

ARYTMETYKA PIERŚCIENIA LICZB CAŁKOWITYCH

Arytmetyka pierścienia liczb całkowitych i wielomianów jest analogiczna, dlatego najpierw prześledzimy poniżej zagadnienie podzielności i rozkładu na czynniki w $(\mathbf{Z}, +, *)$.

Def. Liczba całkowita b nazywa się **dzielnikiem** liczby a (lub a wielokrotnością b), jeśli istnieje taka liczba całkowita q , że $qb = a$. Oznaczamy $b \mid a$.

Wn.1 Dla każdego $a \in \mathbf{Z}$ mamy $\pm 1 \mid a$ (dzielnikiem każdej liczby jest ± 1) oraz $a \mid 0$.

Tw. (o dzieleniu z resztą)

Dla każdej pary liczb całkowitych, a i b , gdzie $b \neq 0$, istnieje jedna i tylko jedna para liczb całkowitych, q i r (zwanych ilorazem i resztą), dla których

$$a = qb + r \text{ i } 0 \leq r < |b|.$$

Dowód pomijamy.

Wn.2 Warunki $b \mid a$ i $r = 0$ są równoważne.

Def. Liczba d nazywa się **wspólnym dzielnikiem** liczb x, y, z, \dots , jeśli $d \mid x, d \mid y, d \mid z, \dots$

Największym wspólnym dzielnikiem liczb x, y, z, \dots , z których choć jedna jest różna od zera, nazywamy największy ze wszystkich wspólnych dzielników liczb x, y, z, \dots , co ozn. (x, y, z, \dots) .

Algorytm Euklidesa

Procedura wyznaczania największego wspólnego dzielnika (NWD) dwóch liczb całkowitych.

Dla a_0 i $a_1 > 0$ mamy wobec tw. o dzieleniu z resztą:

$$a_0 = q_1 a_1 + a_2 \quad \text{i} \quad 0 \leq a_2 < a_1;$$

jeśli $a_2 > 0$, to dzieląc a_1 przez a_2 , tzn. stosując ponownie tw. o dzieleniu z resztą, daje

$$a_1 = q_2 a_2 + a_3 \quad \text{i} \quad 0 \leq a_3 < a_2,$$

i dalej postępując analogicznie otrzymujemy ciąg równości:

$$a_{n-1} = q_n a_n + a_{n+1} \quad \text{i} \quad 0 \leq a_{n+1} < a_n, \quad (*)$$

aż w końcu: $a_n = q_{n+1} a_{n+1} + a_{n+2}$ i $a_{n+2} = 0$, gdyż $0 \leq a_{n+1} < a_n < \dots < a_3 < a_2 < a_1$.

Niezerowa reszta a_{n+1} nazwana jest ostatnią resztą.

Tw. Ostatnia reszta jest największym wspólnym dzielnikiem liczb a_0 i a_1 , tzn.

$$a_{n+1} = (a_0, a_1).$$

Dowód: Ponieważ $a_{n+2} = 0$, więc $a_{n+1} \mid a_n$, ale wówczas wobec (*) również $a_{n+1} \mid a_{n-1}$, itd, co znaczy że a_{n+1} jest dzielnikiem wszystkich liczb a_n, a_{n-1}, \dots, a_2 , oraz a_1 i a_0 .

Pozostaje do wykazania, że a_{n+1} jest największym dzielnikiem liczb a_1 i a_0 , tzn. jeśli d jest dzielnikiem tych liczb, to również $d \mid a_{n+1}$ i $d \leq a_{n+1}$. Istotnie, wobec równości w algorytmie Euklidesa, jeśli d jest dzielnikiem liczb a_1 i a_0 , to i $d \mid a_2$, a następnie $d \mid a_3$, itd. aż $d \mid a_{n+1}$ co wynika z (*). Stąd, oraz wobec warunku $0 < a_{n+1}$ otrzymujemy $d \leq a_{n+1}$, c.b.d.o.

Wn.3 Dla dwóch liczb a_0 i $a_1 > 0$, istnieją takie liczby całkowite x i y , że

$$a_0 x + a_1 y = (a_0, a_1).$$

Dowód polega na wykorzystaniu równań algorytmu Euklidesa, co pokażemy na przykładzie:

Przykład (algorytm Euklidesa)

Niech $a_0 = 273$ i $a_1 = 132$. Algorytm Euklidesa daje:

$$273 = 132 * 2 + 9$$

$$132 = 9 * 14 + 6$$

$$9 = 6 * 1 + 3$$

$$6 = 3 * 2 + 0.$$

Ostatnia resztą jest więc 3, tzn. $(273, 132) = 3$.

Z powyższych równości rugując kolejne reszty mamy odpowiednio:

$$\begin{aligned} 3 &= 9 - 6 * 1 = 9 - (132 - 9 * 14) = (273 - 132 * 2) - (132 - (273 - 132 * 2) * 14) = \\ &= 273 - 132 * 2 - 132 + 273 * 14 - 132 * 28 = 273 * 15 + 132 * (-31), \end{aligned}$$

co daje $x = 15$ i $y = -31$ w rozkładzie NWD liczb 273 i 132 we Wn.3.

Wn.4 Prawo łączności dla NWD: $(a_0, a_1, a_2, a_3, \dots, a_n) = (a_0, (a_1, a_2, a_3, \dots, a_n))$.

Wn.5 O wielokrotności NWD: $(b a_0, b a_1, b a_2, b a_3, \dots, b a_n) = |b| * (a_0, a_1, a_2, a_3, \dots, a_n)$

Def. Liczby a i b nazywamy **względnie pierwszymi**, jeśli $(a, b) = 1$,

(wtedy istnieją takie liczby całkowite x i y , że $a*x + b*y = 1$).

Tw. (**zasadnicze tw. arytmetyki liczb naturalnych**)

Jeśli $(a, b) = 1$ i $a \mid (b*c)$, to $a \mid c$.

Dowód: Mamy $a*x + b*y = 1$, co mnożymy przez c : $a*c*x + b*c*y = c$.

Ponieważ $a \mid (a*c)$ i z założenia $a \mid (b*c)$, to $a \mid (a*c*x + b*c*y)$ i dlatego $a \mid c$, c.b.d.o.

Wn.6 Ponieważ liczbą pierwszą $p > 1$ jest liczba której dzielnikiem jest jedynie 1 i p , to łatwo stwierdzić, że jeśli $p \mid (b*c)$, to $p \mid b$ lub $p \mid c$ – sprawdzić!

Tw. (o rozkładzie na czynniki pierwsze)

Każda liczba naturalna $a > 1$ daje się jednoznacznie przedstawić w postaci iloczynu liczb pierwszych.

Dowód pomijamy.

Przykład.

Każdą liczbę naturalną można przedstawić w postaci iloczynu potęg kolejnych liczb pierwszych, np.

$$30 = 2^1 * 3^1 * 5^1 * 7^0 * 11^0 * 13^0 * 17^0 * 19^0 * 23^0 * \dots, \text{ albo}$$

$$700 = 2^2 * 3^0 * 5^2 * 7^1 * 11^0 * 13^0 * 17^0 * 19^0 * 23^0 * \dots .$$

Def. Dla dwóch liczb całkowitych a i b oraz ich rozkładów na czynniki pierwsze w postaci

$$a = \pm \prod_j p_j^{k_j}, \quad b = \pm \prod_j p_j^{l_j},$$



gdzie wykładniki są liczbami nieujemnymi: $0 \leq k_j, l_j$ dla dowolnego $j = 1, 2, \dots$ **najmniejszą wspólną wielokrotnością (NWW)** liczb a i b nazywamy liczbę

$$[a, b] = \prod_j p_j^{n_j}, \text{ gdzie } n_j = \max(k_j, l_j) \text{ dla każdego } j = 1, 2, \dots$$

Przykład.

Dla liczb 30 i 700 z powyższego przykładu mamy maksymalne wykładniki rozkładów:

$$n_1 = 2, n_2 = 1, n_3 = 2, n_4 = 1, n_5 = 0, n_6 = 0, \text{ itd.}, \text{ a stąd } [30, 700] = 4*3*25*7 = 2100.$$

$$\text{Wn.7 } (a, b) = \prod_j p_j^{m_j}, \text{ gdzie } m_j = \min(k_j, l_j) \text{ dla każdego } j = 1, 2, \dots$$

Wn. 8 (związek NWD i NWW)

$$(a, b) [a, b] = a * b$$

PIERŚCIEŃ WIELOMIANÓW $K[x]$ NAD CIAŁEM K

Def. Niech K będzie ciałem liczbowym. Wielomianem nad ciałem K nazywamy wyrażenie

$$\varphi = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \quad (1)$$

Gdzie każde $a_k \in K$ i $a_n \neq 0$. Oznaczamy $\varphi = \sum_{i=1}^n a_i x^i$.

Def. W (1) każdy wyraz a_k nazywamy k -tym współczynnikiem wielomianu φ , a_0 – wyrazem wolnym, a stopniem wielomianu nazywamy najwyższy wykładnik potęg zmiennej x : $n = \text{st}\varphi$.

Wn.1 Suma, różnica i iloczyn dwóch wielomianów nad wspólnym ciałem K jest wielomianem nad tym ciałem, przy czym spełnione są aksjomaty definicji pierścienia przemiennego z jedynką (ale nie ciała!). Pierścień ten oznaczamy $K[x]$.

Def. Dwa wielomiany φ i ψ nazywamy **równymi**, jeśli są tego samego stopnia ($\text{st}\varphi = \text{st}\psi$) i wszystkie ich współczynniki są parami równe, tzn. $a_k = b_k$ dla każdego $k = 1, 2, \dots, \text{st}\varphi$.

Tw. (o tożsamości wielomianów o wspólnych wartościach w $n + 1$ węzłach)



Jeśli dla dwóch wielomianów

$$\varphi = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0 \quad (2)$$

$$\psi = b_m x^m + b_{m-1} x^{m-1} + \dots + b_2 x^2 + b_1 x + b_0 \quad (3)$$

o stopniach $m = \text{st}\psi \leq \text{st}\varphi = n$ zachodzi równość $\psi(x_j) = \varphi(x_j)$ dla wszystkich danych $n+1$ punktów $(x_1, x_2, \dots, x_n, x_{n+1})$ parami różnych, to $\psi = \varphi$ (tzn. $m = n$ i $a_j = b_j$ dla $j = 0, 1, \dots, n$).

Dowód: pomijamy.

Wn.2 $\text{st}(\varphi + \psi) \leq \max(\text{st}\varphi, \text{st}\psi)$

Wn.3 Jeśli $\varphi \neq 0$ i $\psi \neq 0$, to $\varphi * \psi \neq 0$ i $\text{st}(\varphi * \psi) = \text{st}\varphi + \text{st}\psi$.

Istotnie, niech iloczyn ma współczynniki c_j dla $j = 1, 2, \dots, n+m$ wtedy $c_{m+n} = a_n b_m \neq 0$, choć dalsze współczynniki: $c_{m+n-1} = a_{n-1} b_m + a_n b_{m-1}$, etc. mogą równać się zero. Stąd, $\varphi * \psi \neq 0$.

Wn.4 Jeśli $\varphi \neq 0$ i $\varphi * \psi = \varphi * \chi$, to $\psi = \chi$ (prawo skracania dla wielomianów).

Istotnie, z założenia $0 = \varphi * \psi - \varphi * \chi = \varphi(\psi - \chi)$, stąd $\psi - \chi = 0$, jeśli $\varphi \neq 0$.

Def. Dla $\psi, \varphi \in K[x]$, wielomian $\varphi \neq 0$ nazywamy **dzielnikiem** wielomianu ψ , jeśli istnieje taki wielomian $\chi \in K[x]$, że $\psi = \varphi * \chi$, co ozn. $\varphi | \psi$ - przeciwnie $\varphi \nmid \psi$.

Wn.5 Superpozycja (złożenie) dwóch wielomianów jest wielomianem oraz

$$\text{st}(\varphi(\psi)) = \text{st}\varphi * \text{st}\psi.$$

Tw. (o dzieleniu wielomianów z resztą)



Dla każdej pary wielomianów φ i ψ , gdzie $\text{st}\varphi > 0$, istnieje dokładnie jeden układ wielomianów β i ρ , dla których zachodzi tożsamość $\psi = \beta\varphi + \rho$, przy czym $\text{st}\rho < \text{st}\varphi$. Jeśli $\varphi \in K[x]$ i $\psi \in K[x]$, to $\beta \in K[x]$ i $\rho \in K[x]$. Wielomian β nazywamy **ilorazem**, ρ - **resztą**.

Dowód: Indukcja względem stopnia wielomianu ψ (do pominięcia w pierwszym czytaniu).

Jeśli $\text{st}\psi < \text{st}\varphi$, to $\beta = 0$ i $\rho = \psi$.



Dlatego założmy, że tw. jest prawdziwe dla wielomianów ψ stopnia $< n$.

Niech teraz $\text{st}\psi = n \geq \text{st}\varphi = q$, oraz

a i b oznaczają najwyższe współczynniki wielomianu ψ i φ , odpowiednio.

Ponieważ $\text{st}(ax^{n-q}\varphi/b) = n$ i jego najwyższy współczynnik jest równy a , więc wielomian

$$\psi_1 = (\psi - ax^{n-q}\varphi/b) \in K[x] \text{ i } \text{st}\psi_1 < n. \quad (*)$$

Z założenia indukcyjnego wynika istnienie układu wielomianów β_1 i ρ w $K[x]$ dla których

$$\psi_1 = \beta_1\varphi + \rho, \text{ przy czym } \text{st}\rho < \text{st}\varphi.$$

Stąd, wobec (*) mamy

$$\psi = (ax^{n-q}\varphi/b + \beta_1)\varphi + \rho,$$

co przedstawia tezę tw. dla $\beta = ax^{n-q}\varphi/b + \beta_1$ i $\beta \in K[x]$.

Dla wykazania jednoznaczności przypuśćmy, że mamy również

$$\psi = \beta_1\varphi + \rho_1, \text{ przy czym } \text{st}\rho_1 < \text{st}\varphi. \quad (**)$$

Wówczas jednak odejmując stronami tezę i (**) otrzymujemy tożsamość $(\beta - \beta_1)\varphi = \rho - \rho_1$.

Ponieważ nadal $\text{st}(\rho - \rho_1) < \text{st}\varphi$, więc powyższa tożsamość pociąga za sobą $\beta - \beta_1 = 0$, a zatem $\beta = \beta_1$ i $\rho = \rho_1$, c.b.d.o.

Wn.6 Algorytm obliczania ilorazu i reszty z dzielenia wielomianów (jak w dowodzie).

Dla $\psi = ax^n + \dots$ i $\varphi = bx^q + \dots$ należy od ψ odjąć wielomian $ax^{n-q}\varphi/b = \beta_1\varphi$, tzn. $\beta_1 = (a/b)x^{n-q}$.

Oznaczmy różnicę przez $\psi_1 = a_1x^m + \dots$. Należy od ψ_1 znów odjąć wielomian $a_1x^{m-q}\varphi/b = \beta_2\varphi$, gdzie $\beta_2 = (a_1/b)x^{m-q}$ i procedurę prowadzić, aż przez odjęcie $\beta_s\varphi$ od ψ_s uzyskamy wielomian ψ_{s+1} stopnia niższego q . Wówczas przyjmujemy:

$$\rho = \psi_{s+1} \text{ i } \beta = \beta_1 + \beta_2 + \dots + \beta_s.$$

Przykład. Rozważmy wielomiany

$$\psi(x) = x^4 - x^2 - 2x + 1 \quad (n = \text{st}\psi = 4, a = 1)$$

$$\varphi(x) = x^2 - x - 1 \quad (q = \text{st}\varphi = 2, b = 1)$$

Wobec Wn.6 mamy

$$\beta_1 = (a/b)x^{n-q} = x^2 \quad \text{oraz} \quad \psi_1 = \psi - \beta_1\varphi = x^3 - 2x + 1 \quad (\text{st}\psi_1 = 3 > \text{st}\varphi = 2), \text{ więc dalej}$$

$$\beta_2 = x \quad \text{oraz} \quad \psi_2 = \psi_1 - \beta_2\varphi = x^2 - x + 1 \quad (\text{st}\psi_2 = 2 = \text{st}\varphi = 2), \text{ więc dalej}$$

$$\beta_3 = 1 \quad \text{oraz} \quad \psi_3 = \psi_2 - \beta_3\varphi = 2 \quad (\text{st}\psi_3 = 0 < \text{st}\varphi = 2), \text{ co kończy schemat i}$$


otrzymujemy wzór

$$\psi = x^4 - x^2 - 2x + 1 = \varphi(\beta_1 + \beta_2 + \beta_3) + \psi_3 = (x^2 - x - 1)(x^2 + x + 1) + 2.$$

Tw. (Bézout)

Resztą z dzielenia wielomianu $\psi(x)$ przez dwumian $x - a$ jest $\psi(a)$, czyli

$$\psi(x) = (x - a)\beta(x) + \psi(a). \quad (4)$$

Dowód: Z tw. o dzieleniu wielomianów z resztą wynika, że reszta z dzielenia ψ przez $(x - a)$ jest stałą, tzn. $\psi(x) = (x - a)\beta(x) + c$, gdzie podstawiając $x = a$ mamy $c = \psi(a)$, c.b.d.o. 

Wn. 7 Schemat Hornera

Praktyczny algorytm obliczania ilorazu $\beta(x)$, a zwłaszcza reszty $\psi(a)$, przy dzieleniu wielomianów przez dwumiany postaci $(x - a)$. Niech

$$\psi = a_0x^n + a_1x^{n-1} + \dots + a_{n-2}x^2 + a_{n-1}x + a_n$$

wtedy $\beta(x)$ w (4) jest postaci

$$\beta = b_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-3}x^2 + b_{n-2}x + b_{n-1}.$$

Podstawiając powyższe do (4) otrzymujemy tożsamość wielomianów skąd przez porównanie współczynników po obu stronach przy jednakowych potęgach wynikają równości dające rekurencyjny ciąg dla współczynników ilorazu i wartości reszty $\psi(a)$:

$$b_0 = a_0,$$

$$b_1 = a_1 + a b_0,$$

$$b_2 = a_2 + a b_1,$$

.....

$$b_{n-1} = a_{n-1} + a b_{n-2}$$

oraz

$$\psi(a) = a_n + a b_{n-1}.$$

Można schemat ten zapisać następująco:

a_0	a_1	a_2	\dots	a_{n-1}	a_n
	$a b_0$	$a b_1$	\dots	$a b_{n-2}$	$a b_{n-1}$
+_____	+_____	+_____	+_____	+_____	+_____
$b_0 = a_0$	b_1	b_2		b_{n-1}	$\psi(a)$

Przykład. Wyznaczmy iloraz $\beta(x)$ i wartość $\psi(a)$ wielomianu $\psi(x) = 4x^4 - 3x^2 - 2x + 1$

wg. schematu Hornera dla $a = 10$:

4	0	-3	-2	1
	40	400	3970	39680
4	40	397	3968	39681

Zatem

$$\psi(x) = 4x^4 - 3x^2 - 2x + 1 = (x - 10)(4x^3 + 40x^2 + 397x + 3968) + 39681$$

oraz $\psi(a = 10) = 39681$.

