

Keywords

Diophantine Equations, Fermat Equation, Greatest Common Divisor, Newton Binomial Formula.

Dedicatory

Dedicated to my Parents and my Brother

I. INTRODUCTION

The cover of this issue of the Bulletin is the frontispiece to a volume of Samuel de Fermat's 1670 edition of Bachet's Latin translation of Diophantus's Arithmetica. This edition includes the marginalia of the editor's father, Pierre de Fermat. Among these notes one finds the elder Fermat's extraordinary comment in connection with the Pythagorean equation $x^2 + y^2 = z^2$ the marginal comment that hints at the existence of a proof (a demonstratio sane mirabilis) of what has come to be known as Fermat's Last Theorem. Diophantus's work had fired the imagination of the Italian Renaissance mathematician Rafael Bombelli, as it inspired Fermat a century later. [5]

Problem II.8 of the Diophantus's Arithmetica asks how a given square number is split into two other squares. Diophantus's shows how to solve this sum-of-squares problem for 4^2. [2]

It is easy to verify how get the primitive (x, y, z must be are coprime) Pythagorean triple (x, y, z) because – For all relatively prime natural numbers u, v such that $u - v \in \{1,3,5,...\}$:

$$1 = \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 \Rightarrow 4^2 = \left[\frac{4(2^2-1)}{2^2+1}\right]^2 + \left(\frac{4 \cdot 2 \cdot 2 \cdot 1}{2^2+1}\right)^2 \Rightarrow$$

$$(u^2+v^2)^2 = (u^2-v^2)^2 + (2uv)^2 \Rightarrow (u^2-v^2, 2uv,\ u^2+v^2) = (x, y, z)\,.$$

Around 1637, Fermat wrote his Last Theorem in the margin of his copy of the Arithmetica next to Diophantus sum-of-squares problem: it is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain. In number theory, Fermat's Last Theorem (FLT) states that no three positive integers $A, B,$ and C satisfy the equation $A^n + B^n = C^n$ for any integer value of n greater than two. [2]

It is easy to see that if $A^n + B^n = C^n$ then either $A, B,$ and C are co-prime or, if not co-prime that any common factor could be divided out of each term until the equation existed with co-prime bases. (Co-prime is synonymous with pairwise relatively prime and means that in a given set of numbers, no two of the numbers share a common factor). [1]

You could then restate FLT by saying that $A^n + B^n = C^n$ is impossible with co-prime bases. (Yes, it is also impossible without co-prime bases, but non co-prime bases can only exist as a consequence of co-prime bases). [1]

It is known that for some co-prime $x, y, z \in \{3,4,5, \dots\}$:

$$[x^2 + y^2 = z^2 \ \wedge \ (x+y)^2 + (x-y)^2 = 2z^2], \qquad (1)$$

where z is odd because for all $a, b \in \{0,1,2, \dots\}$: the number $\frac{(2a+1)^2+(2b+1)^2}{2}$ is odd.

II. THE PROPER PROOF OF FLT

Theorem 1 (FLT). *For all* $n \in \{3,4,5, \dots\}$ *and for all* $A, B, C \in \{1,2,3, \dots\}$ *the equation*

$$A^n + B^n = C^n$$

has no primitive solutions $[A, B, C]$ *in* $\{1,2,3, \dots\}$.

Proof. Every even number which is not the power of number 2 has odd prime divisor, hence sufficient that we prove FLT for $n = 4$ and for odd prime numbers $n \in \mathbb{P}$. [6]

Suppose that for $n = 4$ or for some $n \in \mathbb{P}$ and for some coprime $A, B, C \in \{1,2,3, \dots\}$:

$$A^n + B^n = C^n.$$

Then only one number out of (A, B, C) is even and the number $A + B - C$ is positive and even.

Proof (Proper Proof For $n = 4$). Suppose that the equation

$$A^4 + B^4 = C^4$$

has primitive solutions $[A, B, C]$ in $\{1,2,3, \dots\}$. [3] and [4] Then $A, B,$ and C are coprime.

