Wielomiany

Arkadiusz Męcel

Podstawowe informacje - przypomnienie.

Definicja 1 ***Funkcją wielomianową zmiennej x***, *nazywamy odwzorowanie:* $f : \mathbb{R} \to \mathbb{R}$, *postaci:*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0. \tag{1}$$

Często rozważa się osobno zakres zmiennej i współczynników. Mogą one pochodzić z różnych źródeł. W zależności od wyboru zbioru, do którego należą współczynniki, będziemy pisać $f \in \mathbb{E}[x]$, *gdzie* $\mathbb{E} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$).

Definicja 2 ***Stopniem wielomianu*** $a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0$ *nazywamy liczbę* $st(f) = k \in \mathbb{Z}$, *że* $a_k \neq 0$ *oraz dla każdego* $n > k$ *zachodzi:* $a_n = 0$.

Zwykle będziemy dla uproszczenia zakładać, że we wzorze (1) zachodzi: $a_n \neq 0$.

Definicja 3 ***Pierwiastkiem wielomianu*** *postaci (1) nazywamy taką liczbę* $x_0 \in \mathbb{R}$, *że* $f(x_0) = 0$.

Definicja 4 *Mówimy, że* ***wielomian*** $f \in \mathbb{E}[x]$ ***jest podzielny przez wielomian*** $g \in \mathbb{E}[x]$ *jeśli istnieje wielomian* $h \in \mathbb{E}[x]$ *taki, że dla każdego* $x \in \mathbb{R}$ *zachodzi:* $f(x) = g(x) \cdot h(x)$.

Definicja 5 *Mówimy, że* ***wielomian*** $f \in \mathbb{E}[x]$ ***jest rozkładalny nad*** $\mathbb{E}$, *jeżeli istnieją dwa wielomiany* $g, h \in \mathbb{E}[x]$ *niezerowego stopnia takie, że dla każdego* $x \in \mathbb{R}$ *zachodzi:* $f(x) = g(x) \cdot h(x)$. *Wielomian jest nierozkładalny, jeżeli takie wielomiany nie istnieją.*

Do rozkładalności można podać przykłady nad różnymi $\mathbb{E}$.

Podstawowe twierdzenia nt. wielomianów.

Twierdzenie 1 (O dzieleniu z resztą) *Dla dowolnych niezerowych wielomianów $f, g \in \mathbb{E}[x]$ takich, że $st(f) \geqslant st(g)$ istnieje dokładnie jedna para wielomianów $h, r \in \mathbb{E}[x]$, dla której: $f(x) = h(x)g(x) + r(x)$ przy czym: $st(g) > st(r)$ lub $r(x)$ jest wielomianem zerowym.*

Uwaga: Jeśli $r(x)$ jest wielomianem zerowym, to wielomian f dzieli się przez wielomian g w zbiorze $\mathbb{E}$.

Twierdzenie 2 (Tw. Bezout) *Reszta z dzielenia wielomianu $f \in \mathbb{E}[x]$ przez wielomian $x - a$ jest równa wartości wielomianu $f(x)$ w punkcie a.*

DOWÓD. Mamy $f(x) = (x - a)g(x) + r(x)$. Skoro $st(x - a) = 1$, to na mocy twierdzenia o dzieleniu z resztą, $st(r) = 0$. Zatem dla każdego $x \in \mathbb{R}$, $r(x) = c \in R$. Jednak: $f(a) = (a - a)g(a) + r \Rightarrow f(a) = r$. ■

Liczba a jest pierwiastkiem wielomianu $f(x)$ wtedy i tylko wtedy, gdy f dzieli się przez $x - a$.

