WIELOMIANY STOPNIA WYŻSZEGO NIŻ DWA

Przypominamy, że wielomianem k–tego stopnia nazywamy funkcję f postaci $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$, gdzie współczynnik a_k jest liczbą różną od 0. Piszemy $\operatorname{st}(f) = k$ lub $\deg(f) = k$. Przyjmujemy, że stopień wielomianu zerowego jest równy $-\infty$.

W tym rozdziale zajmiemy się przedstawianiem wielomianu w postaci iloczynu wielomianów stopnia niższego. Zdefiniujemy dzielenie z resztą, pokażemy, że w zbiorze wszystkich wielomianów można szukać największego wspólnego dzielnika za pomocą algorytmu Euklidesa. Stąd wywnioskujemy twierdzenie o jednoznaczności rozkładu na czynniki nierozkładalne (odpowiednik liczb pierwszych). Ustalimy też związek między znajdowaniem pierwiastków wielomianu i rozkładaniem go na czynniki stopnia niższego.

Niestety w przypadku wielomianów stopnia wyższego znajdowanie pierwiastków jest na ogół trudne. Dlatego podamy przepis na znajdowanie wymiernych pierwiastków wielomianów o całkowitych współczynnikach.

Udowodnimy najpierw, że ,,dla dostatecznie dużych" $|x|$ liczby a_kx^k i $a_0 + a_1x + \cdots + a_kx^k$ mają ten sam znak.

Lemat 12.1
Jeśli k jest liczbą naturalną, $a_0, a_1, \ldots, a_k \in \mathbb{R}$ i $a_k \neq 0$, to istnieje taka liczba rzeczywista $M > 0$, że jeśli $|x| \geqslant M$, to

$$|a_0 + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}| < |a_kx^k|.$$

Dowód. Niech $M = 2 + \frac{|a_0|+|a_1|+\cdots+|a_{k-1}|}{|a_k|}$. Zachodzą oczywiście nierówności $M \geqslant 2 > 1$ i $M > \frac{|a_0|+|a_1|+\cdots+|a_{k-1}|}{|a_k|}$. Załóżmy, że $|x| \geqslant M$. Wtedy $1 < |x|^{k-1}$, $|x| < |x|^{k-1}$, $\ldots$, $|x|^{k-2} < |x|^{k-1}$ oraz $|x| > \frac{|a_0|+|a_1|+\cdots+|a_{k-1}|}{|a_k|}$, zatem

$$|a_0 + a_1x + \cdots + a_{k-1}x^{k-1}| \leqslant |a_0| + |a_1x| + \cdots + |a_{k-1}x^{k-1}| \leqslant$$
$$\leqslant\big(|a_0| + |a_1| + \cdots + |a_{k-1}||x|^{k-1} < |a_kx^k|. \ \blacksquare$$

Czytelnik zechce zastanowić się, w jaki sposób w dowodzie skorzystaliśmy z nierówności $k \geqslant 1$.

Twierdzenie 12.2
Jeśli dla pewnych liczb rzeczywistych a_0, a_1, ... , a_k równość $a_0+a_1x+\cdots+a_kx^k = 0$ zachodzi dla każdej liczby rzeczywistej x, to $0 = a_0 = a_1 = \ldots = a_k$.

Dowód. Jeśli $k \geqslant 1$ i $a_k \neq 0$, to z lematu 12.1 wynika, że dla pewnej liczby rzeczywistej x zachodzi nierówność

$$|a_0 + a_1x + \cdots + a_{k-1}x^{k-1}| < |a_kx^k|.$$

wynika stąd, że

$$|a_0+a_1x+\cdots+a_kx^k| \geqslant |a_kx^k|-|a_0+a_1x+\cdots+a_{k-1}x^{k-1}| > 0,$$

wbrew założeniu. Oznacza to, że muszą być spełnione równości $0 = a_k = a_{k-1} = \ldots = a_1$, więc również $a_0 = 0$. ■

Twierdzenie 12.3 (o jednoznaczności współczynników)
Niech $a_0, a_1, \ldots, a_k, b_0, b_1, \ldots, b_n$ będą takimi liczbami rzeczywistymi, że dla każdej liczby rzeczywistej x zachodzi równość:

$$a_0+a_1x+\cdots+a_{k-1}x^{k-1}+a_kx^k = b_0+b_1x+\cdots+b_{n-1}x^{n-1}+b_nx^n$$

Wtedy $k = n$ i $a_0 = b_0$, $a_1 = b_1$, ... , $a_{k-1} = b_{k-1}$, $a_k = b_k$.

Dowód. Przenosimy wszystkie składniki na jedną stronę i korzystamy z poprzedniego twierdzenia. ■

Uwaga 12.4
Prawdziwe jest twierdzenie mocniejsze — wystarczy założyć, że wartości wielomianów pokrywają się w skończonej liczbie punktów, większej zarówno od $k+1$ i od $n+1$, zob. zad 12.1. ■

Uwaga 12.5
Dzięki twierdzeniu o jednoznaczności współczynników wiemy, że stopień wielomianu jest zdefiniowany poprawnie. ■

Czytelnik bez trudu stwierdzi, że następujące wzory:

$$\mathrm{st}(f + g) \leqslant \max(\mathrm{st}(f), \mathrm{st}(g)), \qquad \mathrm{st}(f \cdot g) \leqslant \mathrm{st}(f) + \mathrm{st}(g)$$

są prawdziwe dla dowolnych wielomianów f i g.