Without loss for the proof we can assume that B is even in view of (1).

For some $C, A \in \{1,3,5, \dots\}$ and for some $B \in \{4,6,8, \dots\}$:

$$(C - A + A)^4 - A^4 = B^4 \Longrightarrow (C-A)^3 + 4(C-A)^2A + 6(C-A)A^2 + 4A^3 = \frac{B^4}{C-A}.$$

Notice that

$$(C-A)^3 + 4(C-A)^2A + 6(C-A)A^2 + 4A^3 = \frac{C^4 - A^4}{C-A} = \frac{(C^2+A^2)(C+A)(C-A)}{C-A}.$$

For some $k \in \{1,2,3,...\}$ and for some $e, c, d \in \{1,3,5,...\}$ such that e, c and d are co-prime:

$$\frac{(2^k ecd)^4}{C-A} = \frac{(2^k ecd)^4}{2^{4k-2}d^4} = 4(ec)^4 = \frac{B^4}{C-A}.$$

Therefore – For some relatively prime $e, c \in \{1,3,5,...\}$ such that $e > c$:

$$4(ec)^4 = (C^2 + A^2)(C + A) \Longrightarrow (C^2 + A^2 = 2e^4 \;\wedge\; C + A = 2c^4) \Longrightarrow$$

$$\begin{aligned}(C = x + y \;\wedge\; A = x - y \;\wedge\; C + A = 2x = 2c^4 \wedge\; x = c^4 \;\wedge\; x^2 + y^2 = e^4 \;\wedge\; x = c^4 \\ = u^2 - v^2 \;\wedge\; y = 2uv \;\wedge\; e^2 = u^2 + v^2 \;\wedge\; e = p^2 + q^2 \;\wedge\; u = p^2 - q^2 \wedge v \\ = 2pq) \\ \Longrightarrow \{x = [(p^2 - q^2)^2 - (2pq)^2] = (c^2)^2 \in \mathbf{0} \;\wedge\; y \\ = 4(p^2 - q^2)pq \;\wedge\; x^2 + y^2 \\ = [(p^2 - q^2)^2 - (2pq)^2]^2 + 16(p^2 - q^2)^2(pq)^2 = (p^2 + q^2)^4 = e^4 \in \mathbf{1}\} \\ \in \mathbf{0},\end{aligned}$$

inasmuch as on the strength of the Guła's Theorem [3] we have

$$(2pq)^2 = (p^2 - q^2)^2 - (c^2)^2 \Longrightarrow p^2 - q^2 = \frac{(2pq)^2 + (2q^2)^2}{2(2q^2)} = p^2 + q^2 \in \mathbf{0}.$$

This is the proof. The proper proof for $n \in \mathbb{P}$ we have in [4].

III. THE PROOF OF - For odd $n > 1$ and for all $z \in \{3,7,11,...\}$ for all $u, v \in \mathbb{N}$: $z^n \neq u^2 + v^2$.

Theorem 2. *For all* $n \in \{3,5,7,...\}$ *and for all* $z \in \{3,7,11,...\}$ *the equation*

$$z^n = u^2 + v^2$$

has no primitive solutions $[z, u, v]$ *in* $\{1,2,3,...\}$.

Proof. Suppose that for some $n \in \{3,5,7,...\}$ and for some $z \in \{3,7,11,...\}$ the equation

$$z^n = u^2 + v^2$$

has primitive solutions $[z, u, v]$ in $\{1,2,3,...\}$. Then $z, u,$ and v are co-prime and $u - v$ is odd.

Without loss for the proof we can assume that $u > v$.

