

## Wykład 4

Określmy teraz pewną ważną klasę pierścieni.

**Twierdzenie 1** Niech  $m, n \in \mathbb{Z}$ . Jeśli  $n > 0$  to istnieje dokładnie jedna para liczb  $q, r$ , że:

$$m = qn + r, \quad 0 \leq r < n.$$

Liczbę  $r$  nazywamy resztą z dzielenia  $m$  przez  $n$  i często oznaczamy ją przez  $m_n$ . Zauważmy, że reszta zawsze jest liczbą większą lub równą zero i jest mniejsza od liczby przez, którą dzielimy.

### Przykłady

1.  $m = 26, n = 6$ , wtedy mamy  $26 = 4 \cdot 6 + 2$ , więc reszta z dzielenia 26 przez 6 wynosi 2.
2.  $m = -26, n = 6$ , wtedy mamy  $26 = (-5) \cdot 6 + 4$ , więc reszta z dzielenia -26 przez 6 wynosi 4.
3.  $m = 5, n = 7$ , wtedy mamy  $5 = 0 \cdot 7 + 5$ , więc reszta z dzielenia 5 przez 7 wynosi 5.

Niech  $Z_n = \{0, 1, \dots, n-1\}$ , gdzie  $n \in \mathbb{N}, n > 0$ , wtedy w zbiorze  $Z_n$  możemy określić działania  $+_n, \cdot_n$  w następujący sposób:

$$\begin{aligned} a +_n b &= (a + b)_n \\ a \cdot_n b &= (a \cdot b)_n \end{aligned}$$

a więc sumę i iloczyn w  $Z_n$  określamy jako resztę z dzielenia zwykłej sumy i zwykłego iloczynu przez  $n$ . Określmy następującą funkcję:

$$f_n : \mathbb{Z} \rightarrow Z_n$$

$f_n(x) =$  reszta z dzielenia liczby  $x$  przez  $n$ . Wtedy funkcja  $f_n$  ma własności:

$$\begin{aligned} f_n(x + y) &= f_n(x) +_n f_n(y) \\ f_n(x \cdot y) &= f_n(x) \cdot_n f_n(y) \end{aligned}$$

Niech  $r, s$  oznaczają reszty z dzielenia  $x$  i  $y$  przez  $n$  wtedy mamy  $x = an + r, y = bn + s$ . Stąd  $x + y = (a + b)n + r + s$  i  $f_n(x + y) = f_n(r + s)$  i  $f_n(x) = r$  oraz  $f_n(y) = s$ . Ponieważ  $0 \leq r, s < n$  to zgodnie z definicją funkcji  $f_n$  i dodawania  $+_n$  otrzymujemy żądaną równość.

**Twierdzenie 2** System algebraiczny  $(Z_n, +_n, \cdot_n)$  jest pierścieniem przemiennym z jedyneką.

**Dowód** Wszystkie własności pierścienia można sprawdzić korzystając z funkcji  $f_n$ . Na przykład jeśli chcemy udowodnić łączność to weźmy dowolne elementy  $a, b, c \in Z_n$ . Wtedy mamy:

$$a +_n (b +_n c) = f_n(a + (b + c)) = f_n((a + b) + c) = (a +_n b) +_n c$$

Inne własności pokazuje się podobnie. Elementem neutralnym dodawania jest 0, mnożenia jest 1. Elementem przeciwnym do  $a \in Z_n$  jest  $n - a$ .  $\square$

Działania  $+_n, \cdot_n$  nazywa się zwykle dodawaniem i mnożeniem modulo  $n$ , a pierścień  $(Z_n, +_n, \cdot_n)$  pierścieniem reszt modulo  $n$ . Można też zdefiniować potęgowanie np.  $a^2$  w  $Z_n$  rozumiemy jako  $a \cdot_n a$  itd... W sensie pierścienia  $Z_n$  możemy formalnie używać dowolnych liczb całkowitych i możemy powiedzieć, że liczba  $a = b$  w  $Z_n$  jeśli  $f_n(a) = f_n(b)$ . Co to daje? Można w prosty sposób wykonywać pewne działania np. jeśli chcemy obliczyć  $7 \cdot_9 (4 +_9 5)$  to wystarczy obliczyć ile wynosi  $7 \cdot (4 + 5)$  w  $Z$ , a potem wziąć resztę z dzielenia wyniku przez 9. Można też inaczej postępować na przykład jeśli chcemy obliczyć  $2^{100}$  w pierścieniu  $Z_5$  to łatwiej jest wykonywać od razu pewne obliczenia modulo 5, bo  $2^4 = 1$  w  $Z_5$ , a więc  $2^{100} = (2^4)^{25} = 1^{25} = 1$ .

