Rozdział 6

Pierścienie $\mathbb{Z}_n$

Teoria

Podzielność w zbiorze liczb całkowitych. Mówimy, że liczba $k \in \mathbb{Z}$ dzieli liczbę $l \in \mathbb{Z}$, gdy istnieje taka liczba całkowita m, że $l = m \cdot k$. Fakt ten zapisujemy skrótowo $k|l$ i czytamy „k dzieli l".

Własności podzielności w zbiorze liczb całkowitych. Dla dowolnych $k, l, m \in \mathbb{Z}$ mamy:

- $k|k$,
- jeśli $k|l$ oraz $l|m$, to $k|m$,
- jeśli $k|l$ oraz $l|k$, to $k = \pm l$,
- jeśli $k|l$, to $k|(m \cdot l)$,
- jeśli $k|l$ oraz $k|m$, to $k|(l + m)$;
- jeśli $k|l$ oraz $k|m$, to $k|(a \cdot l + b \cdot m)$ dla dowolnych $a, b \in \mathbb{Z}$.

Największym wspólnym dzielnikiem liczb $k_1, k_2, \ldots, k_n$ nazywamy taką liczbę naturalną d, że

- $d|k_i$ dla wszystkich $i \in \{1, 2, \ldots, n\}$ oraz
- dla każdej liczy naturalnej c będącej wspólnym dzielnikiem liczb $k_1, k_2, k_3, \ldots, k_n$ zachodzi warunek $c|d$.

Największy wspólny dzielnik liczb $k_1, k_2, k_3, \ldots, k_n$ oznaczamy symbolem $\mathrm{NWD}(k_1, k_2, \ldots, k_n)$.

Liczby względnie pierwsze to takie liczby całkowite $k_1, k_2, \ldots, k_n$, dla których największy wspólny dzielnik wynosi 1, tzn. $\mathrm{NWD}(k_1, k_2, k_3, \ldots, k_n) = 1$.

Dzielenie z resztą w zbiorze liczb całkowitych. Dla dowolnych liczb $k \in \mathbb{Z}$ oraz $n \in \mathbb{N}$ istnieją jednoznacznie wyznaczone liczby $q \in \mathbb{Z}$ oraz $r \in \{0, 1, \ldots, n-1\}$ takie, że $k = n \cdot q + r$. Liczbę r nazywamy wtedy *resztą* z dzielenia k przez n.

ALGORYTM EUKLIDESA. Do wyznaczenia największego wspólnego dzielnika liczb $m, n \in \mathbb{N}$ służy tzw. *algorytm Euklidesa*.(Dla ustalenia uwagi załóżmy, że $m \geqslant n$.) Algorytm ten bazuje na następującej własności: *Jeśli* $m = n \cdot q + r$, *to* $\mathrm{NWD}(m, n) = \mathrm{NWD}(n, r)$.

Dzielimy m przez n z resztą. Mamy $m = n \cdot q_1 + r_1$. Jeśli $r_1 = 0$, to $\mathrm{NWD}(m, n) = n$, natomiast jeśli $r_1 \neq 0$, to korzystamy z równości $\mathrm{NWD}(m, n) = \mathrm{NWD}(n, r_1)$ i dzielimy n przez r_1 z resztą. Mamy więc $n = r_1 \cdot q_2 + r_2$. Dalej, o ile $r_2 \neq 0$ wykonujemy kolejne dzielenie z resztą: $r_1 = r_2 \cdot q_3 + r_3$. Kontynuujemy opisaną procedurę tak długo dopóki nie dostaniemy reszty równej 0 (musi to nastąpić w skończonej liczbie kroków, bo reszty maleją). Otrzymujemy w ten sposób skończony ciąg równości $\mathrm{NWD}(m, n) = \mathrm{NWD}(n, r_1) = \mathrm{NWD}(r_1, r_2) = \ldots$ *Ostatnia niezerowa reszta* powstająca w ciągu kolejnych dzieleń z resztą w algorytmie Euklidesa jest największym wspólnym dzielnikiem liczb m i n.

