

Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 1

Operacje na zbiorach i algebra zbiorów.

Indukcja matematyczna

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



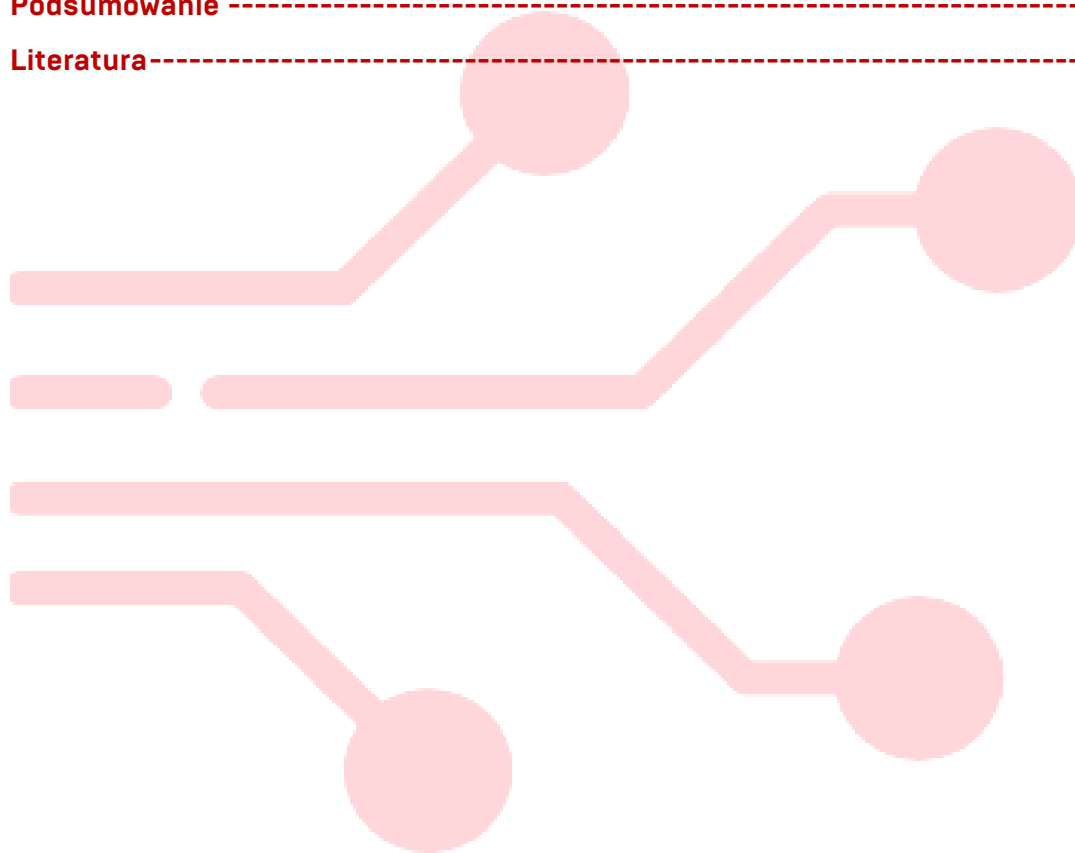
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć -----	3
Cel ćwiczenia/laboratorium -----	5
Instrukcja laboratoryjna/ćwiczeniowa -----	5
Ćwiczenia samodzielne -----	17
Pytania pomocnicze -----	21
Podsumowanie -----	22
Literatura -----	22



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

1. Zbiory – pojęcia podstawowe

Zbiór jest nieuporządkowaną kolekcją obiektów zwanych elementami zbioru. Przynależność elementu x do zbioru A zapisujemy jako $x \in A$, natomiast brak przynależności jako $x \notin A$.

Zbiór A jest podzbiorem zbioru B (co zapisujemy $A \subseteq B$), jeżeli każdy element zbioru A jest jednocześnie elementem zbioru B . Jeżeli $A \subseteq B$ oraz $A \neq B$, to A jest podzbiorem właściwym zbioru B .

Zbiór pusty, oznaczany przez $\emptyset$, jest zbiorem nieposiadającym żadnych elementów i jest podzbiorem każdego zbioru.

Zbiory mogą być opisywane:

- przez wyliczenie elementów,
- za pomocą warunku logicznego, np.

$$A = \{x \in \mathbb{N} \mid x < 5\}.$$

Zbiorem potęgowym zbioru A , oznaczanym jako $\mathcal{P}(A)$, nazywamy zbiór wszystkich podzbiorów zbioru A . Jeżeli zbiór A ma n elementów, to zbiór potęgowy $\mathcal{P}(A)$ ma 2^n elementów.

2. Algebra zbiorów

Dla danych zbiorów A i B definiujemy następujące działania:

- **suma zbiorów**

$$A \cup B = \{x \mid x \in A \text{ lub } x \in B\},$$

- **iloczyn (część wspólna)**

$$A \cap B = \{x \mid x \in A \text{ i } x \in B\},$$

- **różnica zbiorów**

$$A \setminus B = \{x \mid x \in A \text{ i } x \notin B\},$$

- **dopełnienie zbioru**

$$A^c = \{x \in X \mid x \notin A\},$$

gdzie X jest ustaloną przestrzenią (zbiorem uniwersalnym).



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Działania na zbiorach spełniają prawa analogiczne do praw algebry i rachunku zdań, w szczególności:

- **prawo przemienności:**

$$A \cup B = B \cup A, A \cap B = B \cap A,$$

- **prawo łączności:**

$$(A \cup B) \cup C = A \cup (B \cup C),$$

- **prawa rozdzielności:**

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

- **prawa de Morgana:**

$$(A \cup B)^c = A^c \cap B^c, (A \cap B)^c = A^c \cup B^c.$$

Równość zbiorów najczęściej dowodzi się poprzez wykazanie wzajemnych inkluzji.

3. Indukcja matematyczna

Zasada indukcji matematycznej jest podstawową metodą dowodzenia twierdzeń dotyczących liczb naturalnych. Aby udowodnić, że pewna własność $P(n)$ zachodzi dla wszystkich $n \in \mathbb{N}$, należy wykonać następujące kroki:

- a) **Baza indukcji** – wykazać, że własność $P(n)$ jest prawdziwa dla najmniejszej rozpatrywanej liczby naturalnej (najczęściej $n = 1$ lub $n = 0$).
- b) **Założenie indukcyjne** – przyjąć, że własność $P(k)$ jest prawdziwa dla pewnego ustalonego $k \in \mathbb{N}$.
- c) **Krok indukcyjny** – wykazać, że z prawdziwości $P(k)$ wynika prawdziwość $P(k + 1)$.

Jeżeli wszystkie powyższe kroki zostaną spełnione, to własność $P(n)$ zachodzi dla wszystkich $n \in \mathbb{N}$.

Indukcja matematyczna znajduje zastosowanie m.in. w dowodach tożsamości algebraicznych, własności ciągów, nierówności oraz twierdzeń dotyczących podzielności liczb naturalnych.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cel ćwiczenia/laboratorium

Celem ćwiczenia jest:

- utrwalenie podstawowych pojęć i metod matematyki dyskretnej, w szczególności teorii zbiorów, algebry zbiorów oraz zasady indukcji matematycznej,
- wykształcenie umiejętności poprawnego zapisu i interpretacji zbiorów,
- nabycie umiejętności wykonywania działań na zbiorach,
- rozwinięcie umiejętności dowodzenia równości i zależności między zbiorami,
- opanowanie stosowania indukcji matematycznej w dowodach tożsamości, nierówności oraz własności podzielności liczb naturalnych,
- przygotowanie do dalszych zagadnień matematyki dyskretnej poprzez wykorzystanie powyższych umiejętności.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 1.1

Podaj elementy zbiorów:

- 1) $A = \{a, b, c\}$
- 2) $B = \{a, \{a\}, b, \{a, b\}\}$
- 3) $C = 2^{\{a, b, c\}} = \mathcal{P}(\{a, b, c\})$

Rozwiązanie

Ad 1) W przypadku zbioru $A = \{a, b, c\}$ mamy do czynienia ze zbiorem trójelementowym, którego elementami są litery a, b, c . Jest to klasyczny zapis prostego zbioru złożonego z trzech elementów.

Ad 2) W przypadku zbioru $B = \{a, \{a\}, b, \{a, b\}\}$ mamy do czynienia z bardziej wyrafinowanym zapisem. Zbiór B składa się z 4 elementów. Pierwszym z nich jest litera a , drugim zaś jest zbiór jednoelementowy $\{a\}$. W tym miejscu należy zauważyć, że $a \neq \{a\}$. Ponadto do zbioru B należą litera b oraz zbiór dwuelementowy $\{a, b\}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ad 3) W przypadku ostatniego zbioru $C = 2^{\{a,b,c\}}$ mamy do czynienia z bardzo specyficznym zbiorem. Zapis ten oznacza zbiór potęgowy, czyli zbiór złożony ze wszystkich podzbiorów danego zbioru. W przypadku zbioru trójelementowego $\{a, b, c\}$ można określić aż 8 różnych podzbiorów. Pierwszym, dość nieoczywistym podzbiorem jest zbiór pusty $\emptyset$. Zbiór pusty $\emptyset$ jest bowiem podzbiorem dowolnego zbioru i z definicji jest elementem każdego zbioru potęgowego. Do zbioru C należą również 3 podzbiory jednoelementowe $\{a\}$, $\{b\}$ oraz $\{c\}$. Ponadto do zbioru C należą 3 zbiory dwuelementowe $\{a, b\}$, $\{a, c\}$ oraz $\{b, c\}$. Ostatnim elementem zbioru C jest zbiór trójelementowy $\{a, b, c\}$.

Łatwo zauważyć, że zbiór C składa się z 8 elementów. Jest to zgodne z własnościami zbiorów potęgowych podanych na wykładzie oraz we wprowadzeniu. Pamiętamy bowiem, że liczba elementów zbioru potęgowego dowolnego zbioru A , wynosi $2^{\bar{A}}$, gdzie $\bar{A}$ oznacza liczbę elementów zbioru A .

Przykład 1.2

Podaj elementy następujących zbiorów:

$$A = \{x \in N: x \leq 3\}$$

$$B = \{x \in N: x^2 < 7\}$$

$$C = \{x \in N: x^2 + 2x + 1 \leq 10\}$$

$$D = \{x \in Z: x \leq 3\}$$

$$E = \{x \in Z: x^2 < 7\}$$

$$F = \{x \in Z: x^2 + 2x + 1 \leq 10\}$$

$$G = \{x \in R: x \leq 3\}$$

$$H = \{x \in R: x^2 < 7\}$$

$$I = \{x \in R: x^2 + 2x + 1 \leq 10\}$$

Rozwiązanie:

Na wstępie prześledźmy uważnie zapis stosowany w przykładzie.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Mianowicie $\{x \in X: \phi(x)\}$ oznacz, że analizowany zbiór składa się ze wszystkich liczb należących do zbioru X spełniających własność $\phi(x)$.