**Zadanie** Skonstruować tabelki działań w pierścieniu  $Z_5$ .

$+_n$	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

$\cdot_n$	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

**Zadanie** Obliczyć  $888^2$  w pierścieniu  $Z_{889}$ .

**Rozwiązanie** Ponieważ w pierścieniu  $Z_{889}$  liczba  $888 = -1$  to  $888^2 = (-1)^2 = 1$ .

**Zadanie** Rozwiązać równanie  $15 \cdot_{19} x = 1$  w  $Z_{19}$ .

**Rozwiązanie** Trzeba wyznaczyć liczbę, która wymnożona przez 15 modulo 19 da nam 1. Tę liczbę można wyznaczyć badając wszystkie reszty modulo 19. Po przetestowaniu wszystkich liczb modulo 15, stwierdzimy, że jedynym rozwiązaniem naszego równania jest 14.

Opiszemy teraz ogólną metodę odwracania liczb modulo  $n$

Niech  $a, b$  będą liczbami całkowitymi i niech  $b \neq 0$ . Wtedy mówimy, że liczba  $b$  **dzieli**  $a$  (lub, że  $b$  jest dzielnikiem  $a$ ) jeśli istnieje liczba całkowita  $c$ , że  $a = bc$ . Fakt, że liczba  $b$  dzieli  $a$  zapisujemy symbolicznie  $b|a$ , a jeśli liczba  $b$  nie dzieli  $a$  to piszemy  $b \nmid a$ .

Na przykład  $24|96$  bo  $96 = 4 \cdot 24$ . Podobnie  $-4|24$  bo  $24 = (-6) \cdot (-4)$ . Liczba 3 nie dzieli liczby 7, a więc możemy zapisać  $3 \nmid 7$ .

Niech  $a$  i  $b$  będą liczbami całkowitymi, z których przynajmniej jedna jest różna od zera. Wtedy **największym wspólnym dzielnikiem** tych liczb nazywamy największą liczbę całkowitą  $d$ , która dzieli jednocześnie  $a$  i  $b$ . Największy wspólny dzielnik oznaczamy przez  $\text{NWD}(a, b)$  i jest on wyznaczony (w tym przypadku) jednoznacznie. Inaczej mówiąc  $d = \text{NWD}(a, b)$  wtedy i tylko wtedy gdy

- (i)  $d|a$  i  $d|b$ ,
- (ii) jeśli  $c|a$  i  $c|b$  to  $c \leq d$ .

Z powyższej definicji widać, że  $\text{NWD}(a, b) \geq 1$ .

Na przykład  $\text{NWD}(12, 30) = 6$ .

Opiszemy teraz algorytm, który pozwala w prosty sposób wyznaczać największy wspólny dzielnik dwóch liczb. Załóżmy, że  $a \geq b$ . Oczywiście jeśli  $b|a$  to  $\text{NWD}(a, b) = b$  i problemu nie ma. Przypuśćmy, że  $b \nmid a$  wtedy możemy  $a$  podzielić przez  $b$  z niezerową resztą:

$$a = q_0b + r_0, \quad 0 < r_0 < b$$

Jeśli liczba  $c$  dzieli  $a$  i dzieli  $b$  to ta liczba musi dzielić również  $r_0$ . Oznacza to, że zbiór dzielników liczb  $a, b$  jest taki sam jak zbiór dzielników liczb  $b, r_0$ , a więc również  $\text{NWD}(a, b) = \text{NWD}(b, r_0)$ . Można więc proces dzielenia z resztą kontynuować w następujący sposób:

$$\begin{aligned} a &= q_0b + r_0, & 0 < r_0 < b \\ b &= q_1r_0 + r_1, & 0 < r_1 < r_0 \\ r_0 &= q_2r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_3r_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \end{aligned}$$

a więc w następnym kroku dzielimy poprzednią resztę przez następną resztę. Można zauważyć, że

$$\text{NWD}(a, b) = \text{NWD}(b, r_0) = \text{NWD}(r_0, r_1) = \text{NWD}(r_1, r_2) = \dots$$

i ponieważ ciąg reszt jest ściśle malejącym ciągiem liczb całkowitych nieujemnych to po skończonej ilości kroków musimy otrzymać resztę równą zero. Zgodnie z wcześniejszym stwierdzeniem największym wspólnym dzielnikiem liczb  $a$  i  $b$  będzie ostatnia niezerowa reszta w tym procesie. Opisany algorytm znajdowania największego wspólnego dzielnika nosi nazwę **Algorytmu Euklidesa**. Pokażemy teraz na przykładzie działanie tego algorytmu.