Twierdzenie 3 *Wielomian stopnia $n \neq 0$ ma nie więcej niż n pierwiastków.*

DOWÓD. Pokażemy tezę przez indukcję. Jest ona oczywista dla $n = 1$. Załóżmy, że dla $n = k$ wielomian ma nie więcej niż k pierwiastków. Rozważmy wielomian f stopnia k+1. Rozważmy dowolny jego pierwiastek x_0. Zgodnie z wnioskiem, wielomian f jest podzielny przez $x - x_0$. Zatem $f = (x - x_0)g(x)$, dla pewnego wielomianu g stopnia k. Zauważmy, że każdy z pozostałych pierwiastków wielomianu f, jest także pierwiastkiem wielomianu g. Ten jednak zgodnie z założeniem ma nie więcej niż k pierwiastków. Zatem f ma nie więcej niż k+1. ■

Twierdzenie 4 *Wielomian f stopnia n ma dokładnie n pierwiastków $x_1, x_2, \ldots, x_n$. Wówczas zachodzi:*

$$f(x) = a_n((x - x_1)(x - x_2)(x - x_3) \ldots (x - x_n)).$$

DOWÓD. Indukcja. Teza zachodzi oczywiście dla wielomianu stopnia 1. Załóżmy, że zachodzi dla każdego wielomianu stopnia $n = k$. Niech f, stopnia k+1 ma dokładnie k+1 pierwiastków $x_1, x_2, \ldots, x_k, x_{k+1}$. W szczególności f dzieli się przez $(x - x_1)$, zatem jest postaci $f(x) = (x - x_1) \cdot g(x)$, gdzie g jest stopnia k. Jest jasne, że wśród pierwiastków g są liczby $x_2, \ldots, x_k, x_{k+1}$. Jest ich jednak dokładnie k, zatem zgodnie z poprzednim faktem są to wszystkie pierwiastki pierwiastki tego wielomianu, on zaś rozkłada się na iloczyn $a_k((x-x_2)(x-x_3)\ldots(x-x_{k+1}))$. Zauważmy, że współczynnik a_k w wielomianie g jest identyczny ze współczynnikiem a_{k+1} w wielomianie f. Stąd wielomian f ma postać: $f(x) = a_{k+1}((x-x_1)(x-x_2)(x-x_3)\ldots(x-x_{k+1}))$. ■

Twierdzenie 5 (Tw. o wielomianach równych) *Jeżeli dla każdego* $x \in \mathbb{R}$ *zachodzi* $f(x) = g(x)$*, gdzie f,g są wielomianami, wówczas wielomiany te są równych stopni, ponadto współczynniki stojące przy odpowiednich potęgach x są równe.*

Dowód. Łatwe... ■

Twierdzenie 6 (Stopień nieparzysty) *Każdy wielomian stopnia nieparzystego ma pierwiastek rzeczywisty.*

Przykładowe zadania:

Zadanie 1 *Wielomian* $w(x) = x^3 + ax^2 + bx - 6$ *przy dzieleniu przez* $x - 1$ *daje resztę 1, a przy dzieleniu przez* $x - 4$ *daje resztę 6. Wyznacz a i b. (Zał. w* $\in \mathbb{R}[x]$*).*

Zadanie 2 *Pewien wielomian daje przy dzieleniu przez* $x - 5$ *resztę 3, przy dzieleniu przez* $x-11$ *resztę 8, przy dzieleniu przez* $x-2007$ *resztę 1001. Wyznacz resztę z dzielenia tego wielomianu przez* $(x-11)(x-2007)(x-5)$*.*

Zadanie 3 *Udowodnij, że jeżeli wielomian f o współczynnikach całkowitych przyjmuje dla czterech różnych argumentów całkowitych wartość 1, to dla żadnego argumentu całkowitego nie przyjmuje wartości -1.*

Rozw. Wprowadzamy te argumenty, tworzymy wielomian g = f - 1, rozkładamy go na czynniki zgodnie z Bezout, wychodzi, że gdyby f przyjmował -1, to g przyjmowałby -2, a więc -2 byłoby iloczynem pięciu liczb całkowitych, z których co najmniej 4 są różne: $-2 = (x_5 - x_1)(x_5 - x_2)(x_5 - x_3)(x_5 - x_4)h(x_5)$. Sprz.

