Sumy kwadratów wielomianów i funkcji wymiernych

Kazimierz SZYMICZEK

Sumy kwadratów i liczba Pitagorasa

Niniejszy tekst stanowi zapis odczytu PTM wygłoszonego przez Autora w VIII LO w Katowicach w dniu 18.02.1997 r.

W elementarnej teorii liczb dowodzi się twierdzenia Lagrange'a mówiącego, że *każda dodatnia liczba całkowita jest sumą kwadratów czterech liczb całkowitych*. Wynika stąd natychmiast, że również każda dodatnia liczba wymierna jest sumą kwadratów czterech liczb wymiernych.

Oczywiście, każda *dodatnia* liczba całkowita (wymierna) jest sumą kwadratów liczb całkowitych (wymiernych), bowiem dla dowolnych naturalnych n, m mamy $n = n \cdot 1^2$ oraz $\frac{m}{n} = mn \cdot \left(\frac{1}{n}\right)^2$. Istotą twierdzenia Lagrange'a jest zatem to, że każda liczba całkowita (wymierna), która w ogóle jest sumą kwadratów liczb całkowitych (wymiernych) daje się przedstawić jako suma akurat *czterech* takich kwadratów. W związku z tą własnością liczby 4 nazywamy ją *liczbą Pitagorasa* pierścienia liczb całkowitych $\mathbf{Z}$ (a także ciała liczb wymiernych $\mathbf{Q}$). Pojęcie liczby Pitagorasa można wprowadzić dla każdego pierścienia.

Pierścień to zbiór P, w którym określone są dodawanie i mnożenie spełniające następujące warunki:

1. Zbiór P tworzy wraz z dodawaniem *grupę abelową*.
2. Mnożenie jest łączne.
3. Mnożenie jest rozdzielne względem dodawania.

Kto nie wie, co to grupa, niech zajrzy np. do *Delty* 9/1995. Pierścień tworzą np. liczby całkowite czy też wielomiany jednej zmiennej o współczynnikach rzeczywistych (albo wymiernych, albo całkowitych).

Pierścień przemienny, z jedynką i bez dzielników zera nazywamy pierścieniem całkowitym (lub dziedziną całkowitości).

Definicja 1
Niech K będzie dowolnym pierścieniem. *Liczbą Pitagorasa* pierścienia K nazywamy taką najmniejszą liczbę naturalną $p = p(K)$, że każdy element a pierścienia K, który jest sumą kwadratów elementów pierścienia K, można przedstawić jako sumę p kwadratów elementów K. Jeśli taka liczba p nie istnieje, to przyjmujemy, że $p(K) = \infty$.

Na podstawie twierdzenia Lagrange'a mamy $p(\mathbf{Z}) = 4 = p(\mathbf{Q})$. Jest też jasne, że dla ciała liczb rzeczywistych $\mathbf{R}$ i liczb zespolonych $\mathbf{C}$ mamy $p(\mathbf{R}) = 1 = p(\mathbf{C})$.

Wielomiany jednej zmiennej

Rozpatrzmy teraz pierścień $\mathbf{R}[X]$ wielomianów jednej zmiennej X o współczynnikach rzeczywistych. Postaramy się znaleźć liczbę Pitagorasa tego pierścienia. Przede wszystkim więc należy rozpatrzyć te wielomiany $g \in \mathbf{R}[X]$, które można przedstawić w postaci sumy kwadratów wielomianów:

$$g = g_1^2 + \cdots + g_n^2, \quad g_i \in \mathbf{R}[X]\,.$$

Podstawiając tutaj w miejsce zmiennej X dowolną liczbę $x \in \mathbf{R}$ otrzymamy $g(x) = g_1(x)^2 + \cdots + g_n(x)^2 \geq 0$. A więc każdy wielomian $g \in \mathbf{R}[X]$, który jest sumą kwadratów wielomianów pierścienia $\mathbf{R}[X]$, przyjmuje tylko wartości nieujemne. Wynika stąd w szczególności, że *najwyższy współczynnik* wielomianu g jest liczbą dodatnią. Rzeczywiście, jeśli $g = cX^n + c_1X^{n-1} + \cdots + c_n$ i $c < 0$, to z równości

$$g(x) = cx^n\left(1 + \frac{c_1}{cx} + \cdots + \frac{c_n}{cx^n}\right)$$

wynika, że dla dużych dodatnich $x \in \mathbf{R}$ wielomian g przyjmuje wartości ujemne.

Lemat 1
Niech $g \in \mathbf{R}[X]$. Jeśli $g(x) \geq 0$ dla każdej liczby rzeczywistej x, to krotność każdego rzeczywistego pierwiastka a wielomianu g jest liczbą parzystą.