On the strength of the Guła's Theorem [3] we get

$$\mathrm{Lside} = \left(\frac{z^n + d^2}{2d}\right)^2 = u^2 + \left(\frac{z^n - d^2}{2d}\right)^2 + v^2 = \mathrm{Rside} \in \mathbf{0}$$

inasmuch as $4 \mid \mathrm{Lside}$ and $4 \nmid \mathrm{Rside}$ because the numbers $u, \frac{z^n - 1}{2}$ are odd or $v, \frac{z^n - 1}{2}$ are odd.

$$even\;\; \frac{z^n + d^2}{2d} = \frac{2m + 1 + 4s + 1}{2d} = \frac{2(m + 2s) + 2}{2d} = \frac{(m + 2s) + 1}{d},$$

where the numbers d, m are positive and odd and $s \in \{0,1,2,...\}$.

This is the proof.

Golden Nyambuya proved (allegedly) the theorem – For all $n \in \{3,5,7,\dots\}$ the equation

$$z^n = u^2 + v^2$$

has no primitive solutions in $\{1,2,3,\dots\}$ with $z \in \{3,5,7,\dots\} - \{3^2,5^2,7^2,\dots\}$. [7]

Corollary 1. For some $n \in \{3,5,7,\dots\}$ and for some $z \in \{5,9,13,\dots\}$ and for some prime natural numbers u, v such that $u - v$ is positive and odd:

$$z^n = u^2 + v^2 \Longrightarrow (z^n)^2 = (u^2 + v^2)^2 = (u^2 - v^2)^2 + (2uv)^2.$$

This is the Corollary 1.

Example 1.

$$(5^3)^2 = (11^2 + 2^2)^2 = 117^2 + 44^2,$$

where $117 = 11^2 - 2^2 = u^2 - v^2$ and $44 = 2 \cdot 11 \cdot 2 = 2uv$.

This is the Example 1.

Example 2.

$$(17^3)^2 = (52^2 + 47^2)^2 = 495^2 + 4888^2,$$

where $495 = 52^2 - 47^2 = u^2 - v^2$ and $4888 = 2 \cdot 52 \cdot 47 = 2uv$.

This is the Example 2.

Example 3.

$$(29^3)^2 = (145^2 + 58^2)^2 = 17661^2 + 16820^2,$$

where $17661 = 145^2 - 58^2 = u^2 - v^2$ and $16820 = 2 \cdot 145 \cdot 58 = 2uv$.

This is the Example 3.

Example 4.

$$(41^3)^2 = (205^2 + 164^2)^2 = 15129^2 + 67240^2,$$

where $15129 = 205^2 - 164^2$ and $67240 = 2 \cdot 205 \cdot 164$.

This is the Example 4.

Example 5.

$$(13^5)^2 = (597^2 + 122^2)^2 = 341525^2 + 145668^2,$$

where $341525 = 597^2 - 122^2$ and $145668 = 2 \cdot 597 \cdot 122$.

This is the Example 5.

Theorem 3. *For all* $n \in \{1,2,3,\dots\}$ *and for all* $m \in \{3,5,7,\dots\}$ *and for some* $p,q \in \{1,2,3,\dots\}$ *such that* $p > q$:

$$[m^n = p^2 - q^2 \wedge (p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2].$$

Theorem 4. *For all* $n \in \{1,2,3,\dots\}$ *and for all* $m \in \{2,4,6,\dots\}$ *and for some* $p,q \in \{1,2,3,\dots\}$ *such that the number* $\frac{m^n}{2}$ *is even and bigger than two and* $p > q$:

$$[m^n = p^2 - q^2 \wedge (p^2 - q^2)^2 + (2pq)^2 = (p^2 + q^2)^2].$$

SUPPLEMENT

Let $\boldsymbol{gcd}(U,V) = \boldsymbol{gcd}(u,v) = 1$ and $U - V,\ u - v \in \{1,3,5,\dots\}$.

