Równania Pitagorasa i Fermata

Oliwia Jarzęcka, Kajetan Grzybacz, Paweł Jarosz

27 lutego 2018

1 Wstęp

Punktem wyjścia dla naszych rozważań jest klasyczne równanie Pitagorasa związane z trójkątem prostokątnym

$$x^2 + y^2 = z^2. \tag{1}$$

Dobrze znane jest jego rozwiązanie w liczbach całkowitych $x = 3$, $y = 4$ i $z = 5$. Oczywiście, zmiana znaku przy każdej z tych liczb nie wpływa na poprawność równania (1). Podobnie, zamiana x oraz y nie zmienia poprawności tego równania. A zatem to jedno rozwiązanie, odpowiada tak naprawdę aż 16 różnym rozwiązaniom. Zaintrygowało nas pytanie, czy równanie Pitagorasa ma istotnie inne rozwiązania w liczbach całkowitych. Szybko odnaleźliśmy pojęcie trójek pitagorejskich i dowiedzieliśmy się, że jest ich nieskończenie wiele. W pierwszej części naszej pracy przedstawiamy geometryczny sposób znajdowania trójek pitagorejskich.

Druga część pracy związana jest z uogólnieniem równania (1) na wyższe potęgi. Takie uogólnienie, dla $n \geqslant 3$, nosi nazwę równania Fermata:

$$x^n + y^n = z^n. \tag{2}$$

Okazuje się, i to było dla nas zaskoczeniem, że równanie Fermata nie ma nietrywialnych (to znaczy takich, że $x \neq 0$ i $y \neq 0$) rozwiązań w liczbach całkowitych. Jeszcze bardziej zdziwiła nas informacja, że problem nieistnienia takich rozwiązań, został rozstrzygnięty dopiero bardzo niedawno, bo w 1994 roku, przez Andrew Wilesa. Druga część naszej pracy poświęcona jest... rozwiązaniom równania Fermata. Zamiast liczb całkowitych posługujemy się jednak macierzami takich liczb. Ale po kolei.

2 Trójki pitagorejskie, czyli użycie koła

Równanie (1) przekształcimy do równoważnego równania

$$\frac{x^2}{z^2} + \frac{y^2}{z^2} = 1. \tag{3}$$

Podstawiając $p = x/z$ i $q = y/z$ możemy zapisać

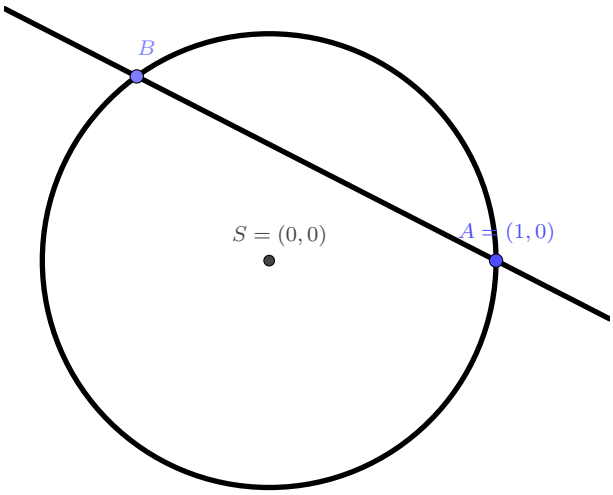
$$p^2 + q^2 = 1, \tag{4}$$

a to jest równanie okręgu jednostkowego. Zauważmy, że jeśli x, y, z są liczbami całkowitymi, to p, q są liczbami wymiernymi. Czyli, jeśli równanie (1) ma rozwiązanie

w liczbach całkowitych, to równanie (4) ma rozwiązanie w liczbach wymiernych. Również na odwrót. Jeśli p i q są wymiernymi rozwiązaniami równania (4), to zapisując $p = \frac{a}{b}$ i $q = \frac{c}{d}$ i podstawiając $x = ad$, $y = cb$ i $z = bd$ dostajemy całkowite rozwiązanie równania (1). Reasumując, wykazaliśmy następującą zależność.