Algorytm 1 Największy wspólny dzielnik (algorytm Euklidesa)

```
1:  procedure NWD(m, n)
2:      a ← m
3:      b ← n
4:      while b ≠ 0 do
5:          c ← reszta z dzielenia a przez b
6:          a ← b
7:          b ← c
8:      end while
9:      return NWD(m, n) = a
10: end procedure
```

ALGORYTM EUKLIDESA – PRZYKŁAD. Obliczyć NWD liczb 3328 oraz 1599. Mamy

$$\begin{aligned} 3328 &= 1599 \cdot 2 + 130, \\ 1599 &= 130 \cdot 12 + 39, \\ 130 &= 39 \cdot 3 + 13, \\ 39 &= 13 \cdot 3. \end{aligned}$$

W algorytmie Euklidesa największym wspólnym dzielnikiem jest ostatnia niezerowa reszta, więc $\mathrm{NWD}(3328, 1599) = 13$.

ZBIÓR RESZT. Możliwe do otrzymania reszty z dzielenia danej liczby całkowitej dodatniej k przez liczbę naturalną n, to liczby $0, 1, 2, 3, \ldots, n-1$. Zbiór reszt z dzielenia przez liczbę n oznaczamy symbolem $\mathbb{Z}_n$, tj. $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$.

DZIAŁANIA MODULO. Dla ustalonego $n \in \mathbb{N}$ w zbiorze liczb całkowitych określamy działania: $\underset{n}{+}$ – *dodawania modulo* n oraz $\underset{n}{\cdot}$ – *mnożenia modulo* n w następujący sposób:

$$\begin{aligned} k \underset{n}{+} l &= \text{reszta z dzielenia } k + l \text{ przez } n, \\ k \underset{n}{\cdot} l &= \text{reszta z dzielenia } k \cdot l \text{ przez } n. \end{aligned}$$

Symbol mod. By zaznaczyć, że równości zachodzą *modulo* n, tzn. reszty z dzielenia lewej i prawej strony równości przez n są równe, stosuje się symbol mod, np. $4 = 1 \pmod 3$ lub $(7+5) = (3 \cdot 6) \pmod 6$. Wyrażenie $5 = 1 \pmod 2$ (lub pojawiające się równie często $5 \equiv 1 (\mathrm{mod}\, 2)$) czytamy „pięć przystaje do 1 modulo 2".

Liczby przeciwne i odwrotne w zbiorach $\mathbb{Z}_n$. W zbiorach $\mathbb{Z}_n$ z działaniami modulo można zdefiniować pojęcie liczby przeciwnej i odwrotnej, podobnie jak robi się to w przypadku zwykłych działań w zbiorze liczb rzeczywistych. Mianowicie liczbę $l \in \mathbb{Z}_n$ nazwiemy *przeciwną* do liczby $k \in \mathbb{Z}_n$, gdy $k \underset{n}{+} l = 0$. Podobnie liczbę $l \in \mathbb{Z}_n$ nazwiemy *odwrotną* do liczby $k \in \mathbb{Z}_n$, gdy $k \underset{n}{\cdot} l = 1$. O liczbie k (ale także o l) mówimy wtedy, że jest *odwracalna*. Liczbę przeciwną do k oznaczamy symbolem $-k$, a liczbę odwrotną k^{-1}.

Uwaga: Każda liczba $k \in \mathbb{Z}_n$ zawsze posiada jednoznacznie wyznaczoną liczbę przeciwną. Gdy mówimy o liczbach odwrotnych sytuacja jest bardziej skomplikowana. Jeżeli $n \geqslant 2$ jest liczbą pierwszą, to każdy element w $\mathbb{Z}_n$ różny od 0 ma odwrotność. W przeciwnym przypadku w $\mathbb{Z}_n$ zawsze można znaleźć liczbę różną od 0 i 1, która nie posiada liczby odwrotnej.

Dzielniki zera w $\mathbb{Z}_n$. Jeżeli liczba naturalna $n \geqslant 2$ nie jest liczbą pierwszą (tzn. jest liczbą złożoną), można zawsze znaleźć elementy $k, l \in \mathbb{Z}_n \setminus \{0\}$ takie, że $k \underset{n}{\cdot} l = 0$. Liczby takie nazywamy *dzielnikami zera*.

