ELEMENTARNY DOWÓD WIELKIEGO TWIERDZENIA FERMATA

LESZEK W. GUŁA

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 $a, u \in \mathbb{Z}$:

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

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]

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 oznaczmy 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 $n=4$. Istnieją pary względnie pierwszych liczb naturalnych $U>V$ i $u>v$ i $y>x$ takich, że $U-V,\ u-v,\ y^2-x^2,\ z\in\{1,3,5,...\}$:

$$\Big[\left(u^2-v^2\right)^2=\left(u^2+v^2\right)^2-(2uv)^2=X^2\wedge\ 2UV=2\left(u^2+v^2\right)(2uv)=Y^2\wedge$$

$$U^2+V^2=\left(u^2+v^2\right)^2+(2uv)^2=Z^2\wedge\ u=y^2\wedge\ v=x^2\wedge\ u^2+v^2=z^2\wedge$$

$$\left(X^2\right)^2+\left(Y^2\right)^2=\left(Z^2\right)^2\Big]\Rightarrow x^4=z^2-y^4.$$

Przyjmujemy, że liczba z jest minimalna. Istnieją względnie pierwsze nieparzyste liczby naturalne $p>q$:

$$\Big[(pq)^4=x^4=\left(z+y^2\right)\left(z-y^2\right)\Rightarrow$$

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

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

$$\Big[g^2=\frac{p^2+q^2}{2}\ \wedge\ (2we)^2=\left(w^2+e^2\right)^2-\left(w^2-e^2\right)^2=p^2-q^2\wedge$$

$$w^2+e^2=p\ \wedge\ w^2-e^2=q\ \wedge\ 2w^4+2e^4=p^2+q^2\wedge$$

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

co stoi w sprzeczności z minimalnością liczby z. ✠

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

Z powyższego wynika, że dla liczby dodatniej 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 $h \in \{1, 3, 5, ...\}$:

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

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

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

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