**Zadanie** Wyznaczyć przy pomocy Algorytmu Euklidesa największy wspólny

dzielnik liczb 324 i 148. A więc wykonujemy kolejne dzielenia:

$$\begin{aligned}324 &= 2 \cdot 148 + 28 \\148 &= 5 \cdot 28 + 8 \\28 &= 3 \cdot 8 + 4 \\8 &= 4 \cdot 2 + 0\end{aligned}$$

Ostatnią niezerową resztą jest 4. To oznacza, że  $NWD(324, 148) = 4$ . Jest to dużo lepszy i szybszy algorytm od rozkładania liczb na czynniki pierwsze.

Pokażemy teraz, że korzystając z powyższego algorytmu można poszukiwać całkowitych rozwiązań równania  $ax + by = NWD(a, b)$ . Jak można znaleźć te liczby?

W przypadku liczb  $a = 324$ ,  $b = 148$  równanie to rozwiązujemy w następujący sposób. Najpierw z przedostatniego kroku możemy wyznaczyć 4 jako:

$$4 = 28 - 3 \cdot 8$$

dalej krok wyżej mamy  $8 = 148 - 5 \cdot 28$  podstawiając to do wcześniej otrzymanego wzoru mamy:

$$4 = 28 - 3 \cdot 8 = 28 - 3 \cdot (148 - 5 \cdot 28) = 16 \cdot 28 - 3 \cdot 148$$

w kroku wyżej mamy formułę na 28, więc możemy otrzymać:

$$4 = 28 - 3 \cdot 8 = 16 \cdot 28 - 3 \cdot 148 = 16 \cdot (324 - 2 \cdot 148) - 3 \cdot 148 = 16 \cdot 324 - 35 \cdot 148$$

co daje nam jedno z możliwych rozwiązań całkowitych równania  $324u + 148v = 4$ , a mianowicie  $u = 16$ ,  $v = -35$ .

A więc Algorytm Euklidesa można wykorzystywać nie tylko do poszukiwania największego wspólnego dzielnika dwóch liczb, ale również do rozwiązywania równań typu

$$ax + by = NWD(a, b)$$

Wprost z powyższych rozumowań można wywnioskować następujące Twierdzenie:

**Twierdzenie 3** *Niech  $a, b$  będą dwiema liczbami całkowitymi z których przynajmniej jedna liczba jest różna od 0. Wtedy istnieją liczby całkowite  $u, v$ , takie że*

$$ua + vb = NWD(a, b)$$

Z powyższego twierdzenia wynika natychmiast następujący wniosek:

**Wniosek 1** Liczba  $d$  jest największym wspólnym dzielnikiem liczb  $a$  i  $b$  wtedy i tylko wtedy gdy

- (i)  $d|a$  i  $d|b$ ,
- (ii) jeśli  $c|a$  i  $c|b$  to  $c|d$

**Dowód**

( $\Rightarrow$ ) Niech  $d = \text{NWD}(a, b)$  wtedy zgodnie z powyższym twierdzeniem istnieją liczby całkowite  $u$  i  $v$  takie, że  $d = ua + vb$ . Jeśli liczba  $c|a$  i  $c|b$  to  $a = kc$ ,  $b = lc$  dla pewnych  $k, l$ . Stąd  $d = ukc + vlc = (uk + vl)c$ , a więc  $c|d$ .

( $\Leftarrow$ ) Jeśli  $c|d$  to  $c \leq d$  a więc punkty (i), (ii) pociągają warunki:

- (i)  $d|a$  i  $d|b$ ,
- (ii) jeśli  $c|a$  i  $c|b$  to  $c \leq d$

które stanowią definicję największego wspólnego dzielnika.  $\square$