Funkcje tworzące - duży skrypt

Mateusz Rapicki, Piotr Suwara

9 sierpnia 2012

1 Kombinatoryka

Definicja 1 (dwumian Newtona)**.** $\binom{n}{k}$ dla liczb całkowitych nieujemnych n, k to liczba sposobów wybrania k elementów z n-elementowego zbioru.

Definicja 2 (silnia)**.** $n! = n \cdot (n-1) \cdot \ldots \cdot 1$. $0! = 1$.

Twierdzenie 3. *$n!$ to liczba permutacji zbioru n-elementowego (liczba ustawień n elementów w rzędzie).*

Twierdzenie 4. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *dla* $0 \leqslant k \leqslant n$, $\binom{n}{k} = 0$ *dla* $n < k$.

Twierdzenie 5 (wzór dwumianowy)**.** $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Twierdzenie 6 (zasada szufladkowa Dirichleta)**.** *Jeśli zbiór $nk+1$ różnych elementów podzielimy na n parami rozłącznych podzbiorów, to co najmniej jeden z nich będzie miał co najmniej $k+1$ elementów.*

Twierdzenie 7 (zasada włączeń i wyłączeń)**.** *Dla zbiorów $S_1, S_2, \ldots, S_n$:*

$$|S_1 \cup S_2 \cup \ldots \cup S_n| = \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} (-1)^k |S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}|.$$

2 Liczby zespolone

2.1 Podstawy

Definicja 8. Liczby zespolone to zbiór $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, gdzie i jest pewnym symbolem. Możemy je utożsamiać z punktami na płaszczyźnie, tj. $a + bi$ utożsamiamy z punktem o współrzędnych (a, b). Definiujemy działania w taki sposób, że $i^2 = -1$:

- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$

Definicja 9 (długość)**.** Dla $z = a + bi \in \mathbb{C}$ definiujemy długość (moduł): $|z| = \sqrt{a^2 + b^2}$.

Definicja 10 (sprzężenie)**.** Sprzężeniem liczby $z = a+bi \in \mathbb{C}$ nazwiemy liczbę $\bar{z} = a-bi \in \mathbb{C}$.

Twierdzenie 11. $z\bar{z} = |z|^2$

Twierdzenie 12. *Liczbą odwrotną do* $a + bi$ *jest* $\frac{\bar{z}}{|z|^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$.

2.2 Postać biegunowa

Definicja 13 (postać biegunowa)**.** Liczbę $z = a+bi$ możemy zapisać w postaci $z = r(\cos\alpha + i\sin\alpha)$ dla $r = |z|$ oraz $\alpha = \operatorname{arctg}\frac{b}{a}$.

Kąt α nazywamy *argumentem* liczby z i oznaczamy Arg z.

W ten sposób możemy patrzeć na liczbę zespoloną z jako na wektor długości $r = |z|$ nachylony pod kątem α do dodatniej półosi rzeczywistej.

Twierdzenie 14. *Jeśli* $z = |z|(\cos\alpha + i\sin\alpha), w = |w|(\cos\beta + i\sin\beta)$*, to* $zw = |z| \cdot |w| \cdot (\cos(\alpha+\beta) + i\sin(\alpha+\beta))$.

Czyli mnożenie liczb zespolonych to mnożenie ich długości oraz dodawanie ich argumentów.

Twierdzenie 15 (wzór de Moivre'a)**.** $z = |z|(\cos\alpha + i\sin\alpha)$*, wtedy* $z^n = |z|^n(\cos n\alpha + i\sin n\alpha)$

2.3 Pierwiastki z jedności

Definicja 16. Pierwiastkiem z 1 stopnia n nazwiemy taką liczbę zespoloną z, że $z^n = 1$. Inaczej mówiąc, z jest pierwiastkiem wielomianu $P(x) = z^n - 1$.

Twierdzenie 17. *Jeśli* z *jest pierwiastkiem z jedności stopnia* n*, to istnieje takie* $0 \leqslant k \leqslant n-1$*, że* $z = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$.

O liczbach zespolonych możecie przeczytać na przykład na Wikipedii `http://pl.wikipedia.org/wiki/Liczby_zespolone` lub na stronie `http://www.ift.uni.wroc.pl/~cislo/algebra/wyklad5.pdf`.

3 Pochodne

3.1 Definicja

Definicja 18. Niech $f : \mathbb{R} \to \mathbb{R}, x_0 \in \mathbb{R}$. Wówczas, jeżeli istnieje granica $\lim_{x\to x_0} \frac{f(x)-f(x_0)}{x-x_0}$ to nazywamy ją pochodną (albo różniczką) funkcji f w punkcie x_0 i oznaczamy $f'(x_0)$.

Zasadniczo, nie będziemy korzystać z tej definicji, lecz z kilku podstawowych własności pochodnych oraz znajomości pochodnych dla kilku ważnych funkcji. Często spotykany jest zapis $(f(x))'$. Zwykle oznacza on $f'(x)$.

3.2 Podstawowe własności

Twierdzenie 19. *Niech $f, g : \mathbb{R} \to \mathbb{R}, x, c \in \mathbb{R}$ oraz istnieją pochodne $f'(x)$ oraz $g'(x)$. Wówczas zachodzą następujące równości:*
Liniowość pochodnej: $(f+g)'(x) = f'(x) + g'(x), \quad (c \cdot f)'(x) = c \cdot f'(x)$.
Wzór na pochodną iloczynu: $(f \cdot g)'(x) = f'(x)g(x) + f(x)g'(x)$.
Wzór na pochodną ilorazu, prawdziwy o ile $g(x) \neq 0$*:* $\left(\frac{f}{g}\right)'(x) = \frac{f'(x)g(x) - f(x)g'(x)}{(g(x))^2}$.
Wzór na pochodną złożenia: $(g \circ f)'(x) = g'(f(x)) \cdot f'(x)$.

3.3 Pochodne popularnych funkcji

Twierdzenie 20. $\forall_{\alpha \in \mathbf{R}} (x^\alpha)' = \alpha x^{\alpha-1}$, *o ile wyrażenie* x^α *ma sens*
$(e^x)' = e^x$
$\ln'(x) = \frac{1}{x}$, *o ile* $x > 0$
$\sin'(x) = \cos(x)$
$\cos'(x) = -\sin(x)$

4 Funkcje tworzące

Definicja 21 (funkcja tworząca)**.** *Funkcją tworzącą* (szeregiem formalnym) ciągu (a_n) nazywamy szereg formalny $A(x) = \sum_{n \geqslant 0} a_n x^n = \sum_n a_n x^n$, dla uproszczenia zapisu przyjmujemy $a_{-1} = a_{-2} = \ldots = 0$.

Definicja 22 (operacje na funkcjach tworzących)**.** $F(x)$ funkcja tworząca ciągu (f_n), $G(x)$ funkcja tworząca ciągu (g_n).

- $\alpha F(x) + \beta G(x) = \sum_n (\alpha f_n + \beta g_n) x^n$
- $x^k G(x) = \sum g_{n-k} x^n$,
- $x^{-k} \left(G(x) - \sum_{j=0}^{k-1} g_j x^j \right) = \sum_{n \geqslant 0} gn + kx^n$,
- $G(cx) = \sum c^n g_n x^n$,
- różniczkowanie: $G'(x) = \sum (n+1) g_{n+1} x^n$,
- $xG'(x) = \sum n g_n x^n$,
- całkowanie: $\int_0^x G(t)\, dt = \sum_{n \geqslant 1} \frac{1}{n} g_{n-1} x^n$,
- mnożenie: $F(x)G(x) = \sum_n \left(\sum_k f_k g_{n-k} \right) x^n$,
- w szczególności $\frac{1}{1-x} G(x) = \sum_n \left(\sum_{k \leqslant n} g_k \right) x^n$.

Definicja 23 (wykładnicza funkcja tworząca)**.** *Wykładniczą funkcją tworzącą* ciągu (a_n) nazywamy szereg formalny $A(x) = \sum_{n\geqslant 0} a_n \frac{x^n}{n!} = \sum_n a_n \frac{x^n}{n!}$, dla uproszczenia zapisu przyjmujemy $a_{-1} = a_{-2} = \ldots = 0$.

Definicja 24 (operacje na wykładniczych funkcjach tworzących)**.** $F(x)$ wykładnicza funkcja tworząca ciągu (f_n), $G(x)$ wykładnicza funkcja tworząca ciągu (g_n).

- $\alpha F(x) + \beta G(x) = \sum_n (\alpha f_n + \beta g_n) \frac{x^n}{n!}$
- $G(cx) = \sum c^n g_n \frac{x^n}{n!}$,
- różniczkowanie: $G^{(k)}(x) = \sum_{n\geqslant 0} g_{n+k} \frac{x^n}{n!}$,
- $xG'(x) = \sum n g_n \frac{x^n}{n!}$,
- całkowanie: $\int_0^x G(t)\ dt = \sum g_{n-1} \frac{x^n}{n!}$,
- mnożenie: $F(x)G(x) = \sum_n \left(\sum_k \binom{n}{k} f_k g_{n-k} \right) \frac{x^n}{n!}$,

Definicja 25 (funkcje analityczne)**.** *Funkcje analityczne* to takie, które rozwijają się w szereg, tj. $f(x)$ jest analityczna w otoczeniu x_0, jeśli zachodzi w nim:

$$f(x) = f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + \ldots + \frac{f^{(n)}(x_0)}{n!}(x - x_0)^n + \ldots.$$

Mówimy, że funkcja rozwija się w szereg Taylora w x_0. Jeśli $x_0 = 0$, to mamy szereg Maclaurina:

$$f(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + \ldots.$$

Twierdzenie 26. *Funkcje: stała, x^a (w tym wielomiany), wykładnicza e^x, logarytmiczna $\ln x$, funkcje trygonometryczne, są analityczne (tam, gdzie są dobrze określone).*

Funkcje: odwrotna do analitycznej, suma funkcji analitycznych, iloczyn funkcji analitycznych, iloraz funkcji analitycznych, złożenie funkcji analitycznych są analityczne (tam, gdzie są dobrze określone).

Funkcje tworzące często wolimy analizować w *postaci zwartej*. Korzystając ze wzoru na szereg Maclaurina funkcji otrzymujemy wzory:

Twierdzenie 27.

- $x^m = \sum_{n\geqslant 0} [n = m] x^n$, *gdzie* $[n = m] = \delta_{nm}$ *jest równe 1 wtedy i tylko wtedy, gdy* $n = m$, *oraz 0 w przeciwnym przypadku.*
- $\frac{1}{1-x} = \sum_{n\geqslant 0} x^n$
- $(1 + x)^c = \sum_{n\geqslant 0} \binom{c}{n} x^n$
- $\frac{1}{(1-x)^c} = \sum_{n\geqslant 0} \binom{c+n-1}{n} x^n$

- $\ln \frac{1}{1-x} = \sum_{n \geqslant 1} \frac{1}{n} x^n$
- $\ln(1+x) = \sum_{n \geqslant 1} \frac{(-1)^{n+1}}{n} x^n$
- $e^x = \sum_{x \geqslant 0} \frac{1}{n!} x^n$ *[jest to poniekąd definicja funkcji wykładniczej]*
- $\cos x = \sum_{n \geqslant 0} \frac{(-1)^n}{(2n)!} x^{2n}$
- $\sin x = \sum_{n \geqslant 0} \frac{(-1)^n}{(2n+1)!} x^{2n+1}$
- $\frac{x}{e^x - 1} = \sum_{x \geqslant 0} \frac{B_n x^n}{n!}$
- $\frac{1}{2x}(1 - \sqrt{1-4x}) = \sum_n \frac{1}{n+1} \binom{2n}{n} x^n$
- $\frac{1}{\sqrt{1-4x}} = \sum_n \binom{2n}{n} x^n$
- $\frac{1}{\sqrt{1-4x}} \left(\frac{1-\sqrt{1-4x}}{2x} \right)^k = \sum_n \binom{2n+k}{n} x^n$

5 Wielomiany

Definicja 28. Zbiór wielomianów o współczynnikach w R będziemy oznaczać jako $R[x]$, na przykład $\mathbb{R}[x]$ to wielomiany o współczynnikach rzeczywistych, $\mathbb{Q}[x]$ – wymiernych, $\mathbb{Z}[x]$ – całkowitych, $\mathbb{C}[x]$ – zespolonych.

Definicja 29. *Wielomian unormowany* to taki, którego współczynnik wiodący (przy najwyższej potędze x) jest równy 1.

Definicja 30. Liczby rzeczywiste $\mathbb{R}$, liczby wymierne $\mathbb{Q}$, liczby zespolone $\mathbb{C}$ będziemy nazywać *ciałami*.

Dokładna definicja ciała jest znacznie ogólniejsza i nie podajemy jej tu – ważne jest, że w każdym ciele można: dodawać i mnożyć w sposób przemienny i łączny (czytaj: tak, jak zawsze to robisz), odwracać elementy niezerowe, znaleźć 0 oraz 1. Innymi ciałami niż powyższe nie będziemy się zajmować. Zauważmy, że $\mathbb{Z}$ nie jest ciałem, bo nie każdy element z $\mathbb{Z}$ można odwrócić, otrzymując przy tym element z $\mathbb{Z}$ (np. $2 \in \mathbb{Z}$, ale $\frac{1}{2} \notin \mathbb{Z}$).

Definicja 31. Ponieważ $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, to zakładamy, że słowo *wielomian* oznacza *wielomian o współczynnikach zespolonych.*

Definicja 32. Wielomian $P(x)$ dzieli wielomian $Q(x)$, jeśli istnieje taki wielomian $R(x)$, że $Q(x) = P(x)R(x)$.

Twierdzenie 33. *Jeśli dla pewnego ciała k (tj. $k \in \mathbb{Q}, \mathbb{R}, \mathbb{C}$) zachodzi $P(x) \in k[x], Q(x) \in k[x]$ (tj. P oraz Q mają współczynniki w ciele k) oraz $Q(x) = P(x)R(x)$ dla pewnego wielomianu $R(x)$, to wielomian $R(x)$ ma współczynniki w tym samym ciele k, czyli $R(x) \in k[x]$.*

Powyższe twierdzenie jest bardzo łatwe do udowodnienia i bardzo ważne. Inaczej mówiąc, oznacza ono, że podzielność w pewnym ciele (np. $\mathbb{R}$) jest tym samym, co podzielność w większym ciele (np. $\mathbb{C}$).

Twierdzenie 34 (Bézout)**.** *Dla dowolnego a, jeśli $P(x)$ to wielomian, wtedy istnieje dokładnie jeden taki wielomian $Q(x)$, że*

$$P(x) = (x-a)Q(x) + P(a).$$

Co więcej, jeśli dla ciała k zachodzi $a \in k, P(x) \in k[x]$, to także $Q(x) \in k[x]$. Wynika to wprost z poprzedniego twierdzenia, bo przy tych założeniach $P(x) - P(a) \in k[x]$ dzieli się przez $(x-a) \in k[x]$. Przypomnijmy, za k można wstawić dowolne ciało: $\mathbb{Q}, \mathbb{R}$ lub $\mathbb{C}$.

Definicja 35 (największy wspólny dzielnik)**.** Dla wielomianów $P(x), Q(x)$ największym wspólnym dzielnikiem jest taki wielomian $R(x)$, który ma największy możliwy stopień i dzieli jednocześnie $P(x)$ oraz $Q(x)$. Oznaczamy $(P(x), Q(x)) = R(x)$.

Jest on określony z dokładnością do współczynnika wiodącego.

Twierdzenie 36 (algorytm Euklidesa)**.** *Dla dowolnych wielomianów $P(x), Q(x), R(x)$ zachodzi $(P(x), Q(x)) = (P(x), Q(x) - R(x)P(x))$.*

Posługując się algorytmem Euklidesa analogicznym do przypadku teorioliczbowego, możemy łatwo obliczać największy wspólny dzielnik dwóch wielomianów [mając $P(x), Q(x)$, gdy stopień P jest nie mniejszy niż stopień Q, mnożymy $Q(x)$ przez $R(x) = ax^n$ tak, aby stopień $P(x) - R(x)Q(x)$ był mniejszy niż stopień $P(x)$ przynajmniej o 1.

Mając dowolne ciało k oraz $P(x), Q(x) \in k[x]$, możemy zawsze tak dobierać $R(x)$, aby $R(x) \in k[x]$. Pokazuje to, że

Twierdzenie 37. *Jeśli $P(x), Q(x) \in k[x]$ dla pewnego ciała k, to $(P(x), Q(x)) \in k[x]$.*

Twierdzenie 38 (zasadnicze twierdzenie algebry)**.** *Każdy wielomian ma pierwiastek w $\mathbb{C}$, to znaczy dla każdego wielomianu $P(x)$ istnieje takie $x_0 \in \mathbb{C}$, że $P(x_0) = 0$.*

Z twierdzenia Bézout wynika, że jeśli $P(x_0) = 0$, to $P(x) = (x - x_0)Q(x)$ dla pewnego wielomianu $Q(x)$. Następnie znajdujemy x_1 takie, że $Q(x_1) = 0$ i mamy $P(x) = (x - x_0)Q(x) = (x - x_0)(x - x_1)R(x)$. Kontynuując, otrzymujemy

Twierdzenie 39. *Każdy wielomian rozkłada się na czynniki liniowe w $\mathbb{C}$, to znaczy dla każdego wielomianu P istnieją takie liczby $a, w_1, \ldots, w_n \in \mathbb{C}$, że $P(x) = a(x - w_1)(x - w_2)\ldots(x - x_n) = a\prod_{i=1}^{n}(x - w_i)$.*

Definicja 40. Jeśli w jest pierwiastkiem $P(x)$ oraz $P(x) = a\prod_{i=1}^{n}(x - w_i)$, to krotnością pierwiastka w jest liczba wystąpień w w ciągu $w_1, \ldots, w_n$. Równoważnie, k jest krotnością w, jeśli $P(x) = (x - w)^k Q(x)$ oraz $Q(w) \neq 0$.

Twierdzenie 41 (wzory Viete'a). *Jeśli* $P(x) = \sum_{k=0}^{n} a_k x^k = a_n \prod_{i=1}^{n}(x - w_n)$ *dla* $a_n \neq 0$, *to zachodzą równości:*

$$\begin{aligned}
\sum_{i=1}^{n} w_i &= -\frac{a_{n-1}}{a_n} \\
\sum_{1 \leqslant i_1 < i_2 \leqslant n} w_{i_1} w_{i_2} &= \frac{a_{n-2}}{a_n} \\
&\vdots \\
\sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} w_{i_1} \ldots w_{i_k} &= (-1)^k \frac{a_{n-k}}{a_n} \\
&\vdots \\
w_1 w_2 \ldots w_n &= (-1)^n \frac{a_0}{a_n}
\end{aligned}$$

Twierdzenie 42 (lemat Gaussa). *Jeśli wielomian unormowany* $P(x) \in \mathbb{Z}[x]$ *rozkłada się na iloczyn wielomianów unormowanych* $Q(x), R(x) \in \mathbb{Q}[x]$, *czyli* $P(x) = Q(x)R(x)$, *to* $Q(x), R(x) \in \mathbb{Z}[x]$, *czyli te wielomiany też mają współczynniki całkowite.*

Twierdzenie 43 (kryterium Eisensteina). *Niech* $P(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. *Jeśli* $p | a_k$ *dla* $k = 0, 1, \ldots, n-1$ *oraz* $p \nmid a_n$ *oraz* $p^2 \nmid a_0$, *to wielomian* $P(x)$ *jest nierozkładalny w* $\mathbb{Z}[x]$.

Twierdzenie 44 (o jednoznaczności rozkładu). *Każdy wielomian w* $\mathbb{R}[x]$ *(odpowiednio: w* $\mathbb{Q}[x], \mathbb{Z}[x]$*) rozkłada się jednoznacznie (z dokładnością do kolejności oraz stałych czynników) na iloczyn wielomianów nierozkładalnych w* $\mathbb{R}[x]$ *(odpowiednio: w* $\mathbb{Q}[x], \mathbb{Z}[x]$*).*