W przypadku zbioru $A = \{x \in N: x \leq 3\}$ mamy do czynienia ze zbiorem liczb naturalnych, dla których prawdziwa jest nierówność $x \leq 3$. Zatem do naszego zbioru należą tylko 4 liczby naturalne 0,1,2 oraz 3. Można zatem zbiór A opisać w inny równoważny sposób, a mianowicie

$$A = \{x \in N: x \leq 3\} = \{0, 1, 2, 3\}$$

W przypadku zbioru $B = \{x \in N: x^2 < 7\}$ mamy również do czynienia z podzbiorem liczb naturalnych. Nie mniej jednak, tym razem, elementy zbioru muszą spełniać nierówność $x^2 < 7$. Łatwo sprawdzić, że nierówność ta jest równoważna układowi nierówności

$$-\sqrt{7} < x < \sqrt{7}.$$

Należy jednak pamiętać, że elementami zbioru B są liczby naturalne. Powyższa nierówność spełniona jest jedynie przez trzy liczby naturalne: 0,1,2. Zbiór B można zatem zapisać w równoważnej postaci

$$B = \{x \in N: x^2 < 7\} = \{0, 1, 2\}.$$

W przypadku zbioru $C = \{x \in N: x^2 + 2x + 1 \leq 10\}$ mamy podobną sytuację jak w poprzednim przykładzie. Elementami zbioru C są wszystkie liczby naturalne spełniające zadaną nierówność.

$$x^2 + 2x + 1 \leq 10$$

Przenosimy 10 na lewą stronę:

$$x^2 + 2x - 9 \leq 0$$

Obliczamy deltę:

$$\Delta = 2^2 - 4 \cdot 1 \cdot (-9) = 4 + 36 = 40$$

Wyznaczamy miejsca zerowe:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$x = \frac{-2 \pm \sqrt{40}}{2} = -1 \pm \sqrt{10}$$

Ponieważ współczynnik przy x^2 jest dodatni, nierówność ≤ 0 jest spełniona między pierwiastkami.

$$x \in [-1 - \sqrt{10}, -1 + \sqrt{10}]$$

Nie mniej jednak do zbioru C należą jedynie liczby naturalne, zatem ostateczna odpowiedź to $C = \{0, 1, 2\}$.

Dla pozostałych zbiorów mamy do czynienia z niewielką modyfikacją powyższych przypadków. W przypadku zbiorów D , E oraz F mamy podzbiory liczb całkowitych, zaś w ostatnich trzech przypadkach podzbiory liczb rzeczywistych. Po uwzględnieniu powyższych rozważań mamy zatem

$$D = \{x \in \mathbb{Z}: x \leq 3\} = \{\dots, -3, -2, -1, 0, 1, 2, 3\}$$

$$E = \{x \in \mathbb{Z}: x^2 < 7\} = \{-2, -1, 0, 1, 2\}$$

$$F = \{x \in \mathbb{Z}: x^2 + 2x + 1 \leq 10\} = \{-2, -1, 0, 1, 2\}$$

$$G = \{x \in \mathbb{R}: x \leq 3\} = (-\infty; 3]$$

$$H = \{x \in \mathbb{R}: x^2 < 7\} = (-\sqrt{7}, \sqrt{7})$$

$$I = \{x \in \mathbb{R}: x^2 + 2x + 1 \leq 10\} = [-1 - \sqrt{10}, -1 + \sqrt{10}]$$

Przykład 1.3

Podaj elementy następujących zbiorów:

a) $A = \{x \in \mathbb{Z} \mid -3 \leq x < 4\}$

b) $B = \{x \in \mathbb{N} \mid x^2 < 20\}$

c) $C = \mathcal{P}(\{a, b\})$

Rozwiązanie:

Ad a) Zbiór A zawiera wszystkie liczby całkowite od -3 do 3 , zatem



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$A = \{-3, -2, -1, 0, 1, 2, 3\}.$$

Ad b) Szukamy liczb naturalnych, których kwadrat jest mniejszy od 20. Są to 0, 1, 2, 3, 4, ponieważ $4^2 = 16 < 20$, a $5^2 = 25 > 20$. Zatem $B = \{0, 1, 2, 3, 4\}$.

Ad c) Zbiór potęgowy zbioru dwuelementowego zawiera $2^2 = 4$ elementy:

$$C = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Przykład 1.4

Dla danych zbiorów $A = \{1, 2, 3, 4\}$ oraz $B = \{3, 4, 5, 6\}$ oblicz:

a) $A \cup B$

b) $A \cap B$

c) $A \setminus B$

Rozwiązanie:

a) $A \cup B = \{1, 2, 3, 4, 5, 6\}$

b) $A \cap B = \{3, 4\}$

c) $A \setminus B = \{1, 2\}$

Przykład 1.5

Niech X będzie zbiorem wszystkich czworokątów,

A – zbiorem kwadratów,

B – zbiorem prostokątów,

C – zbiorem rombów.

Wyznaczyć zbiory:

a) $A \cap B$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



b) $B \setminus A$

c) $A \cap C$

Rozwiązanie:

Ad a) Każdy kwadrat jest prostokątem, więc $A \cap B = A$.

Ad b) Są to prostokąty, które nie są kwadratami.

Ad c) Każdy kwadrat jest rombem, więc $A \cap C = A$.

Przykład 1.6

Udowodnić, że dla dowolnych zbiorów A, B, C zachodzi:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Idea dowodu

Żeby udowodnić równość zbiorów, najczęściej pokazujemy dwie inkluzje:

1. $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

2. $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$

To daje równość.

Krok 1: $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Weźmy dowolny element x taki, że

$$x \in A \cap (B \cup C)$$

Z definicji przekroju $\cap$ oznacza to równocześnie:

$$x \in A \text{ oraz } x \in (B \cup C)$$

A z definicji sumy $\cup$ mamy:

$$x \in (B \cup C) \Leftrightarrow (x \in B) \text{ lub } (x \in C)$$

Czyli mamy dwa przypadki:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przypadek 1: $x \in B$

Wtedy (ponieważ już wiemy, że $x \in A$):

$$x \in A \cap B$$

A jeżeli $x \in A \cap B$, to na pewno zachodzi:

$$x \in (A \cap B) \cup (A \cap C)$$

Przypadek 2: $x \in C$

Analogicznie, skoro $x \in A$, to:

$$x \in A \cap C$$

A więc znów:

$$x \in (A \cap B) \cup (A \cap C)$$

W obu przypadkach x należy do prawej strony, więc inkluzja zachodzi.

Krok 2: $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$

Weźmy dowolny x taki, że:

$$x \in (A \cap B) \cup (A \cap C)$$

Z definicji sumy zbiorów:

$$x \in (A \cap B) \cup (A \cap C) \Leftrightarrow (x \in A \cap B) \text{ lub } (x \in A \cap C)$$

Zatem znów rozbijamy na przypadki.

Przypadek 1: $x \in A \cap B$

Wtedy:

- $x \in A$
- $x \in B$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



jednocześnie.

Skoro $x \in B$, to automatycznie $x \in (B \cup C)$.

Zatem (bo $x \in A$ i $x \in (B \cup C)$):

$$x \in A \cap (B \cup C)$$

Przypadek 2: $x \in A \cap C$

Wtedy:

- $x \in A$
- $x \in C$

jednocześnie.

Skoro $x \in C$, to również $x \in (B \cup C)$.

Zatem znów:

$$x \in A \cap (B \cup C)$$

Czyli w obu przypadkach element należy do lewej strony. Inkluzja zachodzi.

Wniosek

Mamy obie inkluzje, więc:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Przykład 1.7

Udowodnij, że dla każdego $n \in \mathbb{N}$:

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

Krok 1:

Dla $n = 1$:

Lewa strona: 1



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Prawa strona: $\frac{1 \cdot 2}{2} = 1$

Zgadza się $L=P$

Krok 2: założenie indukcyjne

Zakładamy, że dla pewnego $k \geq 1$ zachodzi:

$$1 + 2 + \dots + k = \frac{k(k+1)}{2}$$

Krok 3: krok indukcyjny

Musimy pokazać, że wtedy zachodzi też dla $k+1$:

$$1 + 2 + \dots + k + (k+1) = \frac{(k+1)(k+2)}{2}$$

Zaczynamy od lewej strony:

$$1 + 2 + \dots + k + (k+1)$$

Podstawiamy za sumę do k z założenia indukcyjnego:

$$1 + 2 + \dots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

Wyciągamy $(k+1)$ przed nawias:

$$= (k+1) \left(\frac{k}{2} + 1 \right) = (k+1) \left(\frac{k+2}{2} \right) = \frac{(k+1)(k+2)}{2}$$

Czyli teza dla $k+1$ wynika z tezy dla k . Udowodnione.

Przykład 1.8

Udowodnij, że dla każdego $n \in \mathbb{N}$:

$$1 + 3 + 5 + \dots + (2n-1) = n^2$$

Krok 1: $n = 1$

Lewa: 1



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Prawa: $1^2 = 1$

L=P

Krok 2. Założenie

Dla k :

$$1 + 3 + \dots + (2k - 1) = k^2$$

Krok 3.

Dla $k + 1$:

$$1 + 3 + \dots + (2k - 1) + (2(k + 1) - 1) =$$

$$k^2 + (2k + 1)$$

$$= k^2 + 2k + 1 = (k + 1)^2$$

C.N.D.

Przykład 1.9

Udowodnij, że dla każdego $n \geq 0$:

$$1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$$

Krok 1: $n = 0$

Lewa: 1

Prawa: $2^1 - 1 = 1$

Krok 2. Założenie

Dla k :



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$1 + 2 + \dots + 2^k = 2^{k+1} - 1$$

Krok 3.

Dodajemy kolejny składnik 2^{k+1} :

$$1 + 2 + \dots + 2^k + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{k+2} - 1$$

A to jest dokładnie $2^{(k+1)+1} - 1$

Przykład 1.10

Udowodnij, że dla każdego $n \in \mathbb{N}$ zachodzi podzielność:

$$6 \mid (n^3 - n)$$

czyli że $n^3 - n$ jest zawsze podzielne przez 6.

Krok 1.

Dla $n = 1$:

$$1^3 - 1 = 0$$

0 jest podzielne przez 6.

Krok 2. Założenie

Zakładamy, że dla pewnego $k \geq 1$ zachodzi:

$$6 \mid (k^3 - k)$$

czyli istnieje liczba całkowita t taka, że:

$$k^3 - k = 6t$$

Krok 3.

Musimy pokazać, że:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$6 \mid ((k+1)^3 - (k+1))$$

Liczymy:

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - k - 1 \\ &= k^3 + 3k^2 + 2k\end{aligned}$$

Wyciągamy część z założenia indukcyjnego:

$$= (k^3 - k) + (3k^2 + 3k)$$

$$\text{bo } (k^3 - k) + (3k^2 + 3k) = k^3 + 3k^2 + 2k.$$

Teraz:

- z założenia: $(k^3 - k)$ jest podzielne przez 6,
- sprawdźmy $(3k^2 + 3k)$:

$$3k^2 + 3k = 3k(k+1)$$

Czyli mamy iloczyn $k(k+1)$ – dwóch kolejnych liczb, więc jedna z nich jest parzysta, zatem:

$$k(k+1) \text{ jest podzielne przez } 2$$

Czyli istnieje całkowite m , takie że:

$$k(k+1) = 2m$$

Wtedy:

$$3k(k+1) = 3 \cdot 2m = 6m$$

A więc $(3k^2 + 3k)$ też jest podzielne przez 6.