Liczba $k \geq 1$ jest krotnością pierwiastka a wielomianu g, jeśli istnieje taki wielomian h, że

$$g = (X-a)^k h \quad \text{oraz} \quad h(a) \neq 0\,.$$

Inaczej mówiąc, krotność to najwyższy wykładnik potęgi jednomianu $X - a$ dzielącej wielomian g.

Dowód
Jeśli $a \in \mathbf{R}$ jest pierwiastkiem wielomianu g o *nieparzystej* krotności, to $g = (X-a)^{2k+1}h$, gdzie $h(a) \neq 0$. Stąd wynika, że wartości wielomianu g – wbrew założeniu – zmieniają znak przy przejściu przez a. ■

Twierdzenie 1
$p(\mathbf{R}[X]) = 2$.

Na przykład,
$$x^4+4=(x^2+2x+2)(x^2-2x+2);$$
ogólnie istnienie takiego rozkładu wynika z Zasadniczego Twierdzenia Algebry, które głosi, że wielomian stopnia ≥ 1 o współczynnikach zespolonych ma zespolony pierwiastek.

Dowód

Każdy wielomian $g \in \mathbf{R}[X]$ można przedstawić jako iloczyn wielomianów stopnia 1 oraz wielomianów stopnia 2 z ujemnymi wyróżnikami. Jeśli więc $g \in \mathbf{R}[X]$ jest sumą kwadratów wielomianów, to na podstawie Lematu 1 i wcześniejszej uwagi o najwyższym współczynniku takiego wielomianu, daje się on przedstawić w postaci
$$g=d(X-a_1)^{2n_1}\cdots(X-a_k)^{2n_k}(X^2+2b_1X+c_1)\cdots(X^2+2b_mX+c_m),$$
gdzie $d, a_1, \ldots, a_k, b_1, c_1, \ldots, b_m, c_m$ są liczbami rzeczywistymi, $d>0$ i wyróżniki $4b_i^2-4c_i$ są ujemne. Każdy trójmian kwadratowy o ujemnym wyróżniku jest sumą kwadratów dwóch wielomianów, bo $X^2+2bX+c=(X+b)^2+(\sqrt{c-b^2})^2$. Stąd i z tożsamości

(1) $$(A^2+B^2)(C^2+D^2)=(AC-BD)^2+(AD+BC)^2$$

wynika przez indukcję, że iloczyn $(X^2+2b_1X+c_1)\cdots(X^2+2b_mX+c_m)$ jest sumą kwadratów dwóch wielomianów. Ponieważ $c(X-a_1)^{2n_1}\cdots(X-a_k)^{2n_k}$ jest kwadratem wielomianu, więc także g jest sumą kwadratów dwóch wielomianów.

Udowodniliśmy więc, że $p(\mathbf{R}[X]) \leq 2$. Wystarczy teraz wskazać taki wielomian $g \in \mathbf{R}[X]$, który jest sumą kwadratów wielomianów należących do $\mathbf{R}[X]$, ale sam nie jest kwadratem w $\mathbf{R}[X]$. Weźmy np. wielomian X^2+1. Gdyby był on kwadratem wielomianu, to byłby kwadratem wielomianu stopnia 1 i wobec tego miałby pierwiastek rzeczywisty, a tak, oczywiście, nie jest. ■

W ciele $\mathbf{R}(X)$ obowiązują dokładnie takie same reguły dla dodawania, odejmowania, mnożenia i dzielenia ułamków, jak w ciele liczb wymiernych.

Ciało $\mathbf{Q}$ liczb wymiernych jest *ciałem ułamków* pierścienia $\mathbf{Z}$ liczb całkowitych. Podobnie można dla pierścienia $\mathbf{R}[X]$ wielomianów utworzyć jego ciało ułamków $\mathbf{R}(X)$, które nazywa się ciałem *funkcji wymiernych* o współczynnikach rzeczywistych i zawiera wszystkie ułamki $\frac{f}{g}$, gdzie $f, g \in \mathbf{R}[X]$ oraz $g \neq 0$. Liczbę Pitagorasa ciała funkcji wymiernych $\mathbf{R}(X)$ zainteresowani Czytelnicy znajdą teraz z łatwością, dowodząc, że $p(\mathbf{R}(X))=2$. (Wskazówka: proszę zauważyć, że dla dowolnych $f, g \in \mathbf{R}[X]$, $g \neq 0$, mamy $f/g=(1/g)^2 fg$.)

Wielomiany dwóch zmiennych

Wyznaczenie liczby Pitagorasa pierścienia $\mathbf{R}[X,Y]$ wielomianów dwóch zmiennych X i Y o współczynnikach rzeczywistych okazuje się bardzo trudne. Rozpatrzymy tak zwany *wielomian Motzkina*
$$f=1+X^2Y^4+X^4Y^2-3X^2Y^2,$$
którego własności sygnalizują, że nie ma analogii w wyznaczaniu liczby Pitagorasa między pierścieniami wielomianów jednej i dwóch zmiennych.

Lemat 2

$f(x,y) \geq 0$ dla każdych $x, y \in \mathbf{R}$, tzn. wielomian f spełnia podstawowy warunek konieczny na to, by mógł być sumą kwadratów wielomianów.

Dowód

Na podstawie twierdzenia o średniej arytmetycznej i geometrycznej mamy
$$\frac{1+x^2y^4+x^4y^2}{3} \geq \sqrt[3]{1\cdot x^2y^4\cdot x^4y^2}=x^2y^2.$$
Stąd wynika, że $f(x,y)=1+x^2y^4+x^4y^2-3x^2y^2 \geq 0$. ■

Lemat 3

Wielomian f jest sumą 4 kwadratów funkcji wymiernych.

Dowód

Zamiast wielomianu f wygodniej będzie rozpatrzyć wielomian $(X^2+1)f$. Tak jak wielomian f przyjmuje on tylko nieujemne wartości i wobec tego ma szansę być sumą kwadratów wielomianów. Zauważamy najpierw, że
$$(X^2+1)f=(X^2+1)(1+X^2Y^4)+(X^2+1)(X^2-3)X^2Y^2=$$
$$=X^4Y^4+1+X^2Y^4+X^2+(X^4-2X^2-3)X^2Y^2.$$
Stąd, zapisując $-3X^2Y^2$ jako $-2X^2Y^2-2X^2Y^2+X^2Y^2$, otrzymujemy
$$(X^2+1)f=(X^2Y^2-1)^2+(XY^2-X)^2+(X^2-1)^2X^2Y^2.$$

Wykazaliśmy więc, że dla pewnych trzech wielomianów A, B i C mamy $(X^2+1)f = A^2 + B^2 + C^2$. Mnożąc obie strony tej równości przez (X^2+1) dostaniemy, dzięki tożsamości (1),

$$(X^2+1)^2 \cdot f = (AX-B)^2 + (BX+A)^2 + (CX)^2 + C^2 .$$

Dzieląc obie strony tej tożsamości przez $(X^2+1)^2$ otrzymamy tezę Lematu. ∎

Lemat 3 nie jest całkiem satysfakcjonujący. Wydaje się, że rozpatrywanie wielomianu $(X^2+1)f$ zamiast f było pójściem na łatwiznę i dało niezbyt elegancki rezultat – przedstawienie wielomianu f w postaci sumy kwadratów *funkcji wymiernych* zamiast sumy kwadratów *wielomianów*. Te pretensje są jednak przedwczesne.

Twierdzenie 2
Wielomian f nie daje się przedstawić jako suma kwadratów wielomianów pierścienia $\mathbf{R}[X,Y]$.

Dowód
Przypuśćmy, że $f = f(X,Y) = f_1^2 + \cdots + f_n^2$, gdzie $f_j = f_j(X,Y) \in \mathbf{R}[X,Y]$, Ponieważ f ma stopień równy 6, więc stopnie wszystkich wielomianów f_j nie przekraczają 3. Z równości $f(X,0)=1$ otrzymujemy $f_1^2(X,0)+\cdots+f_n^2(X,0)=1$, skąd wynika, że $f_j(X,0)$ są wielomianami stałymi. Jeśli więc $f_j(X,0) = a_j \in \mathbf{R}$, to także $f_j(0,0) = a_j$, to znaczy: a_j jest wyrazem wolnym wielomianu f_j.

Podobnie sprawdzamy, że $f_j(0,Y)$ są wielomianami stałymi oraz $f_j(0,Y) = a_j = f_j(0,0)$. Wobec tego wielomian $f_j - a_j$ dzieli się zarówno przez X, jak i przez Y; mając stopień nie większy niż 3 musi być postaci

$$f_j = a_j + (b_j + c_j X + d_j Y) \cdot XY ,$$

gdzie a_j, b_j, c_j, d_j są pewnymi liczbami rzeczywistymi. Porównując współczynniki jednomianu X^2Y^2 w hipotetycznej równości $f = f_1^2 + \cdots + f_n^2$ otrzymujemy $b_1^2 + \cdots + b_n^2 = -3$, sprzeczność. ∎

Wielomiany wielu zmiennych

Problem wyznaczenia liczby Pitagorasa ciała funkcji wymiernych $n \geq 2$ zmiennych $K_n := \mathbf{R}(X_1, \ldots, X_n)$ nad ciałem liczb rzeczywistych jest bardzo trudny i jest otwarty dla $n > 2$.

Wiadomo, że $p(K_n) \geq n+1$ (J.W.S. Cassels, 1964) oraz $p(K_n) \leq 2^n$ (A. Pfister, 1967). Dla $n=2$ te oszacowania wykazują, że $p(K_2) = 3$ lub 4. Ustalenie faktycznej wartości $p(K_2)$ okazało się być niezwykle skomplikowanym zagadnieniem. W 1971 roku J.W.S. Cassels, W.J. Ellison i A. Pfister wykazali, że rozpatrywany wcześniej w tym artykule wielomian Motzkina nie jest sumą trzech kwadratów w K_2 i tym samym udowodnili w końcu, że $p(K_2) = 4$. Ich dowód wykorzystuje bardzo zaawansowane techniki teorii krzywych eliptycznych i nie daje się przenieść na przypadek $n > 2$.

Przypuszcza się, że $p(K_n) = 2^n$ dla wszystkich n, ale dla $n \geq 3$ nie uzyskano żadnego postępu w kierunku dowodu tej hipotezy.

Jest rzeczą interesującą porównać liczbę Pitagorasa pierścienia całkowitego A i jego ciała ułamków K. Z łatwością stwierdza się, że $p(K) \leq p(A)$. Ponadto, dla $A = \mathbf{Z}$ oraz dla $A = \mathbf{R}[X]$ mamy odpowiednio $K = \mathbf{Q}$ oraz $K = \mathbf{R}(X)$ i, jak wiemy, w obydwu przypadkach mamy $p(K) = p(A)$.

Nie jest to jednak obowiązująca reguła. M.D. Choi, Z.D. Dai, T.Y. Lam i B. Reznick udowodnili w 1982 roku, że pierścień wielomianów n zmiennych $(n \geq 2)$ $A = \mathbf{R}[X_1, \ldots, X_n]$ nad ciałem liczb rzeczywistych ma *nieskończoną* liczbę Pitagorasa, podczas gdy dla jego ciała ułamków $K = K_n$ mamy oszacowanie Pfistera $p(K_n) \leq 2^n$. W tej samej pracy udowodniono także inny zaskakujący rezultat: $p(\mathbf{Z}[X]) = \infty$. Z drugiej strony, Y. Pourchet udowodnił, że $p(\mathbf{Q}[X]) = 5$.

Rozwiązanie zadania F 457. Waga mierzy wypadkową sił ciężkości wiadra i wody oraz siły F, z jaką oddziałuje na nią strumień wody. Prędkość wody wpadającej do wiadra obliczamy z zasady zachowania energii

$$\Delta mgh = \frac{\Delta mv^2}{2} \implies v = \sqrt{2gh} .$$

Siła F wynosi

$$F = \frac{\Delta p}{\Delta t} = \frac{\Delta mv}{\Delta t} = Q\sqrt{2gh} .$$

Przeliczając tę siłę na masę i dodając masy wiadra i wody otrzymujemy wskazanie wagi:

$$\frac{Q\sqrt{2gh}}{g} + M + m = 1{,}32\ \mathrm{kg} .$$

Rozwiązanie zadania F 458.
Prędkość cząsteczek wodoru, z których w dominującej części zbudowana była mgławica, obliczamy ze wzoru

$$\frac{mv^2}{2} = \frac{3}{2}\mathrm{k}T ,$$

gdzie k jest stałą Boltzmanna. Z drugiej strony, aby układ był trwały, energia cząsteczek wodoru na powierzchni mgławicy musi być mniejsza od zera

$$\frac{mv^2}{2} - \frac{GMm}{R} < 0 .$$

Stąd

$$R < \frac{2GM}{v^2} = 7{,}1 \cdot 10^{15}\ \mathrm{m} = 0{,}75 \text{ roku świetlnego} .$$

Literatura:

1. J.W.S. Cassels, On the representation of rational functions as sums of squares. *Acta Arith.* **9** (1964), 79–82.
2. J.W.S. Cassels, W.J. Ellison, and A. Pfister, On sums of squares and on elliptic curves over function fields. *J. Number Theory* **3** (1971), 125–149.
3. M.D. Choi, Z.D. Dai, T.Y. Lam, and B. Reznick, The Pythagoras number of some affine algebras and local algebras. *J. Reine Angew. Math.* **336** (1982), 45–82.
4. A. Pfister, Zur Darstellung definiter Funktionen als Summe von Quadraten. *Invent. Math.* **4** (1967), 229–237.
5. Y. Pourchet, Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques, *Acta Arith.* **19** (1971), 89– 104.