PRAWDZIWIE CUDOWNY DOWÓD

LESZEK W. GUŁA

Pracę Dedykuję Moim Rodzicom i Mojemu Bratu

ABSTRACT. Właściwy 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 $a, u \in \mathbb{Z}$:

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

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 [4], jest odtworzony następujący dopisek Pierre de Fermata (1665): *Nie można rozłożyć ani sześcianu na [sumę] dwa sześciany, 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.* [2] 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. [4]

Wzór (1) wynika z równania Diofantosa – dla dowolnej pary względnie pierwszych liczb naturalnych u, v takich, że $u - v \in \{1, 3, 5, ...\}$:

$$\left(u^2+v^2\right)^2 = (2uv)^2 + \left(u^2-v^2\right)^2,$$

które daje wszystkie właściwe trójki pitagorejskie $(x, y, z) = \left(u^2-v^2,\ 2uv,\ u^2+v^2\right)$, gdzie liczby x, y, z są parami względnie pierwsze. Oto nowa metoda wyznaczania takich właściwych trójek Diofantosa, że $2uv - \left(u^2-v^2\right) = y - x = \pm 1$:

$$[u, v] \in \{[2,1],\ [5,2],\ [12,5],\ [29,12],\ [70,29],\ [169,70],\ [408,169],\ ...\} =$$

$$[u, v] \in \{[2,1],\ [(2\cdot 2+1),2],\ [(2\cdot 5+2),5],\ [(2\cdot 12+5),12],\ [(2\cdot 29+12),29],$$

$$[(2\cdot 70+29),70],\ [(2\cdot 169+70),169],\ [(2\cdot 408+169),408],\ ...\} =$$

Date: 03.03.1994 – 29.04.2014.

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.

$$[u,\upsilon]\in\{[2,1]\,,\ [(2+3)\,,2]\,,\ [(5+7)\,,5]\,,\ [(12+17)\,,12]\,,\ [(29+41)\,,29]\,,$$
$$[(70+99)\,,70]\,,\ [(169+239)\,,169]\,,\ [(408+577)\,,408]\,,\ ...\}\Rightarrow$$
$$2u\upsilon-\left(u^2-\upsilon^2\right)=y-x=\pm1.$$

Inną metodę znajdziemy w [1].

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 $X^{n-1}+Y^{n-1}>Z^{n-1}$ (w przeciwnym razie $X^n+Y^n<Z^n$) i liczby $X,Z-Y$ będą dodatnie i nieparzyste i liczba $Z-X$ będzie dodatnia i liczba $X+Y-Z$ będzie dodatnia i parzysta.

Fermat zapewne przyjął, że istnieją względnie pierwsze liczby naturalne $u>\upsilon$ takie, że liczba $u-\upsilon$ jest nieparzysta:

$$\Big\{(u-\upsilon)^2+2\upsilon\,(u-\upsilon)=X\ \wedge\ X+Z-X-(u-\upsilon)^2=Y\ \wedge$$
$$X^2+\Big[X+\Big(Z-X-(u-\upsilon)^2\Big)\Big]^2-(Z-X+X)^2>0\ \wedge$$
$$X^2-2\,(u-\upsilon)^2\,X-2\,(Z-X)\,(u-\upsilon)^2+(u-\upsilon)^4>0\ \wedge$$
$$\sqrt{\Delta}=2\,(u-\upsilon)\,\sqrt{2\,(Z-X)}=4\upsilon\,(u-\upsilon)\ \wedge\ 2\upsilon^2=Z-X\Big\}\Rightarrow$$
$$\Big\{\Big[X<X_1=(u-\upsilon)^2-2\upsilon\,(u-\upsilon)\ \vee\ (u-\upsilon)^2+2\upsilon\,(u-\upsilon)=X_2<X\Big]\equiv0\Big\}.$$

Dowód ten jest fałszywy, bo założenie $\Big[u^2-\upsilon^2=X\wedge(u-\upsilon)^2=Z-Y\Big]\equiv0$, a także niekompletny, bo pomija przypadek, gdy liczba Z jest parzysta (przy $n\in\mathbb{P}$).

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. [5] Zbiór tych liczb oznaczmy przez $\mathbb{P}$.