Skoro suma dwóch liczb podzielnych przez 6 jest podzielna przez 6, to:

$$(k^3 - k) + (3k^2 + 3k)$$

jest podzielne przez 6, czyli:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$6 \mid ((k+1)^3 - (k+1))$$

C.N.D

Ćwiczenia samodzielne

Zadanie 1.1

Podaj elementy następujących zbiorów:

$$A = \{a, b, c, d\}$$

$$B = \{a, \{b, c\}, d\}$$

$$C = \{x \in \mathbb{N} : x \leq 10\}$$

$$D = \{x \in \mathbb{N} : x = -2\}$$

$$E = \{x \in \mathbb{N} : |x - 3| \leq 5\}$$

$$F = \{x \in \mathbb{Z} : |x - 2| \leq 2\}$$

$$G = \{x \in \mathbb{N} : x^2 - 2 < 1\}$$

$$H = \{x \in \mathbb{Z} : |x| = 2\}$$

$$I = \{x \in \mathbb{R} : x^2 + 1 \geq 0\}$$

Zadanie 1.2

Dla zadanych zbiorów $A = \{a, b, c, d, e\}$ oraz $B = \{a, c, e, f, g, h\}$ oblicz:

- 1) $A \setminus B$
- 2) $B \setminus A$
- 3) $A \cup B$
- 4) $A \cap B$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 1.3

Dla zadanych zbiorów $A = \{x \in \mathbb{N}: x \leq 10\}$ oraz $B = \{x \in \mathbb{N}: x \geq 5\}$ oblicz:

- 1) $A \setminus B$
- 2) $B \setminus A$
- 3) $A \cup B$
- 4) $A \cap B$

Zadanie 1.4

Dla zadanych zbiorów $A = \{x \in \mathbb{R}: x \leq 10\}$ oraz $B = \{x \in \mathbb{R}: x \geq 5\}$

oblicz $A \setminus B; B \setminus A; A \cup B; A \cap B$.

Zadanie 1.5

Niech X będzie zbiorem wszystkich wielokątów i niech A będzie zbiorem trójkątów prostokątnych, B zbiorem trójkątów równoramiennych C zbiorem trójkątów równobocznych. Wyznaczyć zbiory

- 1) $(A \cap B) \cap C$
- 2) $(A \cap \neg B) \cap C$
- 3) $(\neg A) \cap (B \cap C)$
- 4) $(\neg A) \cap (\neg B \cap C)$
- 5) $(A \cap B) \cap (\neg C)$

Zadanie 1.6

Udowodnić, że przy ustalonej przestrzeni X dla wszystkich zbiorów A, B, C zachodzą następujące równości

- 1) $A \cup B = B \cup A$
- 2) $A \cap B = B \cap A$
- 3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$4) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$5) A \cup \emptyset = A$$

$$6) A \cap \emptyset = \emptyset$$

Zadanie 1.7

Sprawdzić, czy poniższe równości są tożsamościami. Jeżeli nie, podać odpowiedni kontrprzykład.

$$1) A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$

$$2) A \cup (A \cap B) = A$$

$$3) A \cap (B \cup C) = B$$

Zadanie 1.8

Dowieść, że dla wszystkich zbiorów A, B oraz C zachodzą następujące implikacje bądź równoważności

$$1) (A \subset B) \wedge (C \subset D) \Rightarrow (A \cap C) \subset (B \cap D)$$

$$2) A \setminus B = B \setminus A \Rightarrow A = B$$

$$3) A \subset B \Rightarrow (C \setminus B) \subset (C \setminus A)$$

Zadanie 1.9

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Zadanie 1.10

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$1^3 + 2^3 + \dots + n^3 = (1 + 2 + \dots + n)^2 = \frac{n^2(n+1)^2}{4}$$

Zadanie 1.11



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$$

Zadanie 1.12

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$\sum_{i=1}^n \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$$

Zadanie 1.13

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$\sum_{i=1}^n (2i-1) = n^2$$

Zadanie 1.14

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$2^n > n$$

Zadanie 1.15

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$2|(n^2 + n)$$

Zadanie 1.16

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi

$$30|(n^5 - n)$$

Zadanie 1.17

Udowodnić, że dla każdej liczby $n \in \mathbb{N}$ zachodzi



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$6|(n^3 + 5n)$$

Pytania pomocnicze

- 1) Czym różni się zapis $x \in A$ od $x \subseteq A$? Podaj przykład, gdzie elementem zbioru jest inny zbiór.
- 2) Podaj różnicę między $\emptyset$ a $\{\emptyset\}$. Ile elementów ma każdy z tych zbiorów?
- 3) Jak interpretujesz zapis zbioru metodą „warunku” (opisowej), np. $\{x \in \mathbb{Z}: x^2 < 10\}$? Jak przejść do zapisu przez wyliczenie elementów?
- 4) Podaj definicje działań: $A \cup B$, $A \cap B$, $A \setminus B$, A^c [dopełnienie w przestrzeni X].
- 5) Jak rozumiesz „przestrzeń [zbiór uniwersalny] X ” i dlaczego dopełnienie A^c zawsze zależy od wyboru X ?
- 6) Na czym polega dowodzenie równości zbiorów metodą podwójnej inkluzji? Jak wygląda schemat takiego dowodu?
- 7) Wymień prawa algebry zbiorów (przemienność, łączność, rozdzielność, de Morgana) i wskaż, do czego są najczęściej używane w uproszczeniach.
- 8) Podaj przykład, w którym $(A \cup B)^c = A^c \cap B^c$ widać „na elementach” (np. dla małych zbiorów liczbowych).
- 9) Jak sprawdzić, czy dana równość zbiorów jest tożsamością? (wskazówka: użyj albo praw algebry zbiorów, albo kontrprzykładu).
- 10) Opisz kroki dowodu indukcyjnego: baza, założenie indukcyjne, krok indukcyjny. Jaką rolę pełni założenie indukcyjne?
- 11) Dlaczego w kroku indukcyjnym wolno korzystać z założenia $P(n)$, ale nie wolno zakładać prawdziwości $P(n + 1)$?
- 12) Podaj przykład tezy, gdzie baza indukcji zaczyna się od $n = 0$, a nie od $n = 1$. Kiedy to jest naturalniejsze?
- 13) W zadaniach o podzielności: jak zwykle zapisuje się formalnie „ $6 \mid (7^n - 1)$ ” i jak wykorzystać to w indukcji?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Podsumowanie

W trakcie ćwiczeń utrwalono pojęcia związane z teorią zbiorów: przynależność, podzbiór, zbiór pusty, zapis zbiorów przez wyliczenie oraz opis warunkowy. Przećwiczone podstawowe działania na zbiorach: sumę, iloczyn, różnicę oraz dopełnienie w ustalonej przestrzeni X . Wykorzystano również podstawowe prawa algebry zbiorów (w tym prawa de Morgana) do przekształcania i upraszczania wyrażeń oraz do dowodzenia równości zbiorów.

Druga część ćwiczeń dotyczyła stosowania zasady indukcji matematycznej do dowodzenia twierdzeń o liczbach naturalnych: tożsamości sum, własności ciągów oraz podzielności. Zwrócono uwagę na poprawną strukturę dowodu: baza indukcji, założenie indukcyjne oraz krok indukcyjny. Umiejętności te stanowią fundament dla dalszych zagadnień matematyki dyskretnej, w szczególności w analizie struktur dyskretnych i dowodach własności algorytmów.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 2

Relacje i ich własności

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	25
Własności relacji (klasyfikacja)	25
Relacja równoważności	26
Cel ćwiczenia/laboratorium	27
Instrukcja laboratoryjna/ćwiczeniowa	28
Ćwiczenia samodzielne	34
Pytania pomocnicze	37
Podsumowanie	37
Literatura	38



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Relacja binarna

Niech A, B będą zbiorami.

Relacją binarną R z A do B nazywamy dowolny podzbiór iloczynu kartezjańskiego:

$$R \subseteq A \times B.$$

Jeżeli $A = B$, mówimy o relacji na zbiorze A :

$$R \subseteq A \times A.$$

Dla $(a, b) \in R$ zapisujemy:

$$a R b.$$

Własności relacji (klasyfikacja)

Niech $R \subseteq A \times A$.

Relacja zwrotna (reflexive)

$$R \text{ jest zwrotna} \Leftrightarrow \forall_{a \in A} (a, a) \in R.$$

Relacja przeciwzwrotna (irreflexive, antyzwrotna)

$$R \text{ jest przeciwzwrotna} \Leftrightarrow \forall_{a \in A} (a, a) \notin R.$$

Relacja symetryczna (symmetric)

$$R \text{ jest symetryczna} \Leftrightarrow \forall_{a, b \in A} ((a, b) \in R \Rightarrow (b, a) \in R).$$

Relacja antysymetryczna (antisymmetric)

$$R \text{ jest antysymetryczna} \Leftrightarrow \forall_{a, b \in A} ((a, b) \in R \wedge (b, a) \in R \Rightarrow a = b).$$

Uwaga: antysymetryczność $\neq$ asymetryczność.

Relacja słabo antysymetryczna

Najczęściej spotykana definicja (równoważna antysymetryczności):

$$\forall_{a \neq b} \sim((a, b) \in R \wedge (b, a) \in R).$$

Relacja asymetryczna (asymmetric)

$$R \text{ jest asymetryczna} \Leftrightarrow \forall_{a, b \in A} ((a, b) \in R \Rightarrow (b, a) \notin R).$$

Własność:

$$\text{asymetryczna} \Rightarrow \text{przeciwzwrotna}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Relacja przechodnia (transitive)

R jest przechodnia $\Leftrightarrow \forall_{a,b,c \in A} ((a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R)$.

Relacja spójna (total, connected)

R jest spójna $\Leftrightarrow \forall_{a,b \in A} (a \neq b \Rightarrow (a,b) \in R \vee (b,a) \in R)$.

Relacja równoważności

Relacja $R \subseteq A \times A$ jest relacją równoważności, gdy jest:

- zwrotna
- symetryczna
- przechodnia

Formalnie:

$$\forall_{a \in A} (a,a) \in R$$

$$\forall_{a,b \in A} ((a,b) \in R \Rightarrow (b,a) \in R)$$

$$\forall_{a,b,c \in A} ((a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R)$$

Klasy abstrakcji (klasy równoważności)

Dla $a \in A$:

$$[a]_R = \{x \in A \mid (a,x) \in R\}.$$

Własności:

$$aRb \Leftrightarrow [a]_R = [b]_R$$

Zbiór wszystkich klas:

$$A/R = \{[a]_R \mid a \in A\}.$$

Klasy tworzą rozbitcie (partycję) zbioru A .