Warto zwrócić uwagę na to, że dzięki umowie o stopniu wielomianu zerowego nie trzeba nic zakładać o f, o g, o $f+g$ lub o fg. W szczególności z drugiego z tych wzorów wynika, że jeśli iloczyn dwóch wielomianów jest wielomianem zerowym, czyli stopień iloczynu jest równy $-\infty$, to stopień co najmniej jednego z wielomianów f, g też musi równy $-\infty$, co oznacza, że co najmniej jeden z nich jest wielomianem zerowym.

Twierdzenie 12.6 (o dzieleniu z resztą)

Niech f i g będą dowolnymi wielomianami, przy czym $\mathrm{st}(g) \geqslant 0$, to istnieje wtedy dokładnie jedna para takich wielomianów q, r, że $f = qg + r$ i jednocześnie $\mathrm{st}(r) < \mathrm{st}(g)$.

Wielomian q nazywamy ilorazem z dzielenia wielomianu f przez wielomian g, a wielomian r — resztą.

Dowód. Jeśli $\mathrm{st}(f) < \mathrm{st}(g)$, to przyjmujemy $q = 0$ i $r = f$. Dalej zakładamy, że $k = \mathrm{st}(f) \geqslant \mathrm{st}(g) = n$. Twierdzenie udowodnimy przez indukcję. Załóżmy, że teza jest prawdziwa dla wszystkich wielomianów f stopnia mniejszego niż k. W dalszym ciągu $f(x) = a_0 + a_1x + \cdots + a_kx^k$, $g(x) = b_0 + b_1x + \cdots + b_nx^n$, przy czym $a_k \neq 0 \neq b_n$.

Stopień wielomianu $f(x) - \frac{a_k}{b_n}x^{k-n}g(x)$ jest mniejszy niż k, zatem na mocy założenia indukcyjnego istnieją takie wielomiany q_1 i r, że $f(x) - \frac{a_k}{b_n}x^{k-n}g(x) = q_1(x)g(x) + r(x)$, przy czym $\mathrm{st}(r) < \mathrm{st}(g)$. Niech $q(x) = q_1(x) + \frac{a_k}{b_n}x^{k-n}$. Wtedy $f = qg + r$ i $\mathrm{st}(r) < \mathrm{st}(g)$. Wykazaliśmy istnienie wielomianów q i r.

Załóżmy, że $f = qg + r = q_1g + r_1$ i $\mathrm{st}(r) < \mathrm{st}(g)$ oraz $\mathrm{st}(r_1) < \mathrm{st}(g)$. Wtedy zachodzi równość $(q - q_1)r = r_1 - r$, zatem $\mathrm{st}(q - q_1) + \mathrm{st}(g) = \mathrm{st}(r_1 - r) < \mathrm{st}(g)$. Wynika stąd, że $\mathrm{st}(q - q_1) < 0$, a to oznacza, że $\mathrm{st}(q - q_1) = -\infty$, więc $q - q_1$ jest wielomianem zerowym. Stąd wynika, że również $r_1 - r$ jest wielomianem zerowym, czyli $r_1 = r$. Udowodniliśmy jednoznaczność wielomianów q i r. ■

Uwaga 12.7

Czytelnik zauważy, że podany dowód różni się od dowodu analogicznego twierdzenia dla liczb całkowitych tym jedynie, że porównywanie liczb zastąpiliśmy porównywaniem stopni wielomianów. ■

Uwaga 12.8

Jeśli $\mathrm{st}(g) = 0$, tzn. gdy wielomian jest niezerową funkcją stałą, to dla każdego wielomianu f istnieje taki wielomian q, że $f = qg$. Można to zdanie wywniskować z twierdzenia o dzieleniu z resztą: istnieją takie wielomiany q, r, że $f = qg + r$ i $\mathrm{st}(r) < \mathrm{st}(g) = 0$, więc $\mathrm{st}(r) = -\infty$, zatem wielomian r jest zerowy. ■

Pokażemy teraz jak można znajdować wielomiany q i r.

Przykład 12.1 Niech $f(x)=3x^4-8x^3+7x^2+2$ oraz $g(x)= =x^2+x+1$. Mamy $f(x)-3x^2g(x)=-11x^3+4x^2+2$. Teraz $-11x^3+4x^2+2-(-11x)(x^2+x+1)=15x^2+11x+2$ i wreszcie $15x^2+11x+2-15(x^2+x+1)=-4x-13$. Wynika stąd, że $3x^4-8x^3+7x^2+2=(3x^2-11x+15)(x^2+x+1)-4x-13$. Widać, że powtórzyliśmy dowód twierdzenia o dzieleniu z resztą w tej sytuacji. Zwykle zapisujemy to tak jak dzielenie liczb:

$$
\begin{array}{l}
\underline{3x^2-11x+15\qquad\qquad\qquad\qquad} \\
(3x^4-8x^3+\ 7x^2+\ 0x+2):(x^2+x+1) \\
\underline{\ 3x^4+3x^3+\ 3x^2\qquad\qquad} \\
\qquad -11x^3+\ 4x^2+\ 0x \\
\qquad \underline{-11x^3-11x^2-11x\qquad} \\
\qquad\qquad\qquad 15x^2+11x+\ 2 \\
\qquad\qquad\qquad \underline{15x^2+15x+15} \\
\qquad\qquad\qquad\qquad -\ 4x-13
\end{array}
$$

Przekonamy się niebawem, że szczególnie ważnym przypadkiem jest dzielenie wielomianów przez wielomiany postaci $x-c$. Horner zaproponował takie postępowanie (algorytm Hornera).

Niech $f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x+a_0$. Załóżmy, że $f(x)=(x-c)q(x)+r$, gdzie r jest liczbą, jako wielomian stopnia mniejszego niż 1. Załóżmy, że

$$q(x)=b_{k-1}x^{k-1}+b_{k-2}x^{k-2}+\cdots+b_1x+b_0\,.$$

Mamy wtedy $(x-c)q(x)+r=$
$=b_{k-1}x^k+(b_{k-2}-cb_{k-1})x^{k-1}+\cdots+(b_0-cb_1)x+r-cb_0$.

Ponieważ równe wielomiany mają równe współczynniki, więc $a_k=b_{k-1}$, $a_{k-1}=b_{k-2}-cb_{k-1}$, ..., $a_1=b_0-cb_1$, $a_0=r-cb_0$. Szukamy liczb b_{k-1}, b_{k-2}, ..., b_0, r. Otrzymujemy wzory: $b_{k-1}=a_k$, $b_{k-2}=cb_{k-1}+a_{k-1}$, $b_{k-3}=cb_{k-2}+a_{k-2}$, ..., $b_0=cb_1+a_1$, $r=cb_0+a_0$.

Przykład 12.2 Podzielimy wielomian $-7x^3+2x^2-13x+6$ przez wielomian $x+2$. Wypisujemy współczynniki wielomianu, który dzielimy:

-7	2	-13	6
-7	$(-2)(-7)+2=$ $=16$	$(-2)16+(-13)=$ $=-45$	$(-2)(-45)+6=$ $=96$

W drugim wierszu wypisaliśmy współczynniki ilorazu oraz resztę pokazując działania prowadzące do ich obliczenia. W wyniku otrzymaliśmy równość:

$$-7x^3 + 2x^2 - 13x + 6 = (x+2)(-7x^2 + 16x - 45) + 96\,. \ \blacksquare$$

Definicja 12.9 (wielomianu unormowanego)
Wielomian, którego współczynnik kierujący jest równy 1 nazywamy unormowanym. ■

Czytelnik stwierdzi bez trudu, że jeśli wielomian unormowany w dzieli wielomian unormowany v i $\mathrm{st}(w) = \mathrm{st}(v)$, to $w = v$.

Jesteśmy gotowi do zdefiniowania największego wspólnego dzielnika dwóch wielomianów.

Definicja 12.10 (największego wspólnego dzielnika)
Największym wspólnym dzielnikiem wielomianów f i g nazywamy **unormowany** wielomian d, który dzieli jednocześnie wielomiany f i g i którego stopień jest największy spośród stopni wszystkich wspólnych dzielników tych wielomianów.
Jeśli stopień największego wspólnego dzielnika wielomianów f, g jest równy 0, to mówimy, że są one względnie pierwsze. ■

Podobnie jak w przypadku liczb całkowitych, można znajdować największy wspólny dzielnik wielomianów f, g za pomocą algorytmu Euklidesa. Mamy bowiem:

$$\begin{array}{lllll}
f & = q_0 g + r_0 & \text{i} & \mathrm{st}(r_0) < \mathrm{st}(g) \\
g & = q_1 r_0 + r_1 & \text{i} & \mathrm{st}(r_1) < \mathrm{st}(r_0) \\
r_0 & = q_2 r_1 + r_2 & \text{i} & \mathrm{st}(r_2) < \mathrm{st}(r_1) \\
\multicolumn{4}{l}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\
r_{n-2} & = q_n r_{n-1} + r_n & \text{i} & \mathrm{st}(r_n) < \mathrm{st}(r_{n-1}) \\
r_{n-1} & = q_{n+1} r_n & &
\end{array}$$

Proces dzielenia z resztą musi się zakończyć, bo stopień niezerowego wielomianu jest nieujemną liczbą całkowitą. Wielomian r_n jest tą niezerową resztą, która ma najmniejszy stopień. Następna reszta musi więc być wielomianem zerowym.

Bardzo proste rozumowanie indukcyjne przekonuje nas o tym, że r_n jest wspólnym dzielnikiem f i g oraz że każdy wspólny dzielnik tych wielomianów jest dzielnikiem r_n. Wynika stąd, że wielomian r_n ma największy stopień wśród wszystkich wspólnych dzielników f i g. Dzieląc r_n przez jego współczynnik kierujący otrzymujemy wielomian unormowany d. Jest on największym wspólnym dzielnikiem wielomianów f i g, bo jest wspólnym dzielnikiem maksymalnego stopnia i jest unormowany. ■

Uwaga 12.11
Największy wspólny dzielnik wielomianów f i g jest wyznaczony jednoznacznie. Załóżmy bowiem, że wielomian d_1 jest największym wspólnym dzielnikiem f i g. Wynika stąd, że d_1 jest dzielnikiem r_n, więc również dzielnikiem d. Ponieważ d i d_1 są unormowanymi wielomianami tego samego stopnia i d_1 jest dzielnikiem d, to $d = d_1$. ■

Wracając do przedostatniego przykładu otrzymujemy:

$3x^4 - 8x^3 + 7x^2 + 2 = (3x^2 - 11x + 15) \cdot (x^2 + x + 1) - 4x - 13$

$x^2 + x + 1 = \big(-\frac{1}{4}x + \frac{9}{16}\big) \cdot \big(-4x - 13\big) + \frac{133}{16}$

$-4x - 13 = \big(-\frac{64}{133}x - \frac{208}{133}\big) \cdot \frac{133}{16}$.

Wobec tego w tym przypadku $n = 1$, $r_1 = \frac{133}{16}$, $d = 1$.

Podobnie jak w przypadku liczb całkowitych wykażemy, że największy wspólny dzielnik dwóch wielomianów f i g można zapisać w postaci $sf + tg$, gdzie s, t są pewnymi wielomianami o współczynnikach rzeczywistych. Z poprzednich rozważań wynika, że można w tej postaci zapisać r_n, tzn. istnieją takie wielomiany s_1 i t_1, że $r_n = s_1 f + t_1 g$. Dzieląc wielomiany s_1 i t_1 przez współczynnik kierujący a wielomianu r_n otrzymujemy równość $d = \frac{1}{a} r_n = sf + tg$, gdzie $s = \frac{1}{a}s_1$ i $t = \frac{1}{a}t_1$.

Otrzymane rezultaty można zebrać w jedno

Twierdzenie 12.12 (o największym wspólnym dzielniku)
Największym wspólny dzielnik wielomianów f i g jest podzielny przez każdy ich wspólny dzielnik. Jest to jedyny wielomian unormowany o tej własności.
Istnieją takie wielomiany s i t, że $\mathrm{nwd}(f, g) = sf + tg$. ■

Odpowiednikiem liczb pierwszych są wielomiany nierozkładalne, a liczb złożonych — wielomiany rozkładalne.

Definicja 12.13 (wielomianu nierozkładalnego)
Wielomianem nierozkładalnym nazywamy taki wielomian, który ma dokładnie dwa (różne) dzielniki unormowane. Wielomian, który ma co najmniej trzy (różne) dzielniki unormowane nazywamy rozkładalnym. ■

Wszystkie wielomiany pierwszego stopnia są nierozkładalne. Wielomiany stopnia drugiego są nierozkładalne wtedy i tylko wtedy, gdy ich wyróżnik jest ujemny. Można udowodnić (w rozdziale poświęconym liczbom zespolonym), że innych wielomianów nierozkładalnych (w zbiorze wielomianów o współczynnikach rzeczywistych) nie ma. Z tego twierdzenia nie będziemy korzystać, dopóki go nie udowodnimy.

Lemat 12.14
Wielomian jest rozkładalny wtedy i tylko wtedy, gdy jest iloczynem wielomianów stopnia niższego.
Dowód. Jeśli wielomian f jest rozkładalny, to ma co najmniej trzy różne dzielniki unormowane. Jedynym unormowanym dzielnikiem stopnia 0 jest jest 1, jedynym dzielnikiem stopnia $\mathrm{st}(f)$ jest iloraz wielomianu f przez jego współczynnik kierujący. Istnieje więc taki unormowany wielomian g, który jest dzielnikiem wielomianu f, że $0 < \mathrm{st}(g) < \mathrm{st}(f)$. Wobec tego $f = gh$ dla pewnego wielomianu h. Ponieważ $\mathrm{st}(f) = \mathrm{st}(g) + \mathrm{st}(h)$, więc $\mathrm{st}(h) < \mathrm{st}(f)$, zatem f jest iloczynem wielomianów stopnia niższego. Jeśli f jest iloczynem wielomianów stopnia niższego, to ma co najmniej jeden taki dzielnik g, że $0 < \mathrm{st}(g) < \mathrm{st}(f)$. Iloraz wielomianu g przez jego współczynnik kierujący jest unormowanym dzielnikiem wielomianu f i jest to trzeci unormowany dzielnik. ■

Twierdzenie 12.15 (o istnieniu rozkładu)
Każdy wielomian stopnia większego od 0 może być przedstawiony w postaci iloczynu wielomianów nierozkładalnych.
Dowód. Dla wielomianów stopnia pierwszego twierdzenie jest prawdziwe, bo one nie są rozkładalne. Załóżmy, że twierdzenie jest prawdziwe dla wielomianów stopnia stopnia $\leqslant n$. Niech f będzie wielomianem stopnia $n+1$. Jeśli f jest nierozkładalny, to jest iloczynem wielomianów nierozkładalnych (złożonym z jed-

nego czynnika). Jeśli wielomian f jest rozkładalny, to istnieją wielomiany takie g i h dodatniego stopnia, że $f = gh$. Z równości $\mathrm{st}(f) = \mathrm{st}(g) + \mathrm{st}(h)$ wynika, że $\mathrm{st}(g) \leqslant n$ i $\mathrm{st}(h) \leqslant n$, więc na mocy założenia indukcyjnego każdy z wielomianów g, h jest iloczynem wielomianów nierozkładalnych, a stąd wynika, że również f jest iloczynem wielomianów nierozkładalnych. ■

Twierdzenie 12.16
Jeśli wielomian nierozkładalny p dzieli iloczyn fg, to p jest dzielnikiem jednego lub obu wielomianów f, g.

Dowód. Załóżmy, że p nie dzieli f. Wtedy $\mathrm{nwd}(f,p) = 1$. Wobec tego istnieją takie wielomiany s i t, że $1 = sf + tp$, zatem $g = sfg + tpg$. Prawa strona tej równości jest podzielna przez p jako suma składników podzielnych przez p, więc strona lewa, czyli wielomian g, też jest podzielna przez p. ■

Uwaga 12.17
W dowodzie korzystaliśmy jedynie z tego, że wielomiany p i f są względnie pierwsze. ■

Twierdzenie 12.18 (o jednoznaczności rozkładu)
Każdy wielomian jest iloczynem skończenie wielu unormowanych wielomianów nierozkładalnych i liczby rzeczywistej różnej od 0. Przedstawienie w postaci takiego iloczynu jest jednoznaczne z dokładnością do kolejności czynników.

Dowód. Istnienie rozkładu jest treścią poprzedniego twierdzenia. Udowodnimy jednoznaczność. Załóżmy, że

$$a \cdot f_1 \cdot f_2 \cdot \ldots \cdot f_k = b \cdot g_1 \cdot g_2 \cdot \ldots \cdot g_m ,$$

gdzie f_1, f_2, $\ldots, f_k$ i g_1, g_2 $, \ldots, g_m$ są nierozkładalnymi wielomianami unormowanymi oraz $a, b \in \mathbb{R} \setminus \{0\}$. Ponieważ iloczyn wielomianów unormowanych jest wielomianem unormowanym, więc współczynnikami kierującymi lewej i prawej strony równości są liczby a i b, a ponieważ wielomian wyznacza swe współczynniki jednoznacznie, więc $a = b$. Stąd wynika, że

$$f_1 \cdot f_2 \cdot \ldots \cdot f_k = g_1 \cdot g_2 \cdot \ldots \cdot g_m .$$

Ponieważ iloczyn $g_1 \cdot g_2 \cdot \ldots \cdot g_m$, dzieli się przez nierozkładalny wielomian f_1, więc jeden z jego czynników dzieli się przez f_1. Bez straty ogólności rozważań przyjmujemy, że f_1 dzieli wielomian g_1. Ponieważ oba te wielomiany są nierozkładalne i unormowane, więc

$f_1 = g_1$, zatem $f_2 \cdot \ldots \cdot f_k = g_2 \cdot \ldots \cdot g_m$. Prosta indukcja kończy dowód. ■

Często znajomość czynników wielomianu ułatwia poznawanie jego własności. Np. znajdowanie pierwiastków sprowadza się do znajdowania pierwiastków czynników, czyli wielomianów niższego stopnia. Niestety nie ma ogólnych metod rozkładania wielomianów na czynniki niższego stopnia. Okazuje się też, że rozkładanie na czynniki i znajdowanie pierwiastków wielomianu to w zasadzie ten sam problem. Wzory na pierwiastki wielomianów stopnia trzeciego i czwartego są skomplikowane i dlatego mało przydatne, zaś dla równań wyższego stopnia w ogóle nie istnieją, co udowodniono na przełomie XVIII w XIX w.

Twierdzenie 12.19 (Bézout)
Resztą z dzielenia wielomianu f przez wielomian $x-c$ jest $f(c)$.
Dowód. Reszta z dzielenia wielomianu f przez wielomian $x-c$ jest wielomianem stopnia mniejszego od 1, czyli stałą. Możemy napisać $f(x) = q(x)(x-c) + r$, gdzie q oznacza iloraz z dzielenia wielomianu f przez wielomian $x-c$, a r — resztę. Dla $x = c$ mamy $f(c) = q(c)(c-c) + r = r$, co kończy dowód twierdzenia. ■

Wniosek 12.20
Liczba c jest pierwiastkiem wielomianu f wtedy i tylko wtedy, gdy wielomian f jest podzielny przez dwumian $x-c$. ■

Uwaga 12.21
Zazwyczaj łatwiej i szybciej można sprawdzić podzielność wielomianu przez $x-c$ stosując np. algorytm Hornera niż obliczać $f(c)$ korzystając z definicji funkcji f. ■

Definicja 12.22 (krotności pierwiastka)
Liczba c jest k–krotnym pierwiastkiem wielomianu f wtedy i tylko wtedy, gdy $(x-c)^k$ jest dzielnikiem wielomianu f. ■

Twierdzenie 12.23 (o sumie krotności pierwiastków)
Suma krotności wszystkich pierwiastków wielomianu nie jest większa od jego stopnia.
Dowód. Niech $c_1, c_2, \ldots, c_n$ będą różnymi liczbami rzeczywistymi, a m_1, m_2, $\ldots$, m_k — liczbami naturalnymi. Wielomiany $(x-c_1)^{m_1}$, $(x-c_2)^{m_2}$, $\ldots$, $(x-c_n)^{m_n}$ są parami względnie

pierwsze. Jeśli wielomian f jest podzielny przez każdy z nich, to jest on podzielny przez ich iloczyn. Stąd natychmiast wynika, że $m_1 + m_2 + \cdots + m_n \leqslant \mathrm{st}(f)$. ■

Jeśli wielomian f jest iloczynem wielomianów stopnia pierwszego, to można łatwo rozwiązać nierówność $f(x) \geqslant 0$. Wtedy istnieją takie liczby rzeczywiste $a, c_1, c_2, \ldots, c_k$ i naturalne $m_1, m_2, \ldots, m_k$, że $f(x) = a(x-c_1)^{m_1}(x-c_2)^{m_2}\ldots(x-c_k)^{m_k}$. Ponieważ kwadraty liczb rzeczywistych są nieujemne, więc można założyć, że $m_1 = m_2 = \ldots = m_k = 1$ [12.1] i $c_1 < c_2 < \ldots < c_k$. Wtedy $f(x) = a(x-c_1)(x-c_2)\ldots(x-c_k)$. Dla każdej liczby $x \in \mathbb{R}$ zachodzą nierówności $x - c_1 > x - c_2 > \ldots > x - c_k$.. Wynika stąd, że jeśli $x > c_k$, to liczby $f(x)$ i a mają taki sam znak. Na przedziale (c_{k-1}, c_k) ich znaki są przeciwne (lub $f(x) = 0$), itd.

Teraz zajmiemy się wymiernymi pierwiastkami wielomianów o współczynnikach całkowitych.

Twierdzenie 12.24 (o pierwiastkach wymiernych)
Jeśli $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ jest wielomianem o współczynnikach całkowitych, liczby $p \in \mathbb{Z}$ i $q \in \mathbb{N}$ są względnie pierwsze a liczba $\frac{p}{q}$ jest pierwiastkiem wielomianu f, to liczba p jest dzielnikiem a_0 a liczba q — dzielnikiem a_n.

Dowód. Po pomnożeniu równości

$$0 = f\left(\tfrac{p}{q}\right) = a_0 + a_1 \tfrac{p}{q} + \cdots a_n \left(\tfrac{p}{q}\right)^n$$

przez liczbę q^n otrzymujemy

$$0 = a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-1} + \cdots + a_{n-1} p^{n-1} q + a_{n-1} p^n .$$

Ponieważ wszystkie składniki z wyjątkiem pierwszego są podzielne przez p, więc również liczba $a_0 q^n$ jest podzielna przez p. Liczby p i q^n są względnie pierwsze, więc liczba p jest dzielnikiem liczby a_0. W taki sam sposób dowodzimy, że liczba q jest dzielnikiem liczby a_n. Dowód został zakończony. ■

Wniosek 12.25
Wymierne pierwiastki wielomianu **unormowanego** o współczynnikach całkowitych są liczbami całkowitymi. ■

[12.1] Np. nierównowności $(x-\sqrt{2})^7>0$ i $x-\sqrt{2}>0$ są równoważne.

Twierdzenie o pierwiastkach wymiernych nie daje żadnych informacji o niewymiernych pierwiastkach wielomianu.

Uwaga 12.26 (o uogólnieniach teorii)
Z wyjątkiem twierdzenia o pierwiastkach wymiernych wszystkie twierdzenia dotyczyły wielomianów, których współczynniki były rzeczywiste. Czytelnik jednak zauważy, że w dowodach korzystaliśmy jedynie z twierdzeń, które już udowodniliśmy. Nigdzie nie korzystaliśmy np. z tego, że istnieją rzeczywiste pierwiastki dowolnego stopnia z liczb nieujemnych. Oznacza to, że te twierdzenia są prawdziwe np. w zbiorze wielomianów o współczynnikach wymiernych, albo o współczynnikach z $\mathbb{Q}(\sqrt{2}\,) = \{x + y\sqrt{2}\colon \quad x, y \in \mathbb{Q}\}$ — chodzi o to, by można było współczynniki dodawać, odejmować, mnożyć i dzielić. Jeśli będziemy rozważać np. tylko wielomiany o współczynnikach wymiernych, to okaże się, że wielomian $x^4 + 1$ jest nierozkładalny. Jednak w zbiorze wielomianów o współczynnikach rzeczywistych jest on rozkładalny:

$$x^4 + 1 = \left(x^2 + 1\right)^2 - 2x^2 = (x^2 - x\sqrt{2} + 1)(x^2 + x\sqrt{2} + 1)\,.$$

Jest on też rozkładalny w zbiorze wielomianów o współczynnikach z $\mathbb{Q}(\sqrt{2}\,)$, ale w zbiorze wielomianów o współczynnikach z $\mathbb{Q}(\sqrt{3}\,)$ jest nierozkładalny. Widać korzyść płynącą z wnioskowania z pewników — można teorię stosować wszędzie tam, gdzie są one spełnione bez konieczności dowodzenia twierdzeń w nowej sytuacji. ■

Na zakończenie podamy jeszcze jedno twierdzenie, które pozwala często badać wielomiany o współczynnikach całkowitych za pomocą twierdzeń, które są prawdziwe w przypadku wielomianów o współczynnikach wymiernych.

Twierdzenie 12.27 (lemat Gaussa)
Jeśli wielomian $w(x) = a_0 + a_1x + \cdots + a_nx^n$ ma współczynniki całkowite i jest iloczynem wielomianów $u(x) = b_0 + b_1x + \cdots + b_kx^k$ oraz $v(x) = c_0 + c_1x + \cdots + c_mx^m$ o współczynnikach wymiernych, to istnieją takie liczby wymierne β i γ, że $\beta \cdot \gamma = 1$ i wielomiany $\beta \cdot u$ oraz $\gamma \cdot v$ mają całkowite współczynniki.

Dowód. Niech liczba q będzie najmniejszym wspólnym mianownikiem ułamków $b_0, b_1, \ldots, b_k$, tzn. istnieją takie liczby całkowite β_0, β_1, …, β_k, że $b_j = \frac{\beta_j}{q}$ dla $j = 0, 1, \ldots, k$, przy czym $\mathrm{nwd}(q,\beta_0,\beta_1,\ldots,\beta_k)=1$, analogicznie niech $c_j=\frac{\gamma_j}{r}$ dla $j=0,1,\ldots,m$, przy czym $\mathrm{nwd}(r,\gamma_0,\gamma_1,\ldots,\gamma_k)=1$.

Aby nie komplikować oznaczeń definiujemy dodatkowe współczynniki w trzech wielomianach: $0=\beta_{k+1}=\beta_{k+2}=\ldots$, $0=\gamma_{m+1}=\gamma_{m+2}=\ldots$, $0=a_{n+1}=a_{n+2}=\ldots$.

Jeśli liczba pierwsza p jest wspólnym dzielnikiem liczby q i wszystkich liczb $\gamma_0,\gamma_1,\ldots$, to możemy zastąpić wielomiany u,v wielomianami pu i $\frac{v}{p}$. Analogicznie postępujemy ze wspólnymi dzielnikami liczb r i $\beta_0,\beta_1,\ldots$

W dalszym ciągu zakładamy, że $\mathrm{nwd}(q,\gamma_0,\gamma_1,\ldots)=1$ oraz $\mathrm{nwd}(r,\beta_0,\beta_1,\ldots)=1$. Z równości $w=u\cdot v$ wynika, że:

$\beta_0\gamma_0=a_0qr$,
$\beta_1\gamma_0+\beta_0\gamma_1=a_1qr$,
$\beta_2\gamma_0+\beta_1\gamma_1+\beta_0\gamma_2=a_2qr$,
$\beta_3\gamma_0+\beta_2\gamma_1+\beta_1\gamma_2+\beta_0\gamma_3=a_3qr$,
$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

Jeśli p jest liczbą pierwszą i $p|q$, to $p|\beta_0$ lub $p|\gamma_0$ — wynika to z pierwszej równości. Załóżmy, że $p\mid\beta_0$. Niech i będzie najmniejszą liczbą naturalną, dla której $p\nmid\beta_i$. Ponieważ $p\mid\beta_0$, $p\mid\beta_1$, $p\mid\beta_2$, $\ldots$, $p\mid\beta_{i-1}$ oraz $p\mid q$, więc z równości

$$\beta_i\gamma_0+\beta_{i-1}\gamma_1+\beta_{i-2}\gamma_2+\cdots+\beta_1\gamma_{i-1}+\beta_0\gamma_i=a_iqr$$

wynika, że $p\mid\gamma_0$. Stąd i z równości

$$\beta_{i+1}\gamma_0+\beta_i\gamma_1+\beta_{i-1}\gamma_2+\beta_{i-2}\gamma_3+\cdots+\beta_1\gamma_i+\beta_0\gamma_{i+1}=a_{i+1}qr$$

wynika, że $p\mid\gamma_1$. Kontynuując to rozumowanie (indukcja) przekonujemy się, że $p\mid\gamma_j$ dla każdej nieujemnej liczby całkowitej j, wbrew założeniu, które uczyniliśmy.

Wykazaliśmy, że liczba pierwsza nie może jednocześnie dzielić liczb q i β_0. Takie samo rozumowanie wyklucza możliwość $p\mid q$ i $p\mid\gamma_0$. Oznacza to, że liczba q nie ma dzielników pierwszych, zatem $q=1$. W taki sam sposób dowodzimy, że $r=1$. W ten sposób wykazaliśmy, że po wstępnych przeróbkach (wielu) polegających na dzieleniu jednego czynnika przez liczbę pierwszą i jednoczesnym mnożeniu drugiego przez tę samą liczbę pierwszą otrzymujemy wielomiany o współczynnikach całkowitych. ■

Na zakończenie tego rozdziału kilka słów o tzw. funkcjach wymiernych.

Definicja 12.28 (funkcji wymiernej)
Funkcją wymierną nazywamy iloraz dwóch wielomianów. Przyjmujemy, że jej dziedziną jest zbiór tych liczb rzeczywistych, dla których mianownik (w postaci nieskracalnej) jest różny od 0. ■

Natychmiast z definicji i z własności wielomianów wynika, że

1° Suma funkcji wymiernych jest funkcją wymierną.

2° Iloczyn funkcji wymiernych jest funkcją wymierną.

3° Wielomiany są funkcjami wymiernymi.

4° Niezerowa funkcja wymierna ma skończenie wiele pierwiastków — są to pierwiastki jej licznika (zakładamy, że funkcja jest zapisana w nieskracalnej postaci).

Zadania

1. Dowieść, że jeśli $x_0 < x_1 < \ldots < x_n$ i $w_0, w_1, \ldots, w_n \in \mathbb{R}$, to istnieje dokładnie jeden taki wielomian f stopnia $\leqslant n$, że $f(x_j) = w_j$ dla każdego $j \in \{0, 1, \ldots, n\}$.

2. Dowieść, że funkcja $\frac{x}{1+x^2}$ nie jest wielomianem.

3! Dowieść, że funkcje $\lfloor x \rfloor$ i $\sqrt[3]{x}$ nie są wielomianami ani nawet funkcjami wymiernymi.

4. Niech f oznacza wielomian o współczynnikach całkowitych, a, b, c — takimi liczbami całkowitymi, że $a \neq b \neq c \neq a$ i $b = f(a)$, $c = f(b)$. Dowieść, że $a \neq f(c)$.

5. Niech $P(x)$ będzie wielomianem stopnia $n > 1$ o współczynnikach całkowitych. Dowieść, że jeżeli $x, y \in \mathbb{Z}$ oraz $P(x) \neq P(y)$, to $|P(x) - P(y)| \geqslant |x - y|$.

Definicja 12.29 (punktu okresowego)
Jeśli $f\colon A \longrightarrow A$ jest funkcją i $\underbrace{f(f \ldots f(f}_{k \text{ liter } f}(x))\ldots)) = x$, to mówimy, że x jest punktem okresowym funkcji f, k jest okresem, najmniejszy okres danego punktu nazywamy podstawowym. ■

6. Niech $P(x)$ będzie wielomianem stopnia $n > 1$ o współczynnikach całkowitych Wykazać, że wielomian P ma co najwyżej n **całkowitych** punktów okresowych.

7. Wykazać, że wielomian $4x(1-x)$ ma dokładnie 2^n punktów okresowych o okresie n.

8. Udowodnić, że wielomian $x^{3k}+x^{3m+1}+x^{3n+2}$ jest podzielny przez wielomian x^2+x+1 dla dowolnych $k, m, n \in \mathbb{N}$.

9! Wielomian $a_0+a_1x+\dots+a_nx^n$ ma n różnych pierwiastków. Wyrazić ich sumę i iloczyn za pomocą liczb $a_0, a_1, \dots, a_n$.

10. Dowieść, że jeśli wielomian o współczynnikach całkowitych przyjmuje wartości nieparzyste dla dwóch kolejnych liczb całkowitych, to nie ma całkowitych pierwiastków.

11. Podać przykład wielomianu o współczynnikach niecałkowitych, którego wartości we wszystkich punktach całkowitych są całkowite.

12. Dowieść, że wielomian $(x+1)(x+2)(x+3)+17$ nie jest iloczynem dwóch wielomianów stopnia $\geqslant 1$, o współczynnikach wymiernych.

13. Dowieść, że jeśli $nx^n - x^{n-1} - \ldots - x - 1 = 0$, to $|x| \leqslant 1$.

14. Znaleźć $a \in \mathbb{Z}$, dla którego $(x-a)(x-10)+1$ jest iloczynem wielomianów stopnia 1, o współczynnikach całkowitych.

15. Znaleźć sumę współczynników wielomianu otrzymanego po otwarciu nawiasów i uporządkowaniu wyrazów następującego wyrażenia $(1-3x+x^2)^{745}(3+2x-4x^2)^{746}$.

16. Dla jakich $a, b \in \mathbb{R}$ wielomian $x^4+ax^3+bx^2-8x+1$ jest kwadratem jakiegoś wielomianu.

17. Rozwiązać nierówność $x^5-3x^4+x^3+5x^2-6x+2 \leqslant 0$.

18. Dowieść, że jeśli wielomian o współczynnikach całkowitych jest podzielny przez $x-\sqrt{2}$, to jest też podzielny przez x^2-2.

19. Wielomian w daje z dzielenia przez $x-a$ resztę A, z dzielenia przez $x-b$ — resztę B. Znaleźć resztę z dzielenia w przez $(x-a)(x-b)$ przy założeniu, że $a \neq b$.

20. Dowieść, że wielomian $nx^{n+2}-(n+2)x^{n+1}+(n+2)x-n$ jest podzielny przez $(x-1)^3$ dla dowolnego $n \in \mathbb{N}$.

21. Dowieść, że $x^5-3x^4+6x^3-3x^3+9x-6$ jest nierozkładalny jako wielomian o współczynnikach wymiernych.

22. Rozwiązać nierówność $\left|\frac{x^2+3x+1}{x^2+4x+1}\right| > 1$.

23. Dowieść, że jeśli wielomian x^4+ax+b ma dwukrotny pierwiastek, to $27a^4 = 256b^3$.

24. Liczby $a_1, a_2, \dots, a_n$ są parami różne i całkowite. Dowieść, że wielomian $(x+a_1)^2(x+a_2)^2 \cdot \ldots \cdot (x+a_n)^2+1$ jest nierozkładalny jako wielomian o współczynnikach wymiernych.

25. Obliczyć $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2$.

26. Dowieść, że $20x^5 + 10x^4 + 15x^3 - 9x^2 + 3x - 3$ jest nierozkładalny jako wielomian o współczynnikach wymiernych.

27. Dowieść, że jeśli w jest takim wielomianem, że $w(1) = 0$ i $v(x) = w(x^n)$ dla $x \in \mathbb{R}$, to wielomian v jest podzielny przez $1 + x + \cdots + x^{n-1}$.

28. Czy każdy wielomian o współczynnikach całkowitych jest sumą kilku sześcianów wielomianów o współczynnikach całkowitych?

29. Czy wielomian $x^{44} + x^{33} + x^{22} + x^{11} + 1$ dzieli się: przez wielomian $x^5 - 1$, a przez — $x^4 + x^3 + x^2 + x + 1$?

30. Rozłożyć na czynniki $x^4(y - z) + y^4(z - x) + z^4(x - y)$.

31. Rozłożyć na czynniki $x^4(y^2 - z^2) + y^4(z^2 - x^2) + z^4(x^2 - y^2)$.

32. Rozłożyć na czynniki $x(y - z)^3 + y(z - x)^3 + z(x - y)^3$.

33. Dowieść, że istnieje taki wielomian w o współczynnikach całkowitych, że , to $0 < |w(x)| < \frac{1}{2010}$ dla $0 < x < 1$.

34. Dla jakich $x \in \mathbb{Z}$ wartości funkcji $\frac{2x-3}{5x+4}$ są całkowite?

35. Wykazać, że jeśli mianownik funkcji wymiernej jest iloczynem dwóch wielomianów względnie pierwszych, to tę funkcję można przedstawić jako sumę dwu funkcji wymiernych, których mianowniki to względnie pierwsze czynniki mianownika.

36. Udowodnić, że funkcja postaci $\frac{ax+b}{cx+d}$ jest albo stała, albo różnowartościowa. Dowieść, że jest ściśle monotoniczna wtedy i tylko wtedy, gdy jest wielomianem stopnia pierwszego.

37. Zdefiniujemy nierówność w zbiorze funkcji wymiernych. Mówimy, że wielomian jest dodatni wtedy i tylko wtedy, gdy jego współczynnik kierujący jest dodatni. Funkcja wymierna jest dodatnia wtedy i tylko wtedy, gdy można przedstawić ją jako iloraz dodatnich wielomianów. Funkcja f jest większa od funkcji g wtedy i tylko wtedy, gdy funkcja $f - g$ jest dodatnia. Dowieść, że w zbiorze funkcji wymiernych z tą nierównością są spełnione wszystkie do tej pory sformułowane aksjomaty teorii liczb rzeczywistych. Czytelnik zechce zauważyć, że w tym przypadku nie działa zasada Archimedesa: wielomian x jest większy od każdej liczby naturalnej.