Twierdzenie 2.1. *Istnieje wzajemnie jednoznaczna odpowiedniość między rozwiązaniami równania* (1) *w liczbach całkowitych i rozwiązaniami równania* (4) *w liczbach wymiernych.*

To twierdzenie byłoby bezużyteczne gdybyśmy nie potrafili wyznaczyć punktów wymiernych na okręgu jednostkowym. Ale potrafimy. I właśnie teraz pokażemy jak to zrobić.



Rysunek 1: Okrąg jednostkowy przecięty prostą

Na rysunku 1 zaznaczono punkt $A = (1, 0)$ oraz pewną prostą. Równanie tej prostej jest (w układzie współrzędnych p, q) postaci

$$q = ap - a$$

dla pewnej liczby a, gdyż prosta ta przechodzi przez punkt A. Fundamentalny dla naszych rozważań jest następujący fakt.

Twierdzenie 2.2. *Jeśli współczynnik kierunkowy prostej $q = ap - a$ jest liczbą wymierną, to współrzędne punktu $B \neq A$, w którym ta prosta przecina okrąg jednostkowy są również liczbami wymiernymi.*

Dowód. Wyliczymy współrzędne punktu przecięcia prostej z okręgiem. Mamy układ równań

$$\begin{cases} q &= ap - a \\ p^2 + q^2 &= 1 \end{cases}$$

□

Podstawiając q do drugiego równania dostajemy po przekształceniach

$$(1 + a^2)p^2 - 2a^2p + a^2 - 1 = 0. \tag{5}$$

Wiemy, że jednym z rozwiązań tego równania jest $p = 1$, bo prosta i okrąg na pewno przecinają się w punkcie A. Z kolei, jeśli p_1, p_2 są rozwiązaniami równania, to ze wzorów Viete'a mamy

$$p_1 p_2 = \frac{a^2 - 1}{a^2 + 1}.$$

a zatem drugim (poza $p_1 = 1$) rozwiązaniem równania (5) jest liczba $p_2 = \frac{a^2-1}{a^2+1}$. Ta liczba jest pierwszą współrzędną punktu B. Drugą współrzędną wyliczamy z równania prostej

$$q = ap_2 - a = \frac{-2a}{a^2 + 1}.$$

Zatem para liczb wymiernych

$$p = \frac{a^2 - 1}{a^2 + 1} \quad \text{i} \quad q = \frac{-2a}{a^2 + 1}$$

jest rozwiązaniem równania (4). Co więcej każde rozwiązanie wymierne tego równania jest tej postaci dla pewnej liczby wymiernej a. Wynika to z faktu, że prosta przechodząca przez dwa punkty wymierne ma wymierny współczynnik kierunkowy.

Z twierdzenia 2.1 wynika, że liczby

$$x = a^2 - 1, \quad y = -2a, \quad z = a^2 + 1 \tag{6}$$

są, dla całkowitych wartości a rozwiązaniami równania Pitagorasa, czyli tworzą trójkę pitagorejską.

Wniosek 2.3. *Istnieje nieskończenie wiele trójek Pitagorejskich. Są one parametryzowane przez różne wartości całkowitego parametru a.*

Przykład 2.4. *Podstawiając w* (6) $a = 2$ *dostajemy* $x = 3$, $y = -4$, $z = 5$, *czyli (z dokładnością do znaku i kolejności) podstawowe rozwiązanie równania Pitagorasa.*

Z kolei, dla $a = -5$ *dostajemy* $x = 24$, $y = 10$, $z = 26$. *Dzieląc przez* 2 *mamy*

$$x = 12, \quad y = 5, \quad z = 13.$$

A to jest inne, dobrze znane rozwiązanie równania Pitagorasa w liczbach całkowitych.