Wzory Viete'a

Twierdzenie 7 (Wzory Viete'a) *Niech $x_1, x_2, x_3, \ldots, x_n$ będą pierwiastkami wielomianu stopnia n, postaci: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$. Wówczas prawdziwe są wzory:*

$$\begin{cases} x_1 + x_2 + \ldots + x_n = \frac{-a_{n-1}}{a_n} \\ x_1x_2 + x_1x_3 + \ldots x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\ \vdots \\ x_1x_2x_3\ldots x_n = (-1)^n \frac{a_0}{a_n}. \end{cases}$$

Dowód. Indukcja. Dla n=1 dowód jest oczywisty, ponieważ mamy wówczas wzór na pojedynczy pierwiastek równania liniowego. Załóżmy, że dla każdego wielomianu stopnia n, wzory te są prawdziwe. Rozważmy wielomian stopnia n+1, o pierwiastkach: $x_1, x_2, x_3, \ldots, x_n, x_{n+1}$. Zgodnie z tw. Bezout istnieje wielomian g(x) (którego wiodący współczynnik to 1), taki, że: $f(x) = a_{n+1} \cdot (x - x_1) \cdot g(x)$. Wielomian g jest stopnia n, i jego pierwiastkami są $x_2, x_3, \ldots, x_n, x_{n+1}$. Więcej pierwiastków, zgodnie z udowodnionym wcześniej faktem mieć nie może. Zatem są to jego wszystkie pierwiastki, zatem zachodzą dla niego wzory Viete'a i możemy napisać:

$$g(x) = x^n - (x_2 + x_3 + \ldots + x_{n+1})x^{n-1} + \ldots + (-1)^{n+1}(x_2x_3\ldots x_{n+1}).$$

Wymnażając g w takiej postaci przez $a_{n+1} \cdot (x - x_1)$ dostajemy tezę. ■

Przykład 1 *Dany jest wielomian $f(x) = x^3 + 2x^4 + 3x + 4$. Jego pierwiastki to a,b,c. Znajdź $a^2 + b^2 + c^2$.*

Rozwiązujemy zadanie stosując wzory Viete'a. To będzie początek pewnego uogólnienia.

Wzory Newtona

Twierdzenie 8 (Wzory Newtona) *Niech $f(x) = a_n x^n + \ldots + a_1 x + a_0$ będzie wielomianem stopnia n, posiadającym n pierwiastków $x_1, x_2, x_3, \ldots, x_n$. Oznaczmy przez s_k wyrażenie: ${x_1}^k + {x_2}^k + \ldots + {x_n}^k$. Wówczas prawdziwe są wzory:*

$$a_n s_1 + a_{n-1} = 0$$

$$a_n s_2 + a_{n-1} s_1 + 2a_{n_2} = 0$$

$$a_n s_3 + a_{n-1} s_2 + a_{n-2} s_1 + 3a_{n-3}$$

$$\vdots$$

$$a_n s_d + a_{n-1} s_{d-1} + a_{n-2} s_{d-2} + \ldots + a_{n-d+1} s_1 + d \cdot a_{n-d}$$

$$\vdots$$

Przykład 2 *Znajdź sumę czwartych potęg pierwiastków wielomianu:* $7x^3 - 21x^2 + 9x + 2$.

Przykład 3 *Pierwiastkami wielomianu* $f(x) = x^4 - x^3 - x^2 - 1$ *są liczby* a,b,c,d. *Znajdź* $g(a) + g(b) + g(c) + g(d)$, *gdzie* $g(x) = x^6 - x^5 - x^3 - x^2 - x$.

Zadania domowe

1. Udowodnić, że wielomian $f(x) = x^{2007} + x^5 + 1$ nie ma 2007 pierwiastków rzeczywistych.

2. Wyznaczyć wszystkie takie liczby całkowite a, aby wielomian $f(x) = (x - a)(x - 10) + 1$ był iloczynem dwóch wielomianów pierwszego stopnia o współczynnikach całkowitych.