Relacje porządku

Porządek częściowy (partial order)

Relacja R jest porządkiem częściowym, gdy jest:

- zwrotna
- antysymetryczna
- przechodnia



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Porządek ostry (strict partial order)

Relacja R jest ostrym porządkiem, gdy jest:

- przeciwzrotna
- przechodnia

Relacja R jest porządkiem liniowym, gdy:

- jest porządkiem częściowym
- jest spójna

$$\forall_{a,b \in A} (a \neq b \Rightarrow aRb \vee bRa)$$

Relacja R jest dobrym porządkiem, gdy:

- jest porządkiem liniowym
- każdy niepusty podzbiór $B \subseteq A$ ma element najmniejszy:

$$\forall_{B \subseteq A} (B \neq \emptyset \Rightarrow \exists_{m \in B} \forall_{b \in B} mRb)$$

Porównanie kluczowych klas relacji

Typ relacji	Zwrotna	Symetryczna	Antysymetryczna	Przechodnia
Równoważność	Tak	Tak	Nie	Tak
Porządek częściowy	Tak	Nie	Tak	Tak
Porządek liniowy	Tak	Nie	Tak	Tak
Porządek ostry	Nie	Nie	Tak	Tak

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest zapoznanie studentów z pojęciem relacji binarnej oraz jej podstawowymi własnościami. Studenci uczą się rozpoznawać i formalnie badać własności relacji, takie jak zwrotność, symetria, antysymetria, przechodniość i spójność.

Ponadto celem zajęć jest:

- opanowanie pojęcia relacji równoważności i klas abstrakcji,
- zrozumienie idei zbioru ilorazowego,
- analiza relacji porządku: częściowego, liniowego i ostrego,
- umiejętność wyznaczania elementów minimalnych, maksymalnych, najmniejszych i największych,



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- kształcenie umiejętności formalnego dowodzenia własności relacji przy użyciu definicji i kwantyfikatorów.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 2.1

Niech $A = \{1,2,3\}$. Niech $R \subseteq A \times A$ będzie relacją:

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}.$$

Zbadaj, czy R jest: zwrotna, przeciwzwrotna, symetryczna, asymeryczna, przechodnia.

Rozwiązanie

Zwrotność:

$$R \text{ zwrotna} \Leftrightarrow \bigwedge_{a \in A} (a, a) \in R$$

Sprawdzamy: $(1,1), (2,2), (3,3) \in R$. Zatem R jest zwrotna.

Przeciwzwrotność:

$$R \text{ przeciwzwrotna} \Leftrightarrow \bigwedge_{a \in A} (a, a) \notin R$$

Ponieważ $(1,1) \in R$, to warunek jest fałszywy, więc R **nie** jest przeciwzwrotna.

Symetryczność:

$$R \text{ symetryczna} \Leftrightarrow \bigwedge_{a,b \in A} (a, b) \in R \Rightarrow (b, a) \in R.$$

Sprawdzamy pary „niediagonalne”: mamy $(1,2) \in R$ oraz $(2,1) \in R$. Dla par diagonalnych symetria zachodzi automatycznie (bo (a,a) przechodzi w siebie). Zatem zachodzi własność

$$\forall_{a,b \in A} ((a, b) \in R \Rightarrow (b, a) \in R)$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



stąd R jest **symetryczna**.

Antysymetryczność:

$$R \text{ antysymetryczna} \Leftrightarrow \bigwedge_{a,b \in A} ((a,b) \in R \wedge (b,a) \in R \Rightarrow a = b).$$

Niech $a = 1, b = 2$. Wtedy $(1,2) \in R \wedge (2,1) \in R$, ale $1 \neq 2$. Zatem istnieje kontrprzykład. Relacja R **nie** jest antysymetryczna.

Przechodność:

$$R \text{ przechodnia} \Leftrightarrow \forall_{a,b,c \in A} ((a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R).$$

Sprawdźmy $a = 1, b = 2, c = 1$. Mamy $(1,2) \in R$ oraz $(2,1) \in R$. Wtedy przechodność wymaga $(1,1) \in R$, co zachodzi.

Analogicznie $a = 2, b = 1, c = 2$ wymaga $(2,2) \in R$, co zachodzi. Innych par z elementami 3 brak, poza $(3,3)$. Zatem warunek przechodności jest spełniony, więc R jest **przechodnia**.

Przykład 2.2

Niech $A = \mathbb{Z}$. Zdefiniujmy relację R przez:

$$aRb \Leftrightarrow a \equiv b \pmod{4}.$$

Sprawdź, czy R jest relacją równoważności.

Rozwiązanie

Pokażemy: zwrotność, symetrię, przechodność.

Zwrotność: dla dowolnego $a \in \mathbb{Z}$ mamy $a - a = 0$, $4 \mid 0$, więc $a \equiv a \pmod{4}$.

Symetryczność: załóżmy, że aRb . Wtedy $4 \mid (a - b)$. Stąd $4 \mid -(a - b) = (b - a)$, więc bRa .

Przechodność: załóżmy, że $aRb \wedge bRc$. Wtedy $4 \mid (a - b)$ i $4 \mid (b - c)$.

Zatem $4 \mid [(a - b) + (b - c)] = a - c$, więc aRc .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wniosek: R jest relacją równoważności.

Przykład 2.3

Niech $A = \mathbb{Z}$ i relacja R dana wzorem:

$$aRb \Leftrightarrow 3 \mid (a - b)$$

- 1) Udowodnij, że R jest równoważnością.
- 2) Wyznacz $[0]_R, [1]_R, [2]_R$.
- 3) Wyznacz $\mathbb{Z}/R$ i jego moc.

Rozwiązanie

1) Równoważność

- Zwrotność: $3 \mid (a - a) = 0 \Rightarrow aRa$.
- Symetryczność: $3 \mid (a - b) \Rightarrow 3 \mid (b - a) \Rightarrow aRb \Rightarrow bRa$.
- Przechodność: $3 \mid (a - b) \wedge 3 \mid (b - c) \Rightarrow 3 \mid (a - c)$.

2) Klasy abstrakcji

$$[0]_R = \{x \in \mathbb{Z} : 3 \mid (x - 0)\} = \{x \in \mathbb{Z} : 3 \mid x\} = \{\dots, -6, -3, 0, 3, 6, \dots\}.$$

$$[1]_R = \{x \in \mathbb{Z} : 3 \mid (x - 1)\} = \{\dots, -5, -2, 1, 4, 7, \dots\}.$$

$$[2]_R = \{x \in \mathbb{Z} : 3 \mid (x - 2)\} = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

3) Zbiór ilorazowy i moc

Ponieważ każda liczba całkowita ma dokładnie jedną resztę z dzielenia przez 3, mamy dokładnie trzy klasy:

$$\mathbb{Z}/R = \{[0]_R, [1]_R, [2]_R\}, |\mathbb{Z}/R| = 3.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 2.4

Niech $A = \{1, 2, 3, 6, 12\}$. Definiujemy relację:

$$aRb \Leftrightarrow a \mid b.$$

- 1) Udowodnij, że R jest porządkiem częściowym na A .
- 2) Wyznacz elementy minimalne, maksymalne, najmniejszy, największy.
- 3) Czy R jest porządkiem liniowym?

Rozwiązanie

1) Porządek częściowy (=zwrotna + antysymetryczna + przechodnia)

- **Zwrotność:** $\forall_{a \in A} a \mid a$. Zatem $\forall_{a \in A} (aRa)$.
- **Antysymetryczność:** niech $a, b \in A$ oraz $a \mid b \wedge b \mid a$. Wtedy istnieją $k, \ell \in \mathbb{N}$ takie, że $b = ak$ oraz $a = b\ell$.

Podstawiając: $a = (ak)\ell = a(k\ell)$.

Ponieważ $a \neq 0$, dostajemy $k\ell = 1$, więc $k = \ell = 1$ i $a = b$.

Ostatecznie:

$$\forall_{a, b \in A} ((aRb \wedge bRa) \Rightarrow a = b).$$

- **Przechodniość:** jeżeli $a \mid b$ oraz $b \mid c$, to $a \mid c$.

Powyższa własność zachodzi, zatem

$$\forall_{a, b, c \in A} ((aRb \wedge bRc) \Rightarrow aRc).$$

Wniosek: R jest porządkiem częściowym.

2) Elementy minimalne/maksymalne/najmniejszy/największy

- Element **najmniejszy** m spełnia: $\forall_{x \in A} (mRx)$, czyli $m \mid x$ dla wszystkich x . Tu $1 \mid x$ dla każdego x , więc element **najmniejszy** = 1.
- Element **największy** M spełnia: $\forall_{x \in A} (xRM)$, czyli $x \mid M$ dla wszystkich x . Tu 12 jest podzielne przez wszystkie elementy A , więc **największy** = 12.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- Elementy **minimalne**: x jest minimalny, gdy nie istnieje $y \in A$ takie że yRx oraz $y \neq x$. Ponieważ $1 \mid x$ dla każdego $x \neq 1$, to żaden $x \neq 1$ nie jest minimalny. Zatem **minimalne**: $\{1\}$.
- Elementy **maksymalne**: x jest maksymalny, gdy nie istnieje $y \in A$ takie że xRy i $y \neq x$. Ponieważ dla 12 nie ma większego wielokrotnego w A , a dla 6 jest 12, dla 3 jest 6,12, itd., jedynym maksymalnym jest $\{12\}$.

3) Czy jest to porządek liniowy?

Porządek liniowy wymaga porównywalności wszystkich elementów:

$$\forall_{a \neq b} (aRb \vee bRa)$$

Niech $a = 2, b = 3$. Nie zachodzi $2 \mid 3$ ani $3 \mid 2$. Zatem:

$$\neg(2R3) \wedge \neg(3R2),$$

więc relacja **nie** jest liniowa.

Przykład 2.5

Niech $A = \mathbb{Z} \times \mathbb{Z}$. Definiujemy relację R :

$$(a, b) R (c, d) \Leftrightarrow a < c \vee (a = c \wedge b < d).$$

- 1) Wykaż, że R jest porządkiem ostrym (przeciwny i przechodni).
- 2) Wykaż, że R jest liniowy ostry: dla każdych różnych $x, y \in A$, zachodzi xRy lub yRx .

Rozwiązanie

1) Porządek ostry.

- **Przeciwność:**

Trzeba pokazać, że:

$$\forall (a, b) \in A \neg((a, b) R (a, b)).$$

Zakładamy przeciwnie, że $(a, b) R (a, b)$. Wtedy

$$a < a \vee (a = a \wedge b < b).$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Pierwszy człon jest fałszywy, bo $a < a$ nigdy nie zachodzi. Drugi wymaga $b < b$, co też jest fałszywe. Sprzeczność, więc relacja jest przeciwzrotna.

• Przechodność:

Pokażemy, że

$$\forall_{x,y,z \in A} ((xRy \wedge yRz) \Rightarrow xRz).$$

Niech $x = (a, b), y = (c, d), z = (e, f)$. Załóżmy, że $xRy \wedge yRz$.

Z xRy mamy: $a < c$ lub $(a = c \wedge b < d)$.

Z yRz mamy: $c < e$ lub $(c = e \wedge d < f)$.

Rozważmy przypadki:

- Jeżeli $a < c$ oraz $c < e$, to $a < e$, więc xRz .
- Jeżeli $a < c$ oraz $c = e \wedge d < f$, to nadal $a < e$, więc xRz .
- Jeżeli $a = c \wedge b < d$ oraz $c < e$, to $a < e$, więc xRz .
- Jeżeli $a = c \wedge b < d$ oraz $c = e \wedge d < f$, to $a = e$ oraz z $b < d < f$ wynika $b < f$. Zatem $(a = e \wedge b < f)$, więc xRz .

We wszystkich przypadkach xRz , więc R jest przechodnia. Zatem R jest ostrym porządkiem.

2) Liniowość ostra.