3 Macierze

Jak już wspomnieliśmy, w 1637 roku Pierre de Fermat w swoim dziele „Arithmetica" sformułował twierdzenie, że równanie (2) nie ma rozwiązania w liczbach całkowitych różnych od zera. Fermat nie podał dowodu tego twierdzenia. Dzięki jego równaniu rozwinął się dział matematyki: teoria liczb. Dowód twiedzenia Fermata został podany dopiero pod koniec XX wieku.

Jest to zastanawiająca historia, bo istnieją przecież inne równania, o których dobrze wiadomo, że nie mają rozwiązań. Na przykład równanie

$$x^2 + 1 = 0$$

nie tylko nie ma rozwiązań w liczbach całkowitych, ale nie ma go też w liczbach rzeczywistych! Matematycy jednak nie lubią zadań, których się nie da rozwiązać. I to doprowadziło do powstania liczb zespolonych. Liczba urojona i ma właśnie tą własność, że jej kwadrat jest równy -1, czyli jest ona rozwiązaniem powyższego równania.

W odniesieniu do równania Fermata proponujemy w tej pracy jego rozważanie w jeszcze innym typie obiektów matematycznych, a mianowicie w macierzach. Będziemy je oznaczać dużymi literami alfabetu.

Definicja 3.1. *Macierzą wymiaru* 2×2 *nazywamy czwórkę liczb ustawionych w dwa rzędy i dwie kolumny:*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

W zbiorze macierzy wprowadzamy operacje działań, podobnie jak na liczbach Dodawanie macierzy zdefiniowane jest w naturalny sposób „po współrzędnych".

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}.$$

Definicja mnożenia macierzy jest nieco bardziej skomplikowana

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

To może się wydawać skomplikowane, jednak definicja mnożenia „po współrzędnych" nie doprowadziłaby do niczego istotnie różnego od liczb.

Uwaga 3.2. *Pierwsza, istotna różnica między mnożeniem liczb i mnożeniem macierzy, jest taka, że mnożenie macierzy na ogół nie jest przemienne, tzn.* $A \cdot B$ *nie musi być równe* $B \cdot A$*. Na przykład, dla macierzy*

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad i \quad B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$$

mamy

$$A \cdot B = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix} \quad i \quad B \cdot A = \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix}.$$

Łatwo można sprawdzić, że mnożenie przez macierz jednostkową

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

daje

$$A \cdot I = I \cdot A = A,$$

czyli I zachowuje się tak jak jedynka wśród liczb. Rolę zera odgrywa macierz

$$Z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Istotnie, mamy

$$A + Z = Z$$

dla każdej macierzy A.

Może się zdarzyć, i to też jest istotna różnica w stosunku do liczb, że mnożenie dwóch macierzy, które są niezerowe daje macierz zerową. Na przykład

$$\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Macierze A o takiej własności, że można dobrać macierz $B \neq Z$ taką, że

$$A \cdot B = Z$$

będziemy nazywać *osobliwymi*. Takie macierze można łatwo rozpoznać.

Definicja 3.3. *Wyznacznikiem macierzy* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *nazywamy liczbę*

$$\det(A) = ad - bc.$$

Mamy następujące twierdzenie.

Twierdzenie 3.4. *Jeśli* $\det(A) = 0$*, to istnieje macierz* $B \neq Z$ *taka, że* $AB = Z$*.*

Dowód. Niech $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Załóżmy, że a lub b jest różne od zera. Wtedy macierz $B = \begin{bmatrix} -b & -b \\ a & a \end{bmatrix}$ spełnia warunki zadania.

W przeciwnym przypadku, dla $a = b = 0$ bierzemy $B = \begin{bmatrix} -d & -d \\ c & c \end{bmatrix}$. □

W dalszym ciągu będziemy zajmować się tylko macierzami *nieosobliwymi* (tzn. takimi, które nie są osobliwe, czyli, których wyznacznik nie jest równy zero). Dla takich macierzy można wskazać macierz odwrotną.