A. Dowód dla $n=4$. Przyjmujemy, że dla liczby dodatniej ν:

$$\Big[2\nu=X+Y-Z\wedge\ Z-X+2\nu=Y\wedge\ (Z-X+2\nu)^4=(Z-X+X)^4-X^4\Big]\Rightarrow$$
$$(Z-X)^2\,2\nu+6\,(Z-X)\,\nu^2+8\nu^3+\frac{4\nu^4}{Z-X}=(Z-X)^2\,X+\frac{3}{2}\,(Z-X)\,X^2+X^3.$$

Zatem istnieje $h\in\{1,3,5,...\}$ i istnieją $\nu,Z,X\in\{3,5,7,...\}$:

$$4h^4+2\nu=Y\ \wedge\ h\mid\nu\ \wedge\ 4h^4=Z-X\ \wedge\ 4\nmid Y.$$

Jednocześnie muszą istnieć względnie pierwsze nieparzyste liczby naturalne $p>q$:

$$\Big\{\Big[2p^2 2q^2=Y^2\wedge\left(p^2\right)^2+\left(2q^2\right)^2=Z^2\wedge4\mid2q^2\equiv0\wedge p^4-4q^4=X^2\Big]\in\mathbf{0}\Big\}.\ \text{✠}$$

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

Z powyższego wynika, że dla liczby dodatniej ν:

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

W konsekwencji otrzymujemy koniunkcję trzech równań:

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

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

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

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

$$\{n \nmid mch\ \wedge\ \big[\big(n^{n-1}c^n+2nmch=X\ \wedge\ n \mid X\ \wedge\ h^n+2nmch=Y\ \wedge$$
$$2^n m^n=X+Y=n^{n-1}c^n+h^n+4nmch\ \wedge\ n^{n-1}c^n+Y=Z\big)\ \vee$$
$$\big(c^n+2nmch=X\ \wedge\ n \mid Y\ \wedge\ n^{n-1}h^n+2nmch=Y\ \wedge$$
$$2^n m^n=X+Y=c^n+n^{n-1}h^n+4nmch\ \wedge\ c^n+Y=Z\big)\ \vee$$
$$(c^n+2nmch=X\ \wedge\ n \mid X+Y,\ Z\ \wedge\ h^n+2nmch=Y\ \wedge$$
$$2^n n^{n-1}m^n=X+Y=c^n+h^n+4nmch\ \wedge\ c^n+Y=Z\big)\big]\}\Rightarrow$$
$$\big[\big(2^n m^n-h^n=n^{n-1}c^n+4nmch\ \wedge\ n \mid 2m-h\ \wedge\ n^2 \mid 2^n m^n-h^n\big)\ \vee$$
$$\big(2^n m^n-c^n=n^{n-1}h^n+4nmch\ \wedge\ n \mid 2m-c\ \wedge\ n^2 \mid 2^n m^n-c^n\big)\ \vee$$
$$\big(2^n n^{n-1}m^n=c^n+h^n+4nmch\ \wedge\ n \mid c+h\ \wedge\ n^2 \mid c^n+h^n\big)\big]\Rightarrow n \mid mch,$$

co stoi w sprzeczności z warunkiem, że $n \nmid mch$. ✠

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

$$\{n \nmid mch\ \wedge\ \big[\big(n^{n-1}c^n+2nmch=X\ \wedge\ n \mid X\ \wedge\ 2^n h^n+2nmch=Y\ \wedge$$
$$m^n=X+Y=n^{n-1}c^n+2^n h^n+4nmch\ \wedge\ n^{n-1}c^n+Y=Z\big)\ \vee$$
$$\big(c^n+2nmch=X\ \wedge\ n \mid Y\ \wedge\ 2^n n^{n-1}h^n+2nmch=Y\ \wedge$$
$$m^n=X+Y=c^n+2^n n^{n-1}h^n+4nmch\ \wedge\ c^n+Y=Z\big)\ \vee$$
$$(c^n+2nmch=X\ \wedge\ n \mid X+Y,\ Z\ \wedge\ 2^n h^n+2nmch=Y\ \wedge$$
$$n^{n-1}m^n=X+Y=c^n+2^n h^n+4nmch\ \wedge\ c^n+Y=Z\big)\big]\}\Rightarrow$$
$$\big[\big(m^n-2^n h^n=n^{n-1}c^n+4nmch\ \wedge\ n \mid m-2h\ \wedge\ n^2 \mid m^n-2^n h^n\big)\ \vee$$
$$\big(m^n-c^n=2^n n^{n-1}h^n+4nmch\ \wedge\ n \mid m-c\ \wedge\ n^2 \mid m^n-c^n\big)\ \vee$$
$$\big(n^{n-1}m^n=c^n+2^n h^n+4nmch\ \wedge\ n \mid c+2h\ \wedge\ n^2 \mid c^n+2^n h^n\big)\big]\Rightarrow n \mid mch,$$