Należy wykazać, że spełniony musi być warunek:

$$\forall_{x \neq y \in A} (xRy \vee yRx)$$

Niech $x = (a, b) \neq (c, d) = y$. Wtedy albo $a \neq c$, albo $a = c$ oraz $b \neq d$.

- Jeżeli $a \neq c$, to zachodzi $a < c$ lub $c < a$. W pierwszym przypadku xRy , w drugim yRx .
- Jeżeli $a = c$ i $b \neq d$, to zachodzi $b < d$ lub $d < b$. W pierwszym przypadku xRy , w drugim yRx .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zatem dla każdych, różnych x, y zachodzi $xRy \vee yRx$. Relacja jest porządkiem liniowym ostrym.

Ćwiczenia samodzielne

Zadanie 2.1

Jakie własności mają poniższe relacje

a) $R = \{ \langle a, a \rangle, \langle b, b \rangle, \langle a, b \rangle \}$

b) $R = \{ \langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle, \langle a, b \rangle, \langle b, a \rangle \}$

c) $R = \{ \langle a, b \rangle, \langle a, c \rangle, \langle b, c \rangle, \langle c, c \rangle, \langle a, a \rangle, \langle b, b \rangle \}$

Zadanie 2.2

Zbadać jakie własności mają następujące relacje:

$$R \subset \mathbb{Z}^2 \wedge \bigwedge_{x,y \in \mathbb{Z}} xRy \Leftrightarrow 3|x - y$$

$$R \subset \mathbb{N}^2 \wedge \bigwedge_{x,y \in \mathbb{N}} xRy \Leftrightarrow 2|x + y$$

$$R \subset \mathbb{N}^2 \wedge \bigwedge_{x,y \in \mathbb{N}} xRy \Leftrightarrow x \neq 0 \wedge x|y$$

$$R \subset \mathbb{Z}^2 \wedge \bigwedge_{x,y \in \mathbb{Z}} xRy \Leftrightarrow (x = 2 \wedge y = 3)$$

$$R \subset \mathbb{R}^2 \wedge \bigwedge_{x,y \in \mathbb{R}} xRy \Leftrightarrow x^2 = y^2$$

$$R \subset \mathbb{R}^2 \wedge \bigwedge_{x,y \in \mathbb{R}} xRy \Leftrightarrow x^3 = y^3$$

$$R \subset \mathbb{R}^2 \wedge \bigwedge_{x,y \in \mathbb{R}} xRy \Leftrightarrow |x| + |y| = 3$$

Zadanie 2.3

Zbadać, czy relacja R jest relacją równoważności:

a) $X = \text{Par}, xRy \Leftrightarrow 3|x - y$

b) $X = \mathbb{R}, xRy \Leftrightarrow x - y = 2$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



c) $X = \mathbb{N}$, $xRy \Leftrightarrow 3|x + y$

d) $X = \mathbb{Z}$, $xRy \Leftrightarrow x^2 \leq y^2$

Zadanie 2.4

Niech $A = \mathbb{Z}$. Definiujemy relację $R \subseteq \mathbb{Z} \times \mathbb{Z}$ w następujący sposób:

$$a R b \Leftrightarrow a - b \text{ jest liczbą parzystą.}$$

- Udowodnij, że relacja R jest relacją równoważności na zbiorze $\mathbb{Z}$.
- Wyznacz klasy abstrakcji: $[0]_R$ oraz $[1]_R$.
- Opisz ogólną postać klasy abstrakcji $[a]_R$ dla dowolnego $a \in \mathbb{Z}$.
- Wyznacz zbiór ilorazowy $\mathbb{Z}/R$ i podaj jego moc.

Zadanie 2.5

Niech

$$A = \mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\}.$$

Definiujemy relację $R \subseteq A \times A$ następująco:

$$(a,b) R (c,d) \Leftrightarrow ad = bc.$$

Udowodnij, że relacja R jest relacją równoważności na zbiorze A .

Wyznacz klasę abstrakcji elementu $(1,2)$, tzn. opisz zbiór:

$$[(1,2)]_R.$$

Wykaż, że dla dowolnego $(a,b) \in A$ zachodzi:

$$[(a,b)]_R = \{(ka, kb) \mid k \in \mathbb{Z} \setminus \{0\}\}.$$

Zadanie 2.6

Niech $A = \{1,2,3,4\}$. Rozważ relację $R \subseteq A \times A$ daną przez:

$$a R b \Leftrightarrow a \leq b.$$

- Określ, czy R jest porządkiem częściowym.
- Czy relacja R jest porządkiem liniowym? Odpowiedź uzasadnij.
- Wyznacz element najmniejszy i największy w zbiorze A względem R .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 2.7

Niech $A = \mathbb{Z}$. Definiujemy relację R następująco:

$$a R b \Leftrightarrow |a| \leq |b|.$$

Czy relacja R jest porządkiem częściowym? Uzasadnij.

Czy istnieją w $(\mathbb{Z}, R)$ elementy minimalne lub najmniejsze?

Zadanie 2.8

Niech $A = \{1, 2, 3, 4, 6, 12\}$. Rozważ relację podzielności:

$$a R b \Leftrightarrow a \mid b.$$

Udowodnij, że relacja R jest porządkiem częściowym na A .

Wyznacz wszystkie elementy:

- minimalne,
- maksymalne,
- najmniejsze,
- największe

Odpowiedz, czy (A, R) jest porządkiem liniowym.

Zadanie 2.9

Niech $A = \mathbb{R}^2$. Definiujemy relację R następująco:

$$(x_1, y_1) R (x_2, y_2) \Leftrightarrow x_1 < x_2 \vee (x_1 = x_2 \wedge y_1 < y_2).$$

Wykaż, że relacja R jest porządkiem ostrym.

Pokaż, że dla dowolnych dwóch różnych elementów $u, v \in A$ zachodzi:

$$u R v \vee v R u.$$

Wyjaśnij, dlaczego relacja ta jest **porządkiem liniowym ostrym**.

Zadanie 2.10

Niech $A = \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$. Definiujemy relację:

$$A R B \Leftrightarrow \min A \leq \min B.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- Czy relacja R jest porządkiem częściowym? Uzasadnij.
- Czy każda niepusta rodzina zbiorów w A ma element minimalny względem R ?
- Porównaj relację R z inkluzją $\subseteq$. Czy któraś z nich jest „silniejsza”?

Pytania pomocnicze

- 1) Jakie warunki musi spełniać relacja, aby była relacją równoważności?
- 2) Na czym polega różnica między relacją antysymetryczną a asymetryczną?
- 3) Czym różni się porządek częściowy od porządku liniowego?
- 4) Czy każda relacja przechodnia jest relacją porządku? Uzasadnij odpowiedź.
- 5) Jak interpretować klasy abstrakcji relacji równoważności w sensie podziału zbioru?
- 6) Czy relacja podzielności na zbiorze liczb naturalnych jest porządkiem liniowym? Dlaczego?
- 7) Jakie znaczenie ma istnienie elementu najmniejszego w relacji porządku?

Podsumowanie

W trakcie ćwiczeń omówiono pojęcie relacji binarnej oraz przeanalizowano jej kluczowe własności. Przedstawiono relacje równoważności i porządku jako dwa fundamentalne typy relacji występujące w matematyce dyskretnej.

Studenci nauczyli się:

- formalnie badać własności relacji,
- konstruować klasy abstrakcji i zbiory ilorazowe,
- rozróżniać różne typy porządków,
- stosować aparat pojęciowy relacji w zadaniach problemowych.

Zdobyta wiedza stanowi podstawę do dalszych zagadnień z zakresu teorii zbiorów, algebry abstrakcyjnej, teorii grafów oraz informatyki teoretycznej.



Fundusze Europejskie
dla Rozwoju Społecznego



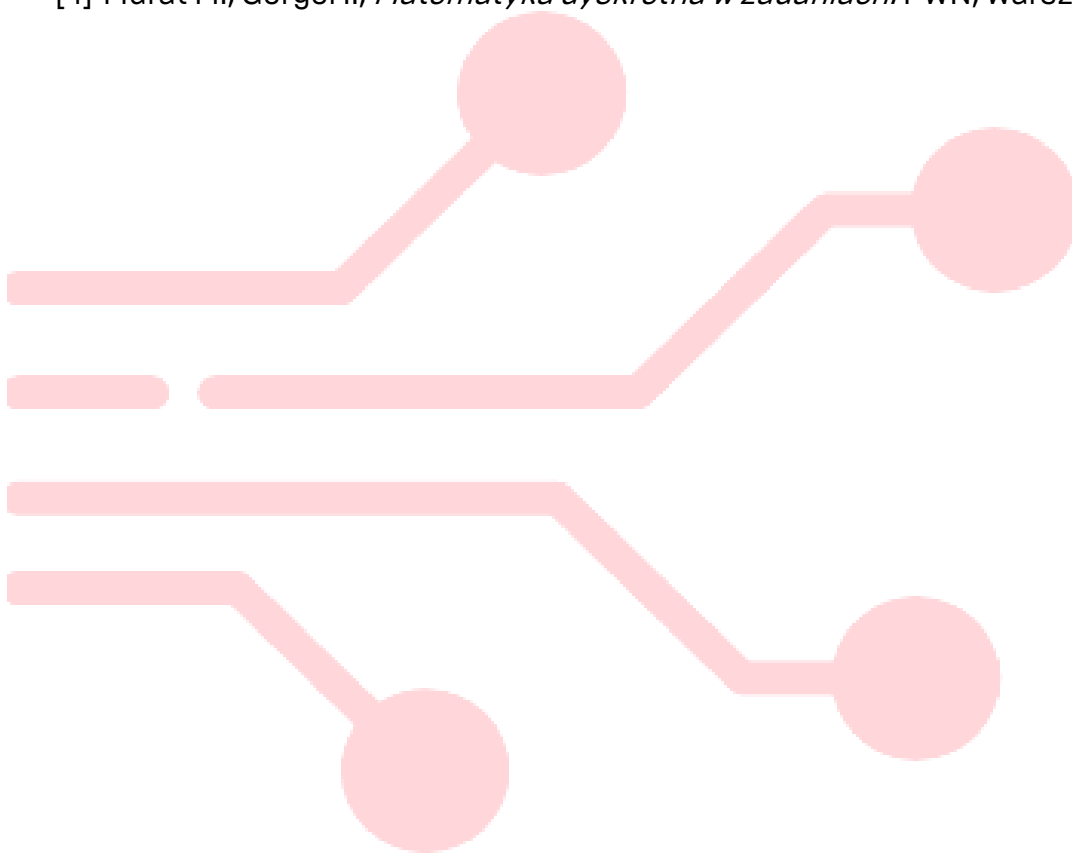
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 3

