PRAWDZIWIE CUDOWNY DOWÓD

LESZEK W. GUŁA

Pracę Dedykuję Moim Rodzicom i Mojemu Bratu

ABSTRACT. 1. Przypuszczalny dowód Fermata, twierdzenia zwanego Wielkim Twierdzeniem Fermata. 2. Elementarny dowód WTF.

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, 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. [1] Zapewne stąd wzięło się 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]

Nietrudno zauważyć, iż (1) wynika z równania Diofantosa – dla każdego $u, v \in N_1$:

$$\begin{gathered}\left(u^2+v^2\right)^2 = \left(u^2-v^2\right)^2 + (2uv)^2 \ \wedge \\ 2\left(u^2+v^2\right)^2 = \left(u^2-v^2+2uv\right)^2 + \left[\pm\left(u^2-v^2-2uv\right)\right]^2.\end{gathered} \tag{2}$$

(2) daje wszystkie trójki pitagorejskie $\left(u^2-v^2,\ 2uv,\ u^2+v^2\right) = (x, y, z)$ w $\mathbb{Z}$, a wśród nich, jeżeli liczby u, v są względnie pierwsze i liczba $u-v$ jest dodatnia i nieparzysta – wszystkie właściwe (pierwotne) rozwiązania równania Pitagorasa w $\mathbb{N}_1$.

Twierdzenie 1. Dla każdej właściwej trójki pitagorejskiej (x, y, z) istnieją dokładnie dwie względnie pierwsze liczby naturalne $u > v$ takie, że liczba $u-v$ jest nieparzysta.

Date: 03.03.1994 – 12.06.2013 – 13.03.2014.

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.

II. Wielkie Twierdzenie Fermata

Twierdzenie 2. 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 $X^n + Y^n < Z^n$.

Z powyższego wynika, że liczby $X, Z-Y$ będą dodatnie i nieparzyste, liczba $Z-X$ będzie dodatnia, a liczba $X + Y - Z$ będzie dodatnia i parzysta.

Fermat zapewne przyjął, że $(u-v)^2 + 2v(u-v) = X$, przy $(u-v)^2 = Z - Y$:

$$X+Z-X-(u-v)^2 = Y \wedge X^2 + \Big[X + \Big(Z - X - (u-v)^2\Big)\Big]^2 - (Z - X + X)^2 > 0 \wedge$$
$$X^2 - 2(u-v)^2 X - 2(Z-X)(u-v)^2 + (u-v)^4 > 0 \wedge$$
$$\sqrt{\Delta} = 2(u-v)\sqrt{2(Z-X)} = 4v(u-v) \ \wedge \ 2v^2 = Z - X.$$

W konsekwencji Fermat uzyskał dwie fałszywe sprzeczności:

$$X < X_1 = (u-v)^2 - 2v(u-v) \ \vee \ (u-v)^2 + 2v(u-v) = X_2 < X. \ [2]$$

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 oznaczmy przez $\mathbb{P}$.

A. Dowód dla $n = 4$. Na mocy (2) i Tw. 1 istnieją dokładnie dwie względnie pierwsze liczby naturalne $U > V$ takie, że $U - V \in \{3, 5, 7, ...\}$:

$$\big[U^2 - V^2 = X^2 \wedge\ 2UV = Y^2 \wedge\ U^2 + V^2 = Z^2 \wedge\ U^2 = X^2 + V^2 \ \wedge$$
$$2U^2 = X^2 + Z^2 \wedge\ \pm X = X - V \ \wedge\ Z = X + V\big] \Rightarrow (Z = X \ \vee\ Z = 3X),$$

co stoi w sprzeczności przy $NWD(X, Z) = 1$. ✠

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:

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

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

$$[(n \mid X, Z-Y \ \vee \ n \mid Y, Z-X \ \vee \ n \mid X+Y, Z) \ \wedge$$

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

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

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

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

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

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

[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