Zadania

Zadanie 6.1. Wyznaczyć największy wspólny dzielnik liczb m oraz n, korzystając z algorytmu Euklidesa:

(a) $m = 213$ oraz $n = 144$,

(b) $m = 272$ oraz $n = 163$,

(c) $m = 282$ oraz $n = 161$,

(d) $m = 282$ oraz $n = 246$,

(e) $m = 1840$ oraz $n = 759$,

(f) $m = 1743$ oraz $n = 945$,

(g) $m = 2352$ oraz $n = 268$,

(h) $m = 4319$ oraz $n = 1232$.

Zadanie 6.2. Dla dowolnej liczby naturalnej $n \in \mathbb{N}$ obliczyć:

(a) $\mathrm{NWD}(n, n+1)$,

(b) $\mathrm{NWD}(n, n+3)$.

Zadanie 6.3. Oblicz

(a) $7 \underset{15}{+} 12$,

(b) $18 \underset{17}{+} 12$,

(c) $12 \underset{23}{+} 48$,

(d) $20 \underset{24}{+} 13$,

(e) $12 \underset{12}{+} 36$,

(f) $8 \underset{7}{+} 20$,

(g) $7 \underset{3}{\cdot} 4$,

(h) $12 \underset{2}{\cdot} 3$,

(i) $18 \underset{5}{\cdot} 4$,

(j) $7 \underset{4}{\cdot} 13$,

(k) $12 \underset{24}{\cdot} 10$,

(l) $6 \underset{7}{\cdot} 13$.

Zadanie 6.4. Uzupełnić tabele dla dodawania i mnożenia modulo 5 w zbiorze $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot_5$	0	1	2	3	4
0					
1					
2					
3					
4					

Zadanie 6.5. Uzupełnić tabele dla dodawania i mnożenia modulo 6 w zbiorze $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

$+_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

$\cdot_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Zadanie 6.6. Znajdź odwrotności wszystkich elementów różnych od zera w

(a) $\mathbb{Z}_2$, (b) $\mathbb{Z}_3$, (c) $\mathbb{Z}_5$, (d) $\mathbb{Z}_7$.

Zadanie 6.7. Wyznacz wszystkie dzielniki zera i wszystkie elementy odwracalne w

(a) $\mathbb{Z}_4$, (b) $\mathbb{Z}_6$, (c) $\mathbb{Z}_8$, (d) $\mathbb{Z}_9$.

Zadanie 6.8. Za pomocą symbolu mod zapisać następujące wyrażenia

(a) liczba n jest parzysta,

(b) liczba n jest nieparzysta,

(c) liczba n przy dzieleniu przez 11 daje resztę 7,

(d) liczba n przy dzieleniu przez 13 daje resztę 8,

(e) liczby m oraz n przy dzieleniu przez 7 dają taką samą resztę,

(f) liczby m oraz n przy dzieleniu przez 15 dają taką samą resztę,

(g) reszta z dzielenia liczby m przez 4 jest o 2 większa niż reszta z dzielenia liczby n przez 4,

(h) reszta z dzielenia liczby m przez 5 jest o 3 mniejsza niż reszta z dzielenia liczby n przez 5,

(i) różnica połowy liczby m i podwojonej liczby n jest parzysta,

(j) suma potrojonej liczby m i ćwierci liczby n jest nieparzysta.

Rozwiązania

6.1. Przypomnijmy, że algorytm Euklidesa można opisać trzema następującymi krokami:

Krok 1: Dzielimy większą liczbę przez mniejszą i zapisujemy resztę.

Krok 2: Mniejsza liczba staje się „nową" większą liczbą, reszta staje się „nowym" dzielnikiem.

Krok 3: Ostatnia *niezerowa* reszta to właśnie NWD.

(a) Wyznaczmy największy wspólny dzielnik liczb $m = 213$ oraz $n = 144$. Mamy

$$\begin{aligned} 213 &= 144 \cdot 1 + 69, \\ 144 &= 69 \cdot 2 + 6, \\ 69 &= 6 \cdot 11 + 3, \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

Zatem $NWD(213, 144) = 3$.

(b) Wyznaczmy największy wspólny dzielnik liczb $m = 272$ oraz $n = 163$. Mamy

$$\begin{aligned} 272 &= 163 \cdot 1 + 109, \\ 163 &= 109 \cdot 1 + 54, \\ 109 &= 54 \cdot 2 + 1, \\ 54 &= 1 \cdot 54 + 0. \end{aligned}$$

Zatem $NWD(272, 163) = 1$.