Badanie własności funkcji. Analiza złożoności algorytmów

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



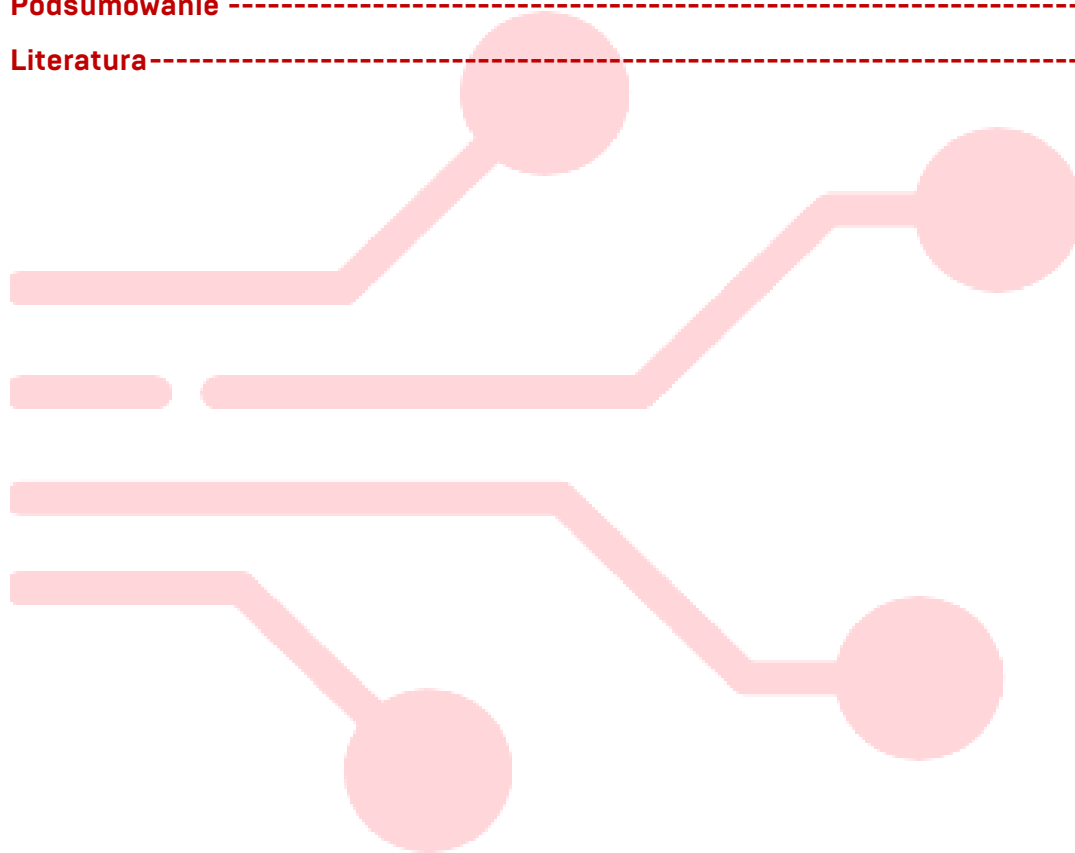
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	41
Cel ćwiczenia/laboratorium	43
Instrukcja laboratoryjna/ćwiczeniowa	44
Ćwiczenia samodzielne	47
Pytania pomocnicze	51
Podsumowanie	51
Literatura	51



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Relacja i funkcja

Niech A i B będą niepustymi zbiorami. Relację

$$R \subseteq A \times B$$

nazywamy funkcją „z A w B ”, jeżeli spełnione są jednocześnie następujące warunki:

- **Istnienie wartości funkcji**

Dla każdego elementu $x \in A$ istnieje element $y \in B$ taki, że $(x, y) \in R$.

- **Jednoznaczność wartości funkcji**

Dla każdego $x \in A$ oraz dla każdych $y_1, y_2 \in B$, jeżeli $(x, y_1) \in R$ oraz $(x, y_2) \in R$, to $y_1 = y_2$.

Jeżeli relacja R spełnia powyższe warunki, to zapisujemy:

$$f: A \rightarrow B$$

oraz zamiast $(x, y) \in R$ piszemy $f(x) = y$.

Zbiór A nazywamy **dziedziną funkcji**, a zbiór B **przeciwdziedziną funkcji**.

Obraz elementu i zbioru

Obraz elementu

Niech $f: A \rightarrow B$ będzie funkcją. Dla elementu $x \in A$ element $f(x) \in B$ nazywamy **obrazem elementu** x przez funkcję f .

Obraz zbioru

Niech $X \subseteq A$. **Obrazem zbioru** X przez funkcję f nazywamy zbiór:

$$f(X) = \{ y \in B : \text{istnieje } x \in X \text{ takie, że } y = f(x) \}.$$

Innymi słowy, element y należy do zbioru $f(X)$ wtedy i tylko wtedy, gdy jest wartością funkcji dla pewnego argumentu x należącego do X .

Przeciwwobraz zbioru

Niech $Y \subseteq B$. Przeciwwobrazem zbioru Y przez funkcję f nazywamy zbiór:

$$f^{-1}(Y) = \{ x \in A : f(x) \in Y \}.$$

Przeciwwobraz jest zawsze podzbiorem dziedziny funkcji.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zapis $f^{-1}(Y)$ nie oznacza funkcji odwrotnej, lecz zbiór argumentów, których obrazy należą do zbioru Y .

Iniekcja (funkcja różnowartościowa)

Funkcję $f: A \rightarrow B$ nazywamy iniekcją, jeżeli spełniony jest następujący warunek:

$$\text{dla każdych } x_1, x_2 \in A, \text{ jeżeli } f(x_1) = f(x_2), \text{ to } x_1 = x_2,$$

lub równoważnie

$$\forall x_1, x_2 \in A \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Oznacza to, że różne elementy dziedziny mają różne obrazy.

Suriekcja (funkcja „na”)

Funkcję $f: A \rightarrow B$ nazywamy **suriekcją** (surjekcją), jeżeli spełniony jest następujący warunek:

$$\text{dla każdego elementu } y \in B \text{ istnieje element } x \in A \text{ taki, że } f(x) = y,$$

lub równoważnie

$$\forall y \in B \quad \exists x \in A \quad f(x) = y$$

Innymi słowy, każdy element przeciwdziedziny jest obrazem pewnego elementu dziedziny.

Warunek ten można równoważnie zapisać w postaci:

$$f(A) = B.$$

Bijekcja

Funkcję $f: A \rightarrow B$ nazywamy **bijekcją**, jeżeli jest jednocześnie iniekcją i surjekcją. Oznacza to, że:

$$\text{dla każdego } y \in B \text{ istnieje dokładnie jeden element } x \in A, \text{ taki że } f(x) = y$$

lub równoważnie

$$\forall y \in B \quad \exists! x \in A \quad f(x) = y$$

Bijekcja wyznacza wzajemnie jednoznaczne przyporządkowanie pomiędzy zbiorami A i B .

Funkcja odwrotna

Jeżeli funkcja $f: A \rightarrow B$ jest bijekcją, to istnieje funkcja

$$f^{-1}: B \rightarrow A,$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



taka że:

- dla każdego $x \in A$ zachodzi $f^{-1}(f(x)) = x$,
- dla każdego $y \in B$ zachodzi $f(f^{-1}(y)) = y$.

Funkcja odwrotna istnieje wtedy i tylko wtedy, gdy funkcja jest bijekcją.

Składanie funkcji

Niech $f: A \rightarrow B$ oraz $g: B \rightarrow C$ będą funkcjami.

Złożeniem funkcji f i g nazywamy funkcję

$$g \circ f: A \rightarrow C$$

określoną w następujący sposób:

$$\text{dla każdego } x \in A \text{ zachodzi } (g \circ f)(x) = g(f(x)).$$

Składanie funkcji jest możliwe wtedy i tylko wtedy, gdy zbiór wartości funkcji f zawiera się w dziedzinie funkcji g .

Własności składania funkcji

- *Łączność*

Jeżeli $f: A \rightarrow B$, $g: B \rightarrow C$ oraz $h: C \rightarrow D$, to dla każdego $x \in A$:

$$h \circ (g \circ f)(x) = (h \circ g) \circ f(x).$$

- *Brak przemienności*

W ogólności nie zachodzi równość:

$$g \circ f \neq f \circ g.$$

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest utrwalenie podstawowych pojęć związanych z relacjami i funkcjami oraz ich własnościami. W szczególności student powinien:

- zrozumieć formalną definicję funkcji jako szczególnego przypadku relacji,
- umieć badać, czy dana relacja jest funkcją,
- rozróżniać oraz sprawdzać własności funkcji: różnowartościowość (iniekcję), „na” (surjekcję) oraz bijekcję,
- wyznaczać obrazy i przeciwobrazy zbiorów względem zadanej funkcji,



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- posługiwać się pojęciem funkcji odwrotnej i określać warunki jej istnienia,
- poprawnie stosować składanie funkcji i znać jego podstawowe własności,
- analizować funkcje z punktu widzenia wzrostu asymptotycznego oraz notacji O ,
- stosować indukcję matematyczną do dowodzenia własności funkcji i rekurencji.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 3.1

Niech $R \subseteq \mathbb{Z} \times \mathbb{Z}$ będzie relacją daną warunkiem

$$(x, y) \in R \Leftrightarrow y^2 = x.$$

Sprawdzić, czy relacja R jest funkcją z $\mathbb{Z}$ w $\mathbb{Z}$.

Rozwiązanie

Relacja R jest funkcją wtedy i tylko wtedy, gdy spełnione są dwa warunki:

- a) Dla każdego $x \in \mathbb{Z}$ istnieje takie $y \in \mathbb{Z}$, że $(x, y) \in R$.
- b) Dla każdego $x \in \mathbb{Z}$ oraz dla każdych $y_1, y_2 \in \mathbb{Z}$, jeżeli $(x, y_1) \in R$ oraz $(x, y_2) \in R$, to $y_1 = y_2$.

Rozważmy punkt $x = -1$. Nie istnieje taka liczba całkowita y , że $y^2 = -1$.

Oznacza to, że nieprawdą jest, iż dla każdego $x \in \mathbb{Z}$ istnieje $y \in \mathbb{Z}$ spełniające $(x, y) \in R$.

Zatem warunek istnienia nie jest spełniony.

Wniosek: Relacja R nie jest funkcją z $\mathbb{Z}$ w $\mathbb{Z}$.

Przykład 3.2

Niech $f: \mathbb{R} \rightarrow \mathbb{R}$ będzie dana wzorem

$$f(x) = 3x - 5.$$

Sprawdzić, czy funkcja f jest różnowartościową.

Rozwiązanie

Funkcja f jest różnowartościowa wtedy i tylko wtedy, gdy:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



dla dowolnych $x_1, x_2 \in \mathbb{R}$ jeżeli $f(x_1) = f(x_2)$, to $x_1 = x_2$.

Niech $x_1, x_2 \in \mathbb{R}$ i niech

$$f(x_1) = f(x_2).$$

Wówczas:

$$3x_1 - 5 = 3x_2 - 5,$$

co implikuje:

$$3x_1 = 3x_2,$$

a stąd:

$$x_1 = x_2.$$

Wniosek:

Funkcja f jest różnowartościowa.

Przykład 3.3

Niech $f: \mathbb{R} \rightarrow \mathbb{R}$ będzie dana wzorem

$$f(x) = x^2.$$

Sprawdzić, czy funkcja f jest „na”.

Rozwiązanie

Funkcja f jest surjekcją wtedy i tylko wtedy, gdy:

dla każdej liczby rzeczywistej y istnieje taka liczba rzeczywista x , że $f(x) = y$.

Zauważmy, że dla każdej liczby rzeczywistej x zachodzi nierówność:

$$x^2 \geq 0.$$

Zatem dla żadnej liczby ujemnej y nie istnieje $x \in \mathbb{R}$ takie, że $x^2 = y$.