If

$$[U^2 - V^2 = A^2 \wedge 2UV = B^2 \wedge U^2 + V^2 = C^2 \wedge (A^2)^2 + (B^2)^2 = (C^2)^2],$$

then on the strength of the Guła's Theorem [3] we get

$$[V^2 = (2uv)^2 = U^2 - A^2 = C^2 - U^2 \wedge U = u^2 + v^2 \wedge u^2 - v^2 = A] \Longrightarrow$$

$$\left[C = \frac{(2uv)^2 + 2^2}{2 \cdot 2} = (uv)^2 + 1 \wedge u^2 + v^2 = U = \frac{(2uv)^2 - 2^2}{2 \cdot 2} = (uv)^2 - 1\right] \in \mathbf{0}. \clubsuit$$

It's not true in [7] that FLT for $n = 4$ can be written equivalently as: $A^2 = C^4 - B^4$ because Fermat did not proved his own theorem for $n = 4$. [6]

In the first case we will have – If

$$[2UV = A \wedge U^2 - V^2 = B^2 \wedge U^2 + V^2 = C^2 \wedge A^2 + (B^2)^2 = (C^2)^2],$$

then on the strength of the Guła's Theorem [3] we get

$$[V^2 = (2uv)^2 = U^2 - B^2 = C^2 - U^2 \wedge U = u^2 + v^2 \wedge u^2 - v^2 = B] \Longrightarrow$$

$$\left[C = \frac{(2uv)^2 + 2^2}{2 \cdot 2} = (uv)^2 + 1 \wedge u^2 + v^2 = U = \frac{(2uv)^2 - 2^2}{2 \cdot 2} = (uv)^2 - 1\right] \in \mathbf{0}. \clubsuit$$

In the second case we have

$$\begin{aligned}[U^2 - V^2 = A \wedge 2UV = B^2 \wedge U^2 + V^2 = C^2 \wedge (U+V)^2(U-V)^2 &= (C^2)^2 - (B^2)^2 \\ = (C^2 + B^2)(C^2 - B^2) \wedge (U+V)^2 = C^2 + B^2 \wedge (U-V)^2 & \\ = C^2 - B^2 \wedge U + V = u^2 + v^2 \wedge u^2 - v^2 = C \wedge 2uv = B] &\Longrightarrow\end{aligned}$$

$$2UV = (2uv)^2 \Longrightarrow UV = 2u^2v^2 \Longrightarrow (U = u^2 \wedge V = 2v^2) \Longrightarrow U + V = u^2 + 2v^2,$$

which is inconsistent with $U + V = u^2 + v^2$. $\clubsuit$

REFERENCES

[1]. N.N.: The Beal Cojecture, p. 1 – http://www.bealconjecture.com

[2]. En. Wikipedia – http://en.wikipedia.org/wiki/Fermat's_Last_Theorem

[3]. Guła, L. W.: Disproof the Birch and Swinnerton-Dyer Conjecture, American Journal of Educational Research, **Volume 4**, No 7, 2016, pp 504-506, doi: 10.12691/education-4-7-1 | Original Article electronically published on May 3, 2016 – http://pubs.sciepub.com/EDUCATION/4/7/1/index.html

[4]. Guła, L. W.: Several Treasures of the Queen of Mathematics, International Journal of Emerging Technology and Advanced Engineering, **Volume 6**, Issue 1, January 2016, pp 50-51 – http://www.ijetae.com/files/Volume6Issue1/IJETAE_0116_09.pdf

[5]. Mazur, B.: Mathematical Perspectivies, Bulletin (New Series) of The American Mathematical Society, **Volume 43**, Number 3, July 2006, p. 399, Article electronically published on May 9, 2006 –

http://www.ams.org/journals/bull/2006-43-03/S0273-0979-06-01123-2/S0273-0979-06-01123-2.pdf

[6]. Narkiewicz, W.: Wiadomości Matematyczne XXX.1, Annuals PTM, **Series II**, Warszawa 1993, p. 3

[7]. Nyambuya, G. G.: On a Simpler, Much More General and Truly Marvellous Proof of Fermat's Last Theprem (II), Department of Applied Physics, National University of Science and Technology, Bulawayo, Republic of Zimbabwe, Preprint submitted to **viXra.org Version 3** - September 24, 2014, pp 6-12, – http://www.rxiv.org/pdf/1405.0023v3.pdf