Twierdzenie 3.5. *Niech* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *i niech* $t = ad - bc \neq 0$*. Niech macierz* B *dana będzie wzorem*

$$B = \begin{bmatrix} d/t & -c/t \\ -b/t & a/t \end{bmatrix}.$$

Wówczas

$$A \cdot B = I.$$

Dowód. To jest łatwy rachunek. □

Na zakończenie krótkiej wyprawy w krainę macierzy zauważmy, że ograniczając się tylko do macierzy, które są podobne do macierzy I, to znaczy mają niezerowe i równe wyrazy tylko na przekatnej, odtwarzamy dobrze znane mnożenie liczb. Konkretnie, niech

$$A = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \quad \text{i} \quad B = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix},$$

wtedy

$$A \cdot B = \begin{bmatrix} ab & 0 \\ 0 & ab \end{bmatrix} = B \cdot A.$$

4 Równanie Fermata w macierzach całkowitych

W tej części zajmiemy się równaniem

$$X^n + Y^n = Z^n, \tag{7}$$

dla $n \geqslant 3$ i dla nieosobliwych macierzy X, Y, Z. Zaczniemy od przygotowawczej obserwacji.

Lemat 4.1. *Niech* $A = \begin{bmatrix} 0 & 1 \\ a & 0 \end{bmatrix}$. *Wówczas* $A^2 = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

Dowód. Dowód polega na pomnożeniu macierzy A przez siebie. □

Nasz główny wynik jest następujący.

Twierdzenie 4.2. *Równanie* (7) *ma dla* $n = 4$ *nieskończenie wiele rozwiązań w macierzach nieosobliwych o współczynnikach całkowitych.*

Dowód. Nasz dowód polega na wskazaniu rozwiązań. Niech liczby całkowite x, y, z będą rozwiązaniami równania Pitagorasa (1), tzn. liczby te tworzą trójkę pitagorejską. Wtedy, macierze

$$X = \begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}, \ Y = \begin{bmatrix} 0 & 1 \\ y & 0 \end{bmatrix}, \ Z = \begin{bmatrix} 0 & 1 \\ z & 0 \end{bmatrix}$$

spełniają równanie

$$X^4 + Y^4 = Z^4.$$

Rzeczywiście, na mocy Lematu 4.1 mamy np.

$$X^2 = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}.$$

Z tego wynika, że

$$X^4 = X^2 \cdot X^2 = \begin{bmatrix} x^2 & 0 \\ 0 & x^2 \end{bmatrix}.$$

Analogicznie

$$Y^4 = \begin{bmatrix} y^2 & 0 \\ 0 & y^2 \end{bmatrix} \ \text{oraz} \ Z^4 = \begin{bmatrix} z^2 & 0 \\ 0 & z^2 \end{bmatrix}.$$

Równość

$$\begin{bmatrix} x^2 & 0 \\ 0 & x^2 \end{bmatrix} + \begin{bmatrix} y^2 & 0 \\ 0 & y^2 \end{bmatrix} = \begin{bmatrix} z^2 & 0 \\ 0 & z^2 \end{bmatrix}$$

jest teraz oczywista.

Liczba rozwiązań jest nieskończona, bo pokazaliśmy we Wniosku 2.3, że jest nieskończenie wiele trójek pitagorejskich. □

5 Podsumowanie

Oczywiście nasza praca nie rozwiązuje problemu szukania rozwiązań w macierzach całkowitych równania Fermata. Wskazaliśmy tylko jedną przykładową rodzinę takich rozwiązań dla konkretnej wartości wykładnika n. Mamy nadzieję, że nasza praca zainspiruje inne osoby do zajęcia się problemem poszukiwania innych rozwiązań oraz poszukiwaniem innych ciekawych własności macierzy.

Nasza praca powstała w czasie zajęć w projekcie „Laboratorium Twórczej Matematyki". Naszymi nauczycielami i mentorami byli panowie Tomasz Szemberg i Daniel Wójcik. Dziękujemy im za pomoc przy tworzeniu tej pracy. Dziękujemy też panu Pawłowi Solarzowi za wprowadzenie do systemu LaTeX.