

The Surprising Proofs

By Leszek W. Gula

Lublin-POLAND

lwgula@wp.pl

May 30, 2017

Abstract. The proof of the Fermat's Last Theorem. The proof of the theorem - *For all $n \in \{3,5,7, \dots\}$ and for all $z \in \{3,7,11, \dots\}$ and for all natural numbers u, v : $z^n \neq u^2 + v^2$.* The proof of the Goldbach's Conjecture.

MSC. Primary: 11A41, 11D41, 11P32; Secondary: 11D45, 11D61.

Keywords. ABC Conjecture, Algebra of Sets, Diophantine Equations, Exponential Equations, Fermat Equation, Goldbach Conjecture, Greatest Common Divisor, Newton Binomial Formula, Trinomial Square.

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]

The Goldbach's Conjecture is one of the oldest and best-known unsolved problems in number theory and all of mathematics. It states: Every even integer greater than 2 can be expressed as the sum of two primes. [1]

II. THE PROOF OF THE FERMAT'S LAST THEOREM

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

Proof. Suppose that for some $n \in \{3,4,5, \dots\}$ and for some $A, B, C \in \{1,2,3, \dots\}$: $A^n + B^n = C^n$.

Then $(A + B > C \wedge A^2 + B^2 > C^2 \wedge \dots \wedge A^{n-1} + B^{n-1} > C^{n-1})$, otherwise $A^n + B^n < C^n$.

Thus for some $A, B, C, C - A, C - B, v \in \{1,2,3, \dots\}$:

$$A + B - C = A - (C - A) = B - (C - B) = 2v > 0 \implies$$

$$[(C - B) + 2v = A \wedge (C - A) + 2v = B \wedge A + B - 2v = C]. \quad (1)$$

At present we can assume for generality of below that A, B and C are coprime.

Moreover $[A^2 + B^2 > C^2 \wedge (1)] \implies 2v^2 > (C - A)(C - B)$.

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]

A. Proof For $n = 4$. Without loss for the proof we can assume that B is even.

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

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

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 $k \in \{1, 2, 3, \dots\}$ and for some coprime $e, c, d, h, m \in \{1, 3, 5, \dots\}$:

$$\left[\frac{B^4}{C - A} = \frac{(2^k ecd)^4}{2^{4k-2}d^4} = 4(ec)^4 \wedge h^4 = C - B \wedge 2^k d(2^{3k-2}d^3 + hm) = 2^k ecd = B \right].$$

Moreover – For some pairwise (mutually) relatively prime $d, h, m \in \{1, 3, 5, \dots\}$ such that $d < h < m$:

$$2v^2 > (C - A)(C - B) = 2^{4k-2}d^4h^4 \implies v^2 > 2^{4k-3}d^4h^4 \implies v = 2^{k-1}mhd.$$

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

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

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

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

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

This is the proof.

B. Proof For $n \in \mathbb{P}$. Without loss for the proof we can assume that A is odd and that $4 \nmid B, C$. [3], [4]

The numbers C, B and A are coprime, therefore in view of (2) we will have – For some $n \in \mathbb{P}$ and for some $C, B, C - A \in \{1, 2, 3, \dots\}$ and for some $C - B, A, v \in \{1, 3, 5, \dots\}$:

$$\begin{aligned} [(C - B + 2v)^n &= (C - B + B)^n - B^n \wedge (C - A + 2v)^n \\ &= (C - A + A)^n - A^n \wedge (A + B - B)^n + B^n = (A + B - 2v)^n] \Rightarrow \end{aligned}$$