3. Udowodnić, że dla każdej liczby całkowitej c, wartość $f(c)$ wielomianu $f(x) = x^4 - 20x^2 + 4$ jest liczbą złożoną.

4. Niech $f \in \mathbb{Z}[x]$. Załóżmy, że istnieją cztery różne liczby całkowite a, b, c, d takie, że:
$$f(a) = f(b) = f(c) = f(d) = 8.$$
Udowodnij, że nie istnieje liczba całkowita k, dla której $f(k) = 5$.

5. Dla jakich $n \in \mathbb{N}$ wielomian $1 + x^2 + x^4 + \ldots + x^{2n-2}$ jest podzielny przez wielomian $1 + x + x^2 + \ldots + x^{n-1}$?

6. Rozwiązać układ równań:
$$\begin{cases} x + y + z = 3 \\ x^2 + y^2 + z^2 = 3 \\ x^3 + y^3 + z^3 = 3 \end{cases}$$
Wsk. Bez straty ogólności można założyć, że niewiadome są pierwiastkami pewnego wielomianu stopnia 3, gdzie $a_3 = 1$.

7. Dany jest wielomian f(x) stopnia 2 o współczynnikach całkowitych, spełniający następujące warunki:

   (a) Obydwa jego pierwiastki są dodatnimi liczbami całkowitymi;

   (b) Suma współczynników tego wielomianu jest liczbą pierwszą;

   (c) Dla pewnej liczby całkowitej k, $f(k) = 55$.

   Wykaż, że jednym z pierwiastków tego wielomianu jest 2. Znajdź drugi pierwiastek.

Największy wspólny dzielnik

Zacznijmy od przypomnienia sobie definicji największego wspólnego dzielnika dla liczb całkowitych i przypomnienia sobie pokrótce algorytmu Euklidesa. Dalej przypominamy zasadnicze twierdzenie arytmetyki, bez dowodu...

Twierdzenie 9 (Równanie Bezout) *Dla dowolnych niezerowych liczb całkowitych a, b istnieją liczby całkowite n, m, że:*

$$an + bm = \mathrm{nwd}(a, b).$$

Definicja 6 (Największy wspólny dzielnik wielomianów) *Jeżeli dla dwóch wielomianów $f, g \in \mathbb{E}[x]$ istnieje niezerowy wielomian $h \in \mathbb{E}[x]$ taki, że: $h \mid f$, $h \mid g$,to wielomian maksymalnego stopnia, posiadający te własności nazywamy* $\mathrm{nwd}(f, g)$ *w* $\mathbb{E}[x]$.

Twierdzenie 10 (Algorytm Euklidesa) *Największy wspólny dzielnik dwóch wielomianów można wyznaczać przy pomocy algorytmu Euklidesa, tak jak dla dwóch liczb całkowitych. Wielomiany porównujemy przez ich stopień i wykonywanie dzielenia z resztą.*

Przykład 4 *Znajdziemy nwd dla wielomianów:* $f(x) = x^3 + x^2 - 3x - 3$, $g(x) = x^2 + 3x + 2$.

Zaczynamy tak, jak przypadku liczb całkowitych. Wielomian wyższego stopnia dzielimy przez wielomian niższego stopnia. Mamy: $f = (x-2)g + (x+1)$. Reszta jest stopnia niższego niż g, jest więc ok. Jest to jednak wciąż niezerowa reszta! Zatem teraz dzielimy g przez $(x + 1)$. Mamy $g(x) = (x + 2)(x + 1) + 0$. Reszta jest zerowa! Zatem ostatnia niezerowa reszta jest nwd. Zatem jest to $(x + 1)$.

Przykład 5 *Udowodnij, że dla każdej liczby całkowitej n, ułamek:*

$$\frac{n^3 + 2n}{n^4 + 3n^2 + 1}$$

jest nieskracalny.