W szczególności dla $y = -1$ nie istnieje $x \in \mathbb{R}$ spełniające $f(x) = y$.

Wniosek:

Funkcja f nie jest surjekcją na $\mathbb{R}$.

Przykład 3.4

Niech $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$. Wyznaczyć obraz zbioru $[-2, 1]$.

Rozwiązanie

Z definicji obrazu zbioru:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$f([-2,1]) = \{ y \in \mathbb{R}: \text{istnieje } x \in [-2,1] \text{ takie, że } y = f(x) \}.$$

Dla $x \in [-2,1]$ funkcja $f(x) = x^2$ przyjmuje wartości:

- minimalną równą 0 (dla $x = 0$),
- maksymalną równą 4 (dla $x = -2$).

Ponadto dla każdej wartości z przedziału $[0,4]$ istnieje $x \in [-2,1]$ takie, że $x^2 = y$.

Wniosek:

$$f([-2,1]) = [0,4].$$

Przykład 3.5

Niech $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2 - 1$. Wyznaczyć przeciwobraz zbioru $(-\infty, 0]$.

Rozwiązanie

Z definicji przeciwobrazu:

$$f^{-1}((-\infty, 0]) = \{ x \in \mathbb{R}: f(x) \leq 0 \}.$$

Rozwiązujemy nierówność:

$$x^2 - 1 \leq 0.$$

Jest ona równoważna:

$$x^2 \leq 1,$$

czyli:

$$-1 \leq x \leq 1.$$

Wniosek:

$$f^{-1}((-\infty, 0]) = [-1, 1].$$

Przykład 3.6

Niech

$$T(n) = \sum_{k=1}^n (2k + 1).$$

Wyznaczyć postać jawną oraz rząd wzrostu funkcji $T(n)$.

Rozwiązanie

Rozkładamy sumę na czynniki:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$T(n) = \sum_{k=1}^n 2k + \sum_{k=1}^n 1.$$

Dla każdego $n \in \mathbb{N}$ zachodzi:

$$\sum_{k=1}^n 2k = n(n+1), \quad \sum_{k=1}^n 1 = n.$$

Zatem:

$$T(n) = n(n+1) + n = n^2 + 2n.$$

Ponieważ dla każdego $n \geq 1$ zachodzi:

$$n^2 \leq n^2 + 2n \leq 3n^2,$$

istnieją dodatnie stałe c_1, c_2 oraz liczba n_0 , takie że:

$$c_1 n^2 \leq T(n) \leq c_2 n^2 \text{ dla każdego } n \geq n_0.$$

Wniosek:

$$T(n) \in \Theta(n^2).$$

Ćwiczenia samodzielne

Zadanie 3.1

Zbadać, czy relacja $R \subset \mathbb{R} \times \mathbb{R}$ określona wzorem $\langle x, y \rangle \in R \Leftrightarrow x^2 = y^2$ jest funkcją.

Zadanie 3.2

Zbadać, czy relacja $R \subset \mathbb{R}^+ \times \mathbb{R}^+$ określona wzorem $\langle x, y \rangle \in R \Leftrightarrow x^2 = y^2$ jest funkcją.

Zadanie 3.3

Zbadać, czy relacja $R \subset \mathbb{N} \times \mathbb{N}$ określona wzorem $\langle x, y \rangle \in R \Leftrightarrow x^2 = y^2$ jest funkcją.

Zadanie 3.4

Dla danego przekształcenia $f: \mathbb{R} \rightarrow \mathbb{R}$ zbadać, czy f jest odwzorowaniem różnowartościowym, czy jest „na”. Jeżeli nie jest „na” wyznaczyć Wf (zbiór wartości). Jeżeli nie jest różnowartościowe, wskazać $x_1, x_2 \in \mathbb{R}$ takie, że $x_1 \neq x_2$ ale $f(x_1) = f(x_2)$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- a) $f(x) = x^2$
- b) $f(x) = 3^x$
- c) $f(x) = x^3$
- d) $f(x) = \text{Ent}(x)$
- e) $f(x) = \begin{cases} \frac{2x+1}{x-1}, & x \neq 1 \\ 0, & x = 1 \end{cases}$
- f) $f(x) = \frac{2x}{x^2+1}$

Zadanie 3.4

Niech $f: \mathbb{R} \rightarrow \mathbb{R}$ będzie określone wzorem $f(x) = x^2 - 3x + 2$.

- a) Znaleźć obraz zbioru $< 0, 1 >$
- b) Znaleźć obraz zbioru $< -2, -1 >$
- c) Znaleźć obraz zbioru $\{1, 2\}$
- d) Znaleźć przeciwobraz zbioru $(-\infty, -6 >$
- e) Znaleźć przeciwobraz zbioru $(-3, 0 >$
- f) Znaleźć przeciwobraz zbioru $\{-4, -3\}$

Zadanie 3.5

Niech $f: \mathbb{R} \rightarrow \mathbb{R}$ będzie określone wzorem $f(x) = x^2 + 3x - 2$.

- a) Znaleźć obraz zbioru $< 0, 1 >$
- b) Znaleźć obraz zbioru $< -2, -1 >$
- c) Znaleźć obraz zbioru $\{1, 2\}$
- d) Znaleźć przeciwobraz zbioru $(-\infty, -6 >$
- e) Znaleźć przeciwobraz zbioru $(-3, 0 >$
- f) Znaleźć przeciwobraz zbioru $\{-4, -3\}$

Zadanie 3.6

Niech $\varphi: \mathbb{N}^2 \rightarrow \mathbb{N}$ będzie określone wzorem $\varphi(< n, k >) = n + k + 1$.

- a) Czy odwzorowanie φ jest „na”?
- b) Czy odwzorowanie φ jest różnowartościowe?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- c) Znaleźć obraz zbioru $\mathbb{N} \times \{2\}$
- d) Znaleźć przeciwobraz zbioru $\{3\}$
- e) Znaleźć przeciwobraz zbioru *Parzyste*

Zadanie 3.7

Niech dana będzie funkcja

$$T(n) = \sum_{k=1}^n (3k^2 + 5).$$

Wyznacz dokładną postać $T(n)$.

Ustal klasę wzrostu funkcji $T(n)$ w sensie notacji $O(\cdot)$

Zadanie 3.8

Dana jest funkcja:

$$T(n) = \sum_{k=1}^n \lfloor \sqrt{k} \rfloor.$$

Wykaż, że

$$T(n) \leq n\sqrt{n}.$$

oraz

$$T(n) \geq \frac{1}{2}n\sqrt{n} \text{ dla } n \geq 1.$$

Na podstawie powyższych oszacowań wyznacz klasę $\Theta(\cdot)$ funkcji $T(n)$.

Zadanie 3.9

Rozważ funkcję:

$$T(n) = \sum_{i=1}^n \sum_{j=1}^i (i+j).$$

Rozbij sumę na dwie składowe i uprość ją algebraicznie.

Wyznacz dokładny rząd wzrostu $T(n)$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 3.10

Dana jest rekurencja:

$$T(1) = 1,$$
$$T(n) = T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + n \text{ dla } n \geq 2.$$

Udowodnij indukcyjnie, że

$$T(n) \leq 2n \text{ dla każdego } n \geq 1.$$

Wykaż, że istnieje stała $c > 0$ taka, że

$$T(n) \geq cn \text{ dla nieskończenie wielu } n.$$

Określ rząd złożoności $\Theta(\cdot)$ funkcji $T(n)$.

Zadanie 3.11

Dane są funkcje:

$$f(n) = n \log n,$$

$$g(n) = \sum_{k=1}^n \log k,$$

$$h(n) = \log(n!).$$

Pokaż, że $g(n) = h(n)$.

Uzasadnij, że $f(n)$ i $h(n)$ należą do tej samej klasy wzrostu asymptotycznego.

Zadanie 3.12

Niech dane będą funkcje:

$$f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x + 1,$$

$$g: \mathbb{R} \rightarrow \mathbb{R}, g(x) = \frac{1}{x}.$$

- Wyznaczyć dziedzinę funkcji $g \circ f$.
- Wyznaczyć wzór funkcji $g \circ f$.
- Wyznaczyć dziedzinę funkcji $f \circ g$.
- Wyznaczyć wzór funkcji $f \circ g$.
- Sprawdzić, czy funkcje $g \circ f$ oraz $f \circ g$ są równe.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Pytania pomocnicze

- 1) Jakie warunki musi spełniać relacja, aby była funkcją?
- 2) Czym różni się obraz zbioru od przeciwobrazu zbioru?
- 3) Czy każda funkcja różnowartościowa ma funkcję odwrotną? Uzasadnij.
- 4) Podaj przykład funkcji, która jest:
 - różnowartościowa, ale nie jest „na”,
 - „na”, ale nie jest różnowartościowa.
- 5) Kiedy złożenie dwóch funkcji jest poprawnie określone?
- 6) Dlaczego składanie funkcji nie jest w ogólności przemienne?
- 7) Na czym polega badanie rzędu wzrostu funkcji i jakie ma znaczenie w analizie algorytmów?

Podsumowanie

W trakcie ćwiczeń omówiono pojęcie relacji i funkcji oraz ich kluczowe własności. Studenci przeanalizowali przykłady funkcji różnowartościowych, „na” oraz bijekcji, a także nauczyli się wyznaczać obrazy i przeciwobrazy zbiorów. Szczególną uwagę poświęcono funkcji odwrotnej oraz składaniu funkcji i jego własnościom.

W dalszej części zajęć wprowadzono pojęcia związane z analizą wzrostu funkcji oraz notacją O , które stanowią podstawę do oceny złożoności obliczeniowej algorytmów. Laboratorium przygotowuje do dalszych zagadnień matematyki dyskretnej, w szczególności do analizy algorytmów i struktur danych.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 4

Implementacja tabel prawdy i przekształcanie wyrażeń logicznych. Weryfikacja tautologii i kontrtautologii. Analiza tabel decyzyjnych i ich zastosowanie