(c) Wyznaczmy największy wspólny dzielnik liczb $m = 282$ oraz $n = 161$. Mamy

$$\begin{aligned} 282 &= 161 \cdot 1 + 121, \\ 161 &= 121 \cdot 1 + 40, \\ 121 &= 40 \cdot 3 + 1, \\ 40 &= 1 \cdot 40 + 0. \end{aligned}$$

Zatem $NWD(282, 161) = 1$.

(d) Wyznaczmy największy wspólny dzielnik liczb $m = 282$ oraz $n = 246$. Mamy

$$\begin{aligned} 282 &= 246 \cdot 1 + 36, \\ 246 &= 36 \cdot 6 + 30, \\ 36 &= 30 \cdot 1 + 6, \\ 30 &= 6 \cdot 5 + 0. \end{aligned}$$

Zatem $NWD(282, 246) = 6$.

(e) Wyznaczmy największy wspólny dzielnik liczb $m = 1840$ oraz $n = 759$. Mamy

$$\begin{aligned} 1840 &= 759 \cdot 2 + 322, \\ 759 &= 322 \cdot 2 + 115, \\ 322 &= 115 \cdot 2 + 92, \\ 115 &= 92 \cdot 1 + 23, \\ 92 &= 23 \cdot 4 + 0. \end{aligned}$$

Zatem $NWD(1840, 759) = 23$.

(f) Wyznaczmy największy wspólny dzielnik liczb $m = 1743$ oraz $n = 945$. Mamy

$$\begin{aligned} 1743 &= 945 \cdot 1 + 798, \\ 945 &= 798 \cdot 1 + 147, \\ 798 &= 147 \cdot 5 + 63, \\ 147 &= 63 \cdot 2 + 21, \\ 63 &= 21 \cdot 3 + 0. \end{aligned}$$

Zatem $NWD(1743, 945) = 21$.

(g) Wyznaczmy największy wspólny dzielnik liczb $m = 2352$ oraz $n = 268$. Mamy

$$\begin{aligned} 2352 &= 268 \cdot 8 + 256, \\ 268 &= 256 \cdot 1 + 12, \\ 256 &= 12 \cdot 21 + 4, \\ 12 &= 4 \cdot 3 + 0. \end{aligned}$$

Zatem $NWD(2352, 268) = 4$.

(h) Wyznaczmy największy wspólny dzielnik liczb $m = 4319$ oraz $n = 1232$. Mamy

$$\begin{aligned} 4319 &= 1232 \cdot 3 + 623, \\ 1232 &= 623 \cdot 1 + 609, \\ 623 &= 609 \cdot 1 + 14, \\ 609 &= 14 \cdot 43 + 7, \\ 14 &= 7 \cdot 2 + 0. \end{aligned}$$

Zatem $NWD(4319, 1232) = 7$.

6.2. (a) Zastosujmy algorytm Euklidesa do dwóch kolejnych liczb naturalnych n oraz $n + 1$. Mamy

$$\begin{aligned} n &= 1 \cdot (n - 1) + 1, \\ n - 1 &= (n - 1) \cdot 1 + 0, \end{aligned}$$

przy czym w pierwszej równości $n - 1$ występujące po prawej stronie jest dzielnikiem, a w drugiej dzielną. Zatem ostatnią niezerową resztą jest 1, a to oznacza, że $NWD(n, n+1) = 1$.

(b) Rozważymy trzy przypadki w zależności od tego jaką resztę daje liczba n przy dzieleniu przez 3. Zacznijmy od sytuacji, gdy n jest wielokrotnością 3, tzn. $n = 3k$ dla pewnego $k \in \mathbb{N}$. Wtedy $n + 3 = 3(k + 1)$. Ale jak wiemy z poprzedniego podpunktu liczy k oraz $k + 1$ są względnie pierwsze, tzn. ich największym wspólnym dzielnikiem jest 1. Zatem $NWD(n, n + 3) = NWD(3k, 3k + 3) = 3$.

Załóżmy teraz, że $n = 3k + 1$ dla pewnego $k \in \mathbb{N}$. Wtedy $n + 3 = 3k + 4$. Stosując algorytm Euklidesa do liczby $3k + 1$ oraz $3k + 4$ mamy

$$\begin{aligned} 3k + 4 &= 1 \cdot (3k + 1) + 3, \\ 3k + 1 &= 3 \cdot k + 1, \\ k &= k \cdot 1 + 0. \end{aligned}$$

Zatem $NWD(n, n+3) = NWD(3k+1, 3k+4) = 1$.

Rozumując podobnie do poprzedniej sytuacji, można pokazać, że $NWD(n, n+3) = 1$, gdy $n = 3k+2$ dla pewnego $k \in \mathbb{N}$.

6.3. (a) 4 (b) 13 (c) 14 (d) 9 (e) 0 (f) 0 (g) 1 (h) 0 (i) 2 (j) 3 (k) 0 (l) 1

6.4.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

6.5.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Uwaga: Analizując tabele mnożenia modulo przedstawione w poprzednich przykładach, można zauważyć interesującą prawidłowość: w ostatnim wierszu oraz ostatniej kolumnie, z pominięciem reszty zerowej, pojawiają się kolejno wszystkie liczby od $n-1$ do 1 w porządku malejącym. Nie jest to przypadek. Rozważmy $(k+1)$-ty element w ostatnim wierszu tabeli mnożenia modulo. Ma on postać:

$$(n-1) \underset{n}{\cdot} k = kn - k = n - k.$$

Korzystamy tu z faktu, że w pierścieniu reszt $\mathbb{Z}_n$ liczby $0, n, 2n, 3n, \ldots, kn, \ldots$ są sobie równoważne (równe), ponieważ wszystkie dają tę samą resztę z dzielenia przez n, czyli 0.

6.6. (a) $1^{-1} = 1$

(b) $1^{-1} = 1$ oraz $2^{-1} = 2$

(c) $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ oraz $4^{-1} = 4$

(d) $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$ oraz $6^{-1} = 6$

6.7. (a) Elementy odwracalne to 1 oraz 3, przy czym $1^{-1} = 1$ oraz $3^{-1} = 3$.
Dzielniki zera to 2, bo $2 \underset{4}{\cdot} 2 = 0$.

(b) Elementy odwracalne to 1 oraz 5, przy czym $1^{-1} = 1$ oraz $5^{-1} = 5$.
Dzielniki zera to 2, 3 oraz 4, bo $2 \underset{6}{\cdot} 3 = 0$ oraz $4 \underset{6}{\cdot} 3 = 0$.

(c) Elementy odwracalne to 1, 3, 5 oraz 7, przy czym $1^{-1} = 1$, $3^{-1} = 3$, $5^{-1} = 5$ oraz $7^{-1} = 7$.
Dzielniki zera to 2, 4 oraz 6, bo $2 \underset{8}{\cdot} 4 = 0$ oraz $4 \underset{8}{\cdot} 6 = 0$.

(d) Elementy odwracalne to 1, 2, 4, 5, 7 oraz 8, przy czym $1^{-1} = 1$, $2^{-1} = 5$, $4^{-1} = 7$ oraz $5^{-1} = 2$, $7^{-1} = 4$ oraz $8^{-1} = 8$.

Dzielniki zera to 3 oraz 6, bo $3 \underset{9}{\cdot} 6 = 0$.

6.8. (a) $n = 0 \pmod 2$

(b) $n = 1 \pmod 2$

(c) $n = 7 \pmod{11}$

(d) $n = 8 \pmod{13}$

(e) $n = m \pmod 7$

(f) $n = m \pmod{15}$

(g) $n = (m - 2) \pmod 4$

(h) $n = (m + 3) \pmod 5$

(i) $(\frac{1}{2}m + 2n) = 0 \pmod 2$

(j) $(3m + \frac{1}{4}n) = 1 \pmod 2$

Literatura

Bibliografia. Niniejszy zestaw zadań został przygotowany w oparciu o następujące materiały:

- *Algorytm Euklidesa*, https://pl.wikipedia.org/wiki/Algorytm_Euklidesa.
- A. Iwaszkiewicz-Rudoszańska, *Wstęp do algebry i teorii liczb*, Wydawnictwo Naukowe UAM, Poznań 2009.
- J. Rutkowski, *Algebra abstrakcyjna w zadaniach*, Wydawnictwo Naukowe PWN, Warszawa, 2006.