co stoi w sprzeczności z warunkiem, że $n \nmid mch$. To jest dowód. □

Konkluzja 1. Ostatnie Twierdzenie Fermata zwane także Wielkim Twierdzeniem Fermata jest prawdziwe dla każdego $n, X, Y, Z \in \{3, 4, 5, ...\}$. Liczby X, Y, Z w żadnej hipotetycznej trójce Fermata (X, Y, Z) nie mogą być jednocześnie kwadratami liczb naturalnych, muszą być parami różne od kwadratów liczb naturalnych i w każdym przypadku dowodu dla $n \in \mathbb{P}$ musi być $n \mid XYZ$ i $n^2 \nmid XYZ$ i $n \notin \{3^2, 5^2, 7^2, ...\}$.

Jednakże załóżmy, że istnieje $n \in \mathbb{P}$ i istnieją $p, q, z, x \in \{3, 5, 7, ...\}$ takie, że $p > q$ i $z > x$ i $NWD(p, q) = NWD(p, z) = NWD(p, x) = NWD(q, z) = NWD(q, x) = NWD(z, x) = 1$:

$$\Big[(2pq)^n = Y^n = (z^n)^2 - (x^n)^2 \ \wedge\ n \mid pq \ \wedge\ n \nmid 2pq + x^2,\ z^2,\ z,\ x^2,\ x \ \wedge$$

$$\frac{(2pq)^n + \left(2^{n-1}q^n\right)^2}{2\left(2^{n-1}q^n\right)} = p^n + 2^{n-2}q^n = z^n = Z^{\frac{n}{2}} \wedge\ z^2 = Z \ \wedge$$

$$\frac{(2pq)^n - \left(2^{n-1}q^n\right)^2}{2\left(2^{n-1}q^n\right)} = p^n - 2^{n-2}q^n = x^n = X^{\frac{n}{2}} \wedge\ x^2 = X\Big].$$

Na mocy powyższego musi być – istnieje $m \in \{3, 5, 7, ...\}$:

$$\Big[m^n = 2pq + x^2 \ \wedge\ n \mid pq \ \wedge\ 2pq + x^2 \mid (2pq)^n + \left(x^2\right)^n,\ \left(z^2\right)^n \ \wedge$$

$$\frac{(2pq)^n + \left(x^2\right)^n}{2pq + x^2} = \frac{(2pq)^n + \left(x^2\right)^n}{m^n} = \frac{\left(z^2\right)^n}{m^n}\Big].$$

Zatem istnieje $w \in \{3, 5, 7, ...\}$:

$$\Big[w^2 = m \ \wedge\ m^n = (w^n)^2 = 2pq + x^2\Big] \Rightarrow$$

$$(w^n)^2 - x^2 = 2pq \Rightarrow [(2 \mid pq \equiv 0) \in \mathbf{0}].\ \text{✠}$$

To jest konkluzja.

Konkluzja 2. W pracy pt. *The Truly Marvellous Proof* [3] nie ma szkody dla tegoż dowodu, w którym nieparzysty wykładnik $n \nmid X$. To jest konkluzja.

References

[1] Gierszewski, M. : poradnik inżyniera i technika budowlanego, t. 1, cz. 1, matematyka, Arkady-Warszawa 1977, 60-61

[2] Gładki, P.: http://www.math.us.edu.pl/~pgladki/faq/node135.html

[3] Guła, L.W. : http://www.ijetae.com/files/Volume2Issue12/IJETAE_1212_14.pdf

[4] 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

[5] Narkiewicz, W. : WIADOMOŚCI MATEMATYCZNE XXX.1, Annuals PTM, Seria II, Warszawa 1993.

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