$$\begin{aligned} &\left\{ (C - B)^{n-2}v + (n - 1)(C - B)^{n-3}v^2 + \dots + 2^{n-2}v^{n-1} + \frac{2^{n-1}v^n}{n(C - B)} \right. \\ &= \frac{B}{2} \left[(C - B)^{n-2} + \frac{n-1}{2}(C - B)^{n-3}B + \dots + B^{n-2} \right] \wedge (C - A)^{n-2}2v \\ &+ \frac{n-1}{2}(C - A)^{n-3}(2v)^2 + \dots + (2v)^{n-1} + \frac{(2v)^n}{n(C - A)} \\ &= A \left[(C - A)^{n-2} + \frac{n-1}{2}(C - A)^{n-3}A + \dots + A^{n-2} \right] \wedge (A + B)^{n-2}(-B) \\ &+ \frac{n-1}{2}(A + B)^{n-3}(-B)^2 + \dots + (-B)^{n-1} \\ &= (A + B)^{n-2}(-2v) + \frac{n-1}{2}(A + B)^{n-3}(-2v)^2 + \dots + (-2v)^{n-1} \\ &+ \frac{(-2v)^n}{n(A + B)} \wedge n \mid v \wedge (n \mid A, C - B \vee n \mid B, C - A \vee n \mid A + B, C) \left. \right\}. \end{aligned}$$

We assume that – For some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime

$$2v^2 > (C - A)(C - B) \Rightarrow (v = nemch \wedge n \nmid emch).$$

B. 1. Proof For Odd $A, B, C - B$, if $n \mid A, C - B$.

For some $n \in \mathbb{P}$ and for some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime:

$$\begin{aligned} (n^{n-1}c^n + 2nemch &= A \wedge h^n + 2nemch = B \wedge n^{n-1}c^n + h^n + 4nemch = 2^n m^n \\ &= A + B \wedge n^{n-1}c^n = C - B) \\ &\Rightarrow (2^n m^n - h^n = n^{n-1}c^n + 4nemch \wedge n \mid 2m - h \wedge n^2 \mid 2^n m^n - h^n) \\ &\Rightarrow n \mid emch, \end{aligned}$$

$$\begin{aligned} [n^{n-1}c^n + 2nemch &= A \wedge h^n + 2nemch = B \wedge n^{n-1}c^n + h^n + 4nemch = 2^n m^n \\ &= A + B \wedge n^{n-1}c^n = C - B] \\ &\Rightarrow [2^n m^n - h^n = n^{n-1}c^n + 4nemch \wedge n \mid 2m - h \wedge n^2 \mid 2^n m^n - h^n] \\ &\Rightarrow n \mid emch, \end{aligned}$$

which is inconsistent with $n \nmid emch$. ♠

B. 2. Proof For Odd $A, B, C - B$, if $n \mid B, C - A$.

For some $n \in \mathbb{P}$ and for some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime:

$$\begin{aligned} [c^n + 2nemch &= A \wedge n^{n-1}h^n + 2nemch = B \wedge c^n + n^{n-1}h^n + 4nemch = 2^n m^n \\ &= A + B \wedge c^n = C - B \wedge n^{n-1}h^n = C - A] \\ &\Rightarrow [2^n m^n - c^n = n^{n-1}h^n + 4nemch \wedge n \mid 2m - c \wedge n^2 \mid 2^n m^n - c^n] \\ &\Rightarrow n \mid emch, \end{aligned}$$

which is inconsistent with $n \nmid emch$. ♠

B. 3. Proof For Odd $A, B, C - B$, if $n \mid A + B, C$.

For some $n \in \mathbb{P}$ and for some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime:

$$[c^n + 2nemch = A \wedge h^n + 2nemch = B \wedge c^n + h^n + 4nemch = n^{n-1}2^nm^n = A + B \wedge c^n = C - B] \Rightarrow [n \mid c + h \wedge n^2 \mid c^n + h^n] \Rightarrow n \mid emch,$$

which is inconsistent with $n \nmid emch$. ♠

B. 4. Proof For Even $B, C - A$, if $n \mid A, C - B$.

For some $n \in \mathbb{P}$ and for some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime:

$$\begin{aligned} [n^{n-1}c^n + 2nemch = A \wedge 2^nh^n + 2nemch = B \wedge n^{n-1}c^n + 2^nh^n + 4nemch = m^n \\ = A + B \wedge 2^nh^n = C - A \wedge n^{n-1}c^n = C - B] \\ \Rightarrow [m^n - 2^nh^n = n^{n-1}c^n + 4nemch \wedge n \mid m - 2h \wedge n^2 \mid m^n - 2^nh^n] \\ \Rightarrow n \mid emch, \end{aligned}$$

which is inconsistent with $n \nmid emch$. ♠

B. 5. Proof For Even $B, C - A$, if $n \mid B, C - A$.

For some $n \in \mathbb{P}$ and for some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime:

$$\begin{aligned} [c^n + 2nemch = A \wedge n^{n-1}2^nh^n + 2nemch = B \wedge c^n + n^{n-1}h^n + 4nemch = m^n \\ = A + B \wedge c^n = C - B \wedge n^{n-1}2^nh^n = C - A] \\ \Rightarrow [2^nm^n - c^n = n^{n-1}h^n + 4nemch \wedge n \mid 2m - c \wedge n^2 \mid 2^nm^n - c^n] \\ \Rightarrow n \mid emch, \end{aligned}$$

which is inconsistent with $n \nmid emch$. ♠

B. 6. Proof For Even $B, C - A$, if $n \mid A + B, C$.

For some $n \in \mathbb{P}$ and for some $e, m, c, h \in \{1, 3, 5, \dots\}$ such that n, e, m, c and h are coprime:

$$[c^n + 2nemch = A \wedge 2^nh^n + 2nemch = B \wedge c^n + 2^nh^n + 4nemch = n^{n-1}m^n = A + B \wedge 2^nh^n = C - A] \Rightarrow [n \mid c + h \wedge n^2 \mid c^n + 2^nh^n] \Rightarrow n \mid emch,$$

which is inconsistent with $n \nmid emch$. ♠

Proof For $n \in \mathbb{P}$ In Special Case. For some $n \in \mathbb{P}$ and for some $p, q, w, r, x \in \{1, 3, 5, \dots\}$ and for some $C, A \in \{3^2, 5^2, 7^2, \dots\}$ such that $p > q$ and $w > r$ and p, q, w, r, x are coprime and $n \mid pq$: [3]

$$\left[\begin{aligned} (2pq)^n = B^n &= \left(C\frac{n}{2}\right)^2 - \left(A\frac{n}{2}\right)^2 \wedge C = (wr)^2 \wedge A = x^2 \wedge \frac{(2pq)^n + (x^2)^n}{2pq + x^2} \\ &= \frac{(2pq)^n + (x^2)^n}{(r^2)^n} = \frac{(w^2 r^2)^n}{(r^2)^n} = (w^2)^n \wedge (r^n)^2 - x^2 \\ &= 2pq \wedge (2 \mid pq \equiv 0) \end{aligned} \right] \in \mathbf{0}. \spadesuit$$

This is the proof.

III. THE PROOF OF THE GOLDBACH'S CONJECTURE

Conjecture 1 (Goldbach Conjecture). For all $Z \in \{6,8,10, \dots\}$ and for some $X, Y \in \mathbb{P}$:

$$Z = X + Y.$$

Proof.

$$\begin{aligned} \{6, 8, 10, \dots\} &= \{6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, \dots\} \cup \\ &\{8, 14, 20, 26, 32, 38, 44, 50, 56, 62, 68, 74, 80, 86, 92, 98, 104, 110, \dots\} \cup \\ &\{10, 16, 22, 28, 34, 40, 46, 52, 58, 64, 70, 76, 82, 88, 94, 100, 106, 112, \dots\}. \end{aligned}$$

Thus

$$\begin{aligned} &[3] \cup [9, 15, 21, 27, 33, 39, 45, 51, 57, 63, \dots] \cup \\ &[7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91, \dots] \cup \\ &[5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, 83, 89, 95, \dots] = [3, 5, 7, \dots]. \end{aligned}$$