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



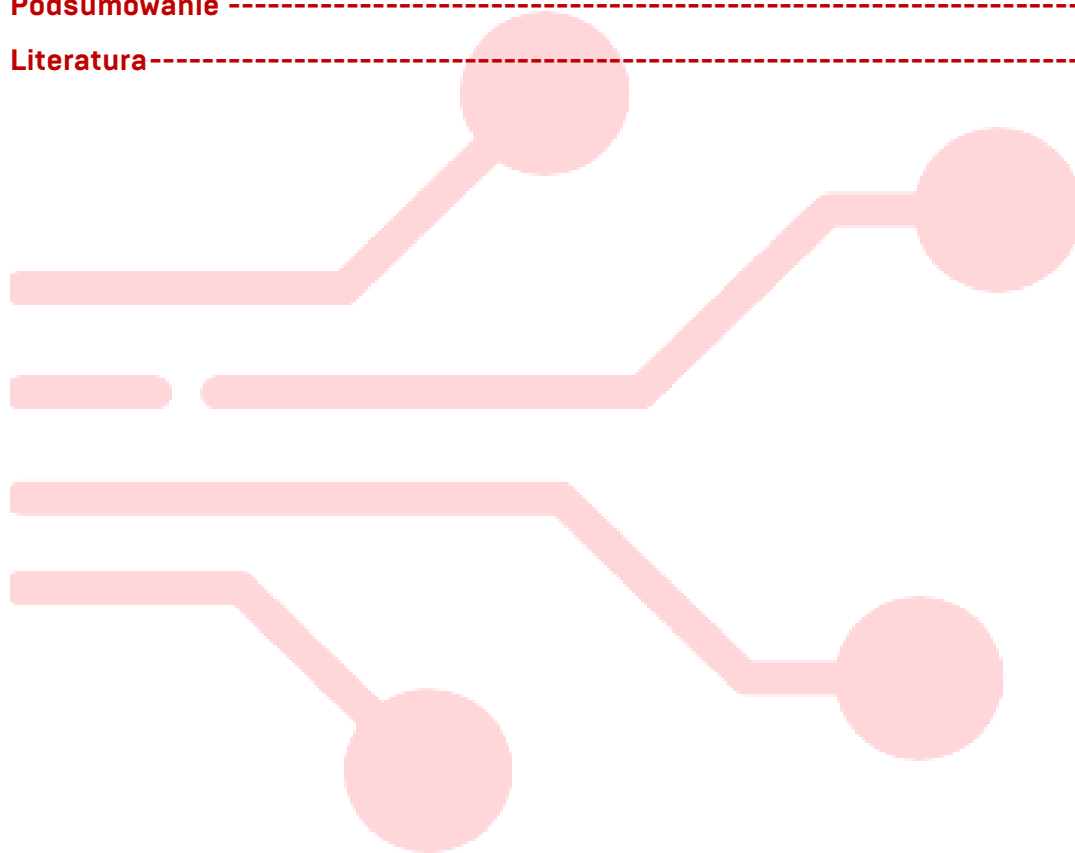
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	54
Cel ćwiczenia/laboratorium	57
Instrukcja laboratoryjna/ćwiczeniowa	57
Ćwiczenia samodzielne	62
Pytania pomocnicze	65
Podsumowanie	65
Literatura	65



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Zdania logiczne i wartości logiczne

Zdaniem logicznym nazywamy wypowiedź, której można jednoznacznie przypisać wartość logiczną:

- 1 (Prawda) lub
- 0 (Fałsz).

Zdaniami logicznymi nie są pytania, rozkazy ani wypowiedzi wieloznaczne.

Przykłady:

„ $2 + 2 = 4$ ” – zdanie logiczne (1),

„ $x > 3$ ” – nie jest zdaniem logicznym (zawiera zmienną wolną).

Spójniki logiczne i ich semantyka

Niech p, q, r będą zdaniami logicznymi. Definiujemy podstawowe spójniki:

Symbol	Nazwa	Znaczenie
$\neg p$ lub $\sim p$	negacja	„nie p ”
$p \wedge q$	koniunkcja	„ p i q ”
$p \vee q$	alternatywa	„ p lub q ”
$p \Rightarrow q$	implikacja	„jeżeli p , to q ”
$p \Leftrightarrow q$	równoważność	„ p wtedy i tylko wtedy, gdy q ”

Tabele prawdy

Tabela prawdy to formalny sposób opisu wartości logicznej wyrażenia złożonego dla wszystkich możliwych wartości logicznych jego zmiennych.

Dla n zmiennych tabela zawiera 2^n wierszy.

Przykład (koniunkcja):

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Tabele prawdy stanowią podstawowe narzędzie do:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- sprawdzania poprawności przekształceń,
- weryfikacji tautologii i sprzeczności,
- porównywania wyrażeń logicznych.

Tautologie, kontrtautologie i spełnialność

Tautologia – formuła logiczna, która przyjmuje wartość 1 dla każdego podstawienia zmiennych.

Kontrtautologia (sprzeczność) – formuła zawsze fałszywa.

Formuła spełnialna – istnieje co najmniej jedno podstawienie, dla którego ma wartość 1.

Przykłady

- a) $p \vee \sim p$ – tautologia,
- b) $p \wedge \sim p$ – kontrtautologia,
- c) $p \wedge q$ – formuła spełnialna, ale nie tautologia.

Równoważność logiczna

Formuły φ i ψ są równoważne logicznie, co zapisujemy:

$$\varphi \equiv \psi$$

jeżeli mają identyczne kolumny wartości w tabelach prawdy.

Równoważność logiczna oznacza, że formuły są nierozróżnialne semantycznie, nawet jeśli różnią się zapisem.

Podstawowe prawa algebry logicznej

- $\sim(\sim p) \equiv p$
- $p \wedge p \equiv p$
- $p \vee p \equiv p$
- $p \wedge \sim p \equiv 0$
- $p \vee \sim p \equiv 1$
- $p \vee (p \wedge q) \equiv p$
- $p \wedge (p \vee q) \equiv p$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Prawa de Morgana

Prawa de Morgana opisują zachowanie negacji względem koniunkcji i alternatywy:

$$\sim(p \wedge q) \equiv (\sim p \vee \sim q)$$

$$\sim(p \vee q) \equiv (\sim p \wedge \sim q)$$

Są one kluczowe w:

- przekształcaniu wyrażeń logicznych,
- upraszczaniu formuł,
- budowie postaci normalnych,
- analizie tabel decyzyjnych.

Uogólnienie:

$$\sim\left(\bigwedge_{i=1}^n p_i\right) \equiv \bigvee_{i=1}^n \sim p_i$$

$$\sim\left(\bigvee_{i=1}^n p_i\right) \equiv \bigwedge_{i=1}^n \sim p_i$$

Tabela decyzyjna to strukturalne przedstawienie:

- warunków logicznych (zmienne wejściowe),
- możliwych kombinacji ich wartości,
- decyzji lub działań wynikających z tych kombinacji.

Formalnie tabela decyzyjna odpowiada:

- tabeli prawdy formuły decyzyjnej,
- lub systemowi reguł typu „jeżeli-to”.

Zastosowania tabel decyzyjnych:

- specyfikacja algorytmów,
- analiza przypadków brzegowych,
- weryfikacja kompletności i niesprzeczności reguł,
- projektowanie systemów decyzyjnych i ekspertowych.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cel ćwiczenia/laboratorium

Celem ćwiczeń jest zapoznanie studentów z podstawami rachunku zdań oraz praktycznym wykorzystaniem narzędzi logiki matematycznej, w szczególności:

- pojęciem zdania logicznego i jego wartości logicznej,
- konstrukcją i analizą tabel prawdy,
- rozpoznawaniem tautologii, kontrtautologii oraz formuł spełnialnych,
- badaniem równoważności logicznej wyrażeń,
- stosowaniem podstawowych praw algebry Boole'a, w tym praw de Morgana,
- przekształcaniem formuł logicznych do równoważnych postaci,
- analizą i budową tabel decyzyjnych oraz wyprowadzaniem reguł decyzyjnych.

Ćwiczenie ma na celu rozwinięcie umiejętności formalnego rozumowania oraz przygotowanie do analizy logicznej algorytmów i systemów decyzyjnych.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 4.1

Sprawdź, czy formuła jest tautologią:

$$(p \Rightarrow q) \vee (q \Rightarrow p).$$

Rozwiązanie:

Budujemy tabelę prawdy:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	φ_1
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

Wniosek: formuła jest tautologią (ostatnia kolumna zawsze „T”).



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 4.2

Sprawdź, czy jest poniższe zdanie jest tautologią:

$$(p \wedge (p \Rightarrow q)) \Rightarrow q.$$

Rozwiązanie:

Tabela prawdy:

p	q	$p \Rightarrow q$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Wniosek: zdanie jest **tautologią**.

Przykład 4.3

Sprawdź, czy zdanie jest tautologią:

$$(p \vee q) \Rightarrow (p \wedge q).$$

Rozwiązanie:

Tabela:

p	q	$p \vee q$	$p \wedge q$	$(p \vee q) \Rightarrow (p \wedge q)$
T	T	T	T	T
T	F	T	F	F
F	T	T	F	F
F	F	F	F	T

Wniosek:

- zdanie nie jest tautologią (np. $p = T, q = F$ daje F),
- nie jest też sprzeczna (czasem jest T),
- więc jest spełnialna, ale nie zawsze prawdziwa.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 4.4

Sprawdź, czy formuła jest sprzeczna:

$$p \wedge \sim p.$$

Rozwiązanie:

Tabela:

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

Wniosek: $p \wedge \sim p$ jest sprzeczna (czyli kontrtautologia).

Przykład 4.5

Rozważ:

$$(p \vee q) \wedge (\sim p \vee \sim q).$$

Czy zdanie jest tautologią, kontrtautologią, czy jest spełnialne?

Rozwiązanie:

To jest klasyczny „XOR” (dokładnie jedno prawdziwe). Sprawdźmy tabelą:

p	q	$p \vee q$	$\sim p$	$\sim q$	$\sim p \vee \sim q$	$(p \vee q) \wedge (\sim p \vee \sim q)$
T	T	T	F	F	F	F
T	F	T	F	T	T	T
F	T	T	T	F	T	T
F	F	F	T	T	T	F

Wniosek: formuła jest spełnialna, ale nie tautologią i nie jest sprzeczna.

Przykład 4.6

Przekształć wyrażenie stosując prawa de Morgana:

$$\sim(p \vee (q \wedge r)).$$

Rozwiązanie:

Krok 1 [de Morgan]:

$$\sim(p \vee (q \wedge r)) \equiv (\sim p) \wedge \sim(q \wedge r).$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Krok 2 (de Morgan drugi raz):

$$\sim(q \wedge r) \equiv (\sim q) \vee (\sim r).$$

Zatem:

$$\sim(p \vee (q \wedge r)) \equiv (\sim p) \wedge ((\sim q) \vee (\sim r))$$

Kontrola tabelą (8 wierszy):

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$\sim(p \vee (q \wedge r))$	$\sim p$	$\sim q \vee \sim r$	$(\sim p) \wedge ((\sim q) \vee (\sim r))$
T	T	T	T	T	F	F	F	F
T	T	F	F	T	F	F	T	F
T	F	T	F	T	F	F	T	F
T	F	F	F	T	F	F	T	F
F	T	T	T	T	F	T	F	F
F	T	F	F	F	T	T	T	T
F	F	T	F	F	T	T	T	T
F	F	F	F	F	T	T	T	T

Kolumny $\sim(p \vee (q \wedge r))$ oraz $(\sim p) \wedge ((\sim q) \vee (\sim r))$ są identyczne, więc przekształcenie jest poprawne.

Przykład 4.7

Rozważmy tabelę decyzyjną zawierającą następujące zmienne logiczne:

- p – załogowany,
- q – admin,
- r – zasób dostępny,
- decyzja D – dostęp przyznany.

p	q	r	D
T	T	T	T
T	F	T	T
T	F	F	F
F	T	T	F
F	F	T	F



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Krok 1. Zapis w DNF (suma iloczynów) z wierszy gdzie $D = T$:

- wiersz 1: $p \wedge q \wedge r$
- wiersz 2: $p \wedge \sim q \wedge r$

Zatem:

$$D \equiv (p \wedge q \wedge r) \vee (p \wedge \sim q \wedge r).$$

Krok 2. Powyższą własność można uprościć

$$D \equiv p \wedge r \wedge (q \vee \sim q) \equiv p \wedge r.$$

Wniosek: dostęp jest przyznany wtedy i tylko wtedy, gdy zalogowany i zasób dostępny.

Przykład 4.8

Dana jