

# PRAWDZIWIE CUDOWNY DOWÓD

LESZEK W. GULA

*Pracę Dedykuję Moim Rodzicom i Mojemu Bratu*

ABSTRACT. Elementarny dowód Wielkiego Twierdzenia Fermata.

## I. WSTĘP

Diofantosa interesowały rozwiązania równań w  $\mathbb{Q}$ . Obecnie równania diofantyczne rozwiązuje się w  $\mathbb{Z}$ . Oto zadanie 8 z drugiej księgi *Arytmetyki Diofantosa*:

'Dany kwadrat rozłożyć na [sumę] dwa kwadraty.'

Rozwiązanie ilustruje wzór – dla każdego  $a, u \in \mathbb{Z}$ :

$$(1) \quad a^2 = \left( \frac{2au}{u^2 + 1} \right)^2 + \left[ \frac{a(u^2 - 1)}{u^2 + 1} \right]^2.$$

W tym właśnie miejscu, tj. na marginesie strony egzemplarza księgi p.t. *Arytmetyka Diofantosa*, łacińskiego przekładu Bacheta, edycji z roku 1670, którego właścicielem był Samuel de Fermat, jest odtworzony następujący dopisek Pierre de Fermata (1665):

*Nie można rozłożyć ani sześciannu na [sumę] dwa sześcianny, ani bikwadratu na [sumę] dwa bikwadraty, i w ogóle żadnej potęgi większej niż druga na [sumę] dwie potęgi z takim samym wykładnikiem. Odkryłem naprawdę zadziwiający dowód tego [faktu]. Margines jest na to za mały. [1] Istnieje także inne tłumaczenie drugiego zdania Fermata: 'Odkryłem prawdziwie cudowny dowód tego faktu, jednakże margines ten jest zbyt wąski, by go zmieścić.' Ten niezwykły komentarz starszego Fermata jest w związku z równaniem Pitagorasa i wskazuje na istnienie dowodu jako faktu (demonstratio sane mirabilis) na treść tegoż dopisku-twierdzenia. [3]*

## II. WIELKIE TWIERDZENIE FERMATA

**Twierdzenie 1.** Dla  $n, X, Y, Z \in \mathbb{N}_3$ :  $X^n + Y^n = Z^n$  nie ma rozwiązań właściwych.

*Dowód.* Niech istnieją  $n, X, Y, Z \in \mathbb{N}_3$ :  $X^n + Y^n = Z^n$  ma rozwiązania właściwe.

Wtedy  $X + Y > Z$  i  $X^2 + Y^2 > Z^2$  i ... i  $X^{n-1} + Y^{n-1} > Z^{n-1}$ , gdyż w przeciwnym razie  $X^n + Y^n < Z^n$ . Liczby  $X, Z - Y$  będą dodatnie i nieparzyste, liczba  $Z - X$  będzie dodatnia, a liczba  $X + Y - Z$  będzie dodatnia i parzysta.

Każda liczba parzysta niebędąca potęgą dwójki ma nieparzysty dzielnik pierwszy, przeto wystarczy udowodnić WTF dla  $n = 4$  i dla  $n$  będących liczbami pierwszymi większymi od dwóch. [4] Zbiór tych liczb oznaczymy przez  $\mathbb{P}$ .

*Date:* 03.March.1994 – December 2009 – January 2010 – 17 March 2014.

*1991 Mathematics Subject Classification.* Pierwszorzędny: 11D41; Drugorzędny: 11D45.

*Key words and phrases.* Dowód Nie Wprost, Największy Wspólny Podzielnik, Trójmian Kwadratowy, Twierdzenie Pitagorasa, Wzór Dwumianowy Newtona.

A. Dowód dla  $n = 4$ .

$$(X^2)^2 = (Z^2)^2 - (Y^2)^2.$$

Zatem istnieją dwie pary względnie pierwszych liczb naturalnych  $u, v$  i  $y, x$  i liczba  $z$  takie, że  $u - v, y - x, z \in \{1, 3, 5, \dots\}$  i  $z$  jest minimalna (założenie):

$$\left[ (u^2 - v^2)^2 = (u^2 + v^2)^2 - (2uv)^2 = X^2 \wedge (u^2 + v^2)^2 + (2uv)^2 = Z^2 \wedge \right. \\ \left. 2(u^2 + v^2)(2uv) = Y^2 \right] \Rightarrow (u = y^2 \wedge v = x^2 \wedge u^2 + v^2 = z^2) \Rightarrow y^4 + x^4 = z^2.$$

Zatem istnieją względnie pierwsze nieparzyste liczby naturalne  $p > q$ :

$$\left[ (pq)^4 = x^4 = (z + y^2)(z - y^2) \Rightarrow \right. \\ \left. \left( z = \frac{p^4 + q^4}{2} \wedge y^2 = \frac{p^4 - q^4}{2} \right) \Rightarrow y^2 = \frac{p^2 + q^2}{2}(p^2 - q^2) \right].$$

Muszą więc istnieć parami względnie pierwsze liczby naturalne  $g > w > e$  takie, że  $g, w - e \in \{3, 5, 7, \dots\}$ :

$$\left[ g^2 = \frac{p^2 + q^2}{2} \wedge (2we)^2 = (w^2 + e^2)^2 - (w^2 - e^2)^2 = p^2 - q^2 \wedge \right. \\ w^2 + e^2 = p \wedge w^2 - e^2 = q \wedge 2w^4 + 2e^4 = p^2 + q^2 \wedge \\ \left. w^4 + e^4 = g^2 = \frac{p^2 + q^2}{2} < \frac{(p^4 + q^4)^2}{4} = z^2 \right] \Rightarrow g < z,$$

co stoi w sprzeczności z minimalnością liczby  $z$ . ❖

B. Dowód dla  $n \in \mathbb{P}$  – wnioski ogólne.

Z powyższego wynika, że dla liczby dodatniej  $\nu$ :

$$2\nu = X - (Z - Y) = Y - (Z - X) \wedge Z - Y + 2\nu = X \wedge Z - X + 2\nu = Y \wedge \\ (Z - Y + 2\nu)^n = (Z - Y + Y)^n - Y^n \wedge (Z - X + 2\nu)^n = (Z - X + X)^n - X^n \wedge \\ [X + Y + (-Y)]^n + Y^n = [X + Y + (-2\nu)]^n = Z^n.$$

W konsekwencji otrzymujemy koniunkcję trzech równań:

$$\begin{aligned} & (Z - Y)^{n-2} \nu + (n-1)(Z - Y)^{n-3} \nu^2 + \dots + 2^{n-2} \nu^{n-1} + \frac{2^{n-1} \nu^n}{n(Z - Y)} = \\ & = \frac{Y}{2} \left[ (Z - Y)^{n-2} + \frac{n-1}{2} (Z - Y)^{n-3} Y + \dots + Y^{n-2} \right] \wedge \\ & (Z - X)^{n-2} 2\nu + \frac{n-1}{2} (Z - X)^{n-3} (2\nu)^2 + \dots + (2\nu)^{n-1} + \frac{(2\nu)^n}{n(Z - X)} = \\ & = X \left[ (Z - X)^{n-2} + \frac{n-1}{2} (Z - X)^{n-3} X + \dots + X^{n-2} \right] \wedge \\ & (X + Y)^{n-2} (-Y) + \frac{n-1}{2} (X + Y)^{n-3} (-Y)^2 + \dots + (-Y)^{n-1} = \\ & = (X + Y)^{n-2} (-2\nu) + \frac{n-1}{2} (X + Y)^{n-3} (-2\nu)^2 + \dots + (-2\nu)^{n-1} + \frac{(-2\nu)^n}{n(X + Y)}. \quad [2] \end{aligned}$$

Zatem liczby  $\nu, Y/2$  muszą być nieparzyste, liczba pierwsza  $n \mid \nu$  oraz

$$\left[ (n \mid X, Z - Y \vee n \mid Y, Z - X \vee n \mid X + Y, Z) \wedge \right. \\ \left. Z - Y, Z - X, X + Y \mid (2\nu)^n \wedge n \mid XYZ \wedge \nu = nmch \right].$$

B.1. Dowód dla liczb nieparzystych  $X, Y, Z - X$ . Istnieją  $m, c \in \{3, 5, 7, \dots\}$  i istnieje  $h \in \{1, 3, 5, \dots\}$ :

$$\begin{aligned} & \{n \nmid mch \wedge [(n^{n-1}c^n + 2nmch = X \wedge n \mid X \wedge h^n + 2nmch = Y \wedge \\ & \quad 2^n m^n = X + Y = n^{n-1}c^n + h^n + 4nmch \wedge n^{n-1}c^n + Y = Z) \vee \\ & \quad (c^n + 2nmch = X \wedge n \mid Y \wedge n^{n-1}h^n + 2nmch = Y \wedge \\ & \quad 2^n m^n = X + Y = c^n + n^{n-1}h^n + 4nmch \wedge c^n + Y = Z) \vee \\ & \quad (c^n + 2nmch = X \wedge n \mid X + Y, Z \wedge h^n + 2nmch = Y \wedge \\ & \quad 2^n n^{n-1}m^n = X + Y = c^n + h^n + 4nmch \wedge c^n + Y = Z)]\} \Rightarrow \\ & [(2^n m^n - h^n = n^{n-1}c^n + 4nmch \wedge n \mid 2m - h \wedge n^2 \mid 2^n m^n - h^n) \vee \\ & (2^n m^n - c^n = n^{n-1}h^n + 4nmch \wedge n \mid 2m - c \wedge n^2 \mid 2^n m^n - c^n) \vee \\ & (2^n n^{n-1}m^n = c^n + h^n + 4nmch \wedge n \mid c + h \wedge n^2 \mid c^n + h^n)] \Rightarrow \\ & \quad \frac{mch}{n} \notin \{3, 5, 7, \dots\}. \quad \spadesuit \end{aligned}$$

B.2. Dowód dla liczb parzystych  $Y, Z - X$ . Istnieją  $m, c \in \{3, 5, 7, \dots\}$  i istnieje  $h \in \{1, 3, 5, \dots\}$ :

$$\begin{aligned} & \{n \nmid mch \wedge [(n^{n-1}c^n + 2nmch = X \wedge n \mid X \wedge 2^n h^n + 2nmch = Y \wedge \\ & \quad m^n = X + Y = n^{n-1}c^n + 2^n h^n + 4nmch \wedge n^{n-1}c^n + Y = Z) \vee \\ & \quad (c^n + 2nmch = X \wedge n \mid Y \wedge 2^n n^{n-1}h^n + 2nmch = Y \wedge \\ & \quad m^n = X + Y = c^n + 2^n n^{n-1}h^n + 4nmch \wedge c^n + Y = Z) \vee \\ & \quad (c^n + 2nmch = X \wedge n \mid X + Y, Z \wedge 2^n h^n + 2nmch = Y \wedge \\ & \quad n^{n-1}m^n = X + Y = c^n + 2^n h^n + 4nmch \wedge c^n + Y = Z)]\} \Rightarrow \\ & [(m^n - 2^n h^n = n^{n-1}c^n + 4nmch \wedge n \mid m - 2h \wedge n^2 \mid m^n - 2^n h^n) \vee \\ & (m^n - c^n = 2^n n^{n-1}h^n + 4nmch \wedge n \mid m - c \wedge n^2 \mid m^n - c^n) \vee \\ & (n^{n-1}m^n = c^n + 2^n h^n + 4nmch \wedge n \mid c + 2h \wedge n^2 \mid c^n + 2^n h^n)] \Rightarrow \\ & \quad \frac{mch}{n} \notin \{3, 5, 7, \dots\}. \end{aligned}$$

To jest dowód. Ten dowód jest równoważny dowodowi WTF w  $\mathbb{Z}$ . □

#### REFERENCES

- [1] Gładki, P.: <http://www.math.us.edu.pl/~pgladki/faq/node135.html>
- [2] Guła, L.W. : [http://www.ijetae.com/files/Volume2Issue12/IJETAE\\_1212\\_14.pdf](http://www.ijetae.com/files/Volume2Issue12/IJETAE_1212_14.pdf)
- [3] Mazur, B. : "About The Cover: Diohantus's Arithmetica", <http://www.ams.org/journals/bull/2006-43-03/S0273-0979-06-01123-2/S0273-0979-06-01123-2.pdf>
- [4] Narkiewicz, W. : WIADOMOŚCI MATEMATYCZNE XXX.1, Annuals PTM, Series II, Warszawa 1993.

LUBLIN-POLAND  
E-mail address: lwgula@wp.pl