Hence

$$\begin{aligned} \{6\} &= \{Z: Z = X + Y \wedge X = Y = 3\} \vee \{8\} = \{Z: Z = X + Y \wedge X = 3 \wedge Y = 5\} \vee \\ &\{14, 20, 26, \dots\} = \\ &\{Z: Z = X + Y \wedge X \leq Y \wedge X, Y \in \mathbb{P} \wedge X, Y \in [7, 13, 19, 25, 31, \dots]\} \vee \\ &\{10, 16, 22, \dots\} = \\ &\{Z: Z = X + Y \wedge X \leq Y \wedge X, Y \in \mathbb{P} \wedge X, Y \in [5, 11, 17, 23, 29, 35, \dots]\} \vee \\ &\{12, 18, 24, \dots\} = \\ &\{Z: Z = X + Y \wedge X, Y \in \mathbb{P} \wedge X \in [5, 11, 17, 23, 29, 35, \dots] \wedge Y \in [7, 13, 19, 25, 31, \dots]\}, \end{aligned}$$

whence it implies that for all $Z \in \{6, 8, 10, \dots\}$ and for some $X, Y \in \mathbb{P}$: $Z = X + Y$. [2], [3]

This is the proof.

SUPPLEMENT

Theorem 2. For each fixed pair (u, v) of the relatively prime natural numbers u and v such that $u - v$ is positive and odd there exists exactly one a primitive Pythagorean triple (x, y, z) such that $(u^2 - v^2, 2uv, u^2 + v^2) = (x, y, z)$ and conversely – Any the primitive Pythagorean triple (x, y, z) such that $(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$ arises exactly from one pair (u, v) of the relatively prime natural numbers u and v such that $u - v$ is positive and odd.

This is the theorem.

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

Suppose that for some $p, q, C \in \{1, 3, 5, \dots\}$ and for some $B \in \{2, 4, 6, \dots\}$ such that the numbers p, q, C and B are coprime and $q < p < C: (pq)^4 = C^2 - (B^2)^2$.

We assume that the number C is minimal.

On the strength of the Gula's Theorem [2] we obtain

$$\begin{aligned} B^2 = \frac{p^4 - q^4}{2} = \frac{p^2 + q^2}{2} (p^2 - q^2) &\Rightarrow \left(\frac{p^2 + q^2}{2} = w^2 \wedge p^2 - q^2 = r^2 \right) \Rightarrow w^2 = \frac{p^2 + q^2}{2} \\ &= \frac{(u^2 + v^2)^2 + (u^2 - v^2)^2}{2} = u^4 + v^4 \Rightarrow w < C, \end{aligned}$$

which is inconsistent with minimal C . ♣

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 Gula's Theorem [2] we get

$$\begin{aligned} [V^2 = (2uw)^2 = U^2 - A^2 = C^2 - U^2 \wedge U = u^2 + v^2 \wedge u^2 - v^2 = A] &\Rightarrow \\ \left[C = \frac{(2uw)^2 + 2^2}{2 \cdot 2} = (uw)^2 + 1 \wedge u^2 + v^2 = U = \frac{(2uw)^2 - 2^2}{2 \cdot 2} = (uw)^2 - 1 \right] &\in \mathbf{0}. \clubsuit \end{aligned}$$

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 Gula's Theorem [2] we get

$$\begin{aligned} [V^2 = (2uw)^2 = U^2 - B^2 = C^2 - U^2 \wedge U = u^2 + v^2 \wedge u^2 - v^2 = B] &\Rightarrow \\ \left[C = \frac{(2uw)^2 + 2^2}{2 \cdot 2} = (uw)^2 + 1 \wedge u^2 + v^2 = U = \frac{(2uw)^2 - 2^2}{2 \cdot 2} = (uw)^2 - 1 \right] &\in \mathbf{0}. \clubsuit \end{aligned}$$

In the second case we have

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

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

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

REFERENCES

- [1] En. Wikipedia – https://en.wikipedia.org/wiki/Goldbach%27s_conjecture
- [2]. 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>
- [3]. 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
- [4]. Guła, L. W.: The Truly Marvellous Proof, International Journal of Emerging Technology and Advanced Engineering, **Volume 2**, Issue 12, December 2012, pp 96-97 – http://www.ijetae.com/files/Volume2Issue12/IJETAE_1212_14.pdf
- [5]. Mazur, B.: Mathematical Perspectives, 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, Annals 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 Theorem (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>