Twierdzenie 11 (Równanie Bezout) *Dla każdych wielomianów $f, g \in \mathbb{E}[x]$ istnieją wielomiany $w, v \in \mathbb{E}[x]$ takie, że:*

$$f(x)w(x) + g(x)v(x) = \mathrm{nwd}(f(x), g(x)).$$

Wielomiany o współczynnikach całkowitych

Twierdzenie 12 (Pierwiastki wymierne wielomianu) *Dany jest wielomian $f(x) \in \mathbb{Z}[x]$ postaci $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Każdy wymierny pierwiastek tego wielomianu jest postaci: $\frac{p}{q}$, gdzie $q \neq 0$, $NWD(|p|, |q|) = 1$, oraz $p \,|\, a_0$, $q \,|\, a_n$.*

Dowód. Jeżeli dla pewnej liczby wymiernej zachodzi: $f(\frac{p}{q}) = 0$, możemy bez straty ogólności założyć, że $NWD(|p|, |q|) = 1$. Mamy:

$$a_n(\frac{p}{q})^n + \ldots + a_1(\frac{p}{q}) + a_0 = 0.$$

Mnożąc przez Q^n, otrzymamy:

$$a_n p^n + \ldots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Zauważmy, że lewa strona przystaje $a_0 q^n (mod\, p)$, zatem: $a_0 q^n$ dzieli się przez p. Skoro jednak p, q są względnie pierwsze, to q^n nie może się dzielić przez p. Stąd $a_0 \,|\, p$. W identyczny sposób rozważając sytuację modulo q, dostajemy, że $a_n \,|\, q$. ■

Wniosek 1 *Jeżeli wielomian o współczynnikach z $\mathbb{Z}$ ma pierwiastek całkowity p, wówczas $p \,|\, a_0$.*

Twierdzenie 13 *Niech $f(x) = a_n x^n + \ldots + a_1 x + a_0$ będzie wielomianem o współczynnikach całkowitych. Jeżeli liczby b, c są całkowite i różne, to liczba $b - c$ jest dzielnikiem$f(b) - f(c)$.*

Zadanie 4 *Wielomian f ma współczynniki całkowite. Uzasadnić, że jeśli liczba f(5) dzieli się przez 2, a liczba f(2) dzieli się przez 5, to liczba w(7) dzieli się przez 10.*

Korzystając z lematu wnioskujemy, że liczba $5 = 7 - 2$ jest dzielnikiem $f(7) - f(2)$, zaś liczba $f(7) - f(5)$ jest podzielna przez $7 - 5 = 2$. Wiadomo ponadto, że $f(2)$ dzieli się przez 5, zaś $f(5)$ dzieli się przez 2. Z faktu, że 5 jest dzielnikiem liczb $f(7) - f(2)$ oraz $f(2)$ wynika, że liczba 5 jest dzielnikiem $f(7)$. Podobnie dowodzimy, że 2 jest dzielnikiem $f(7)$. Stąd $w(7)$ dzieli się przez 10.

Zadanie 5 *Czy istnieje wielomian $f(x)$ o współczynnikach całkowitych taki, że $f(0) = 19$, $f(1) = 97$, $f(2) = 1997$?*

Twierdzenie 14 (Kryterium Eisensteina) *Załóżmy, że istnieje taka liczba pierwsza p, że dla wielomianu $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}$ zachodzą warunki:*

$$p \nmid a_n \,,\; p \,|\, a_{n-1} \,,\; p \,|\, a_{n-2} \,,\; \ldots \,,\; p \,|a_0 \,,\; p^2 \nmid a_0 \,,$$

wówczas wielomian ten jest nierozkładalny w $\mathbb{Z}$.

Przykład 6 *Wielomian $x^{2007} + 2x + 2$ jest nierozkładalny w $\mathbb{Z}$.*

Przykład 7 *Wielomian $2x^5 + 372x^3 - 111111x + 6$ jest nierozkładalny w $\mathbb{Z}$.*

Przykład 8 *Wielomian $x^4 + 1$ jest nierozkładalny w $\mathbb{Z}$ (weź $x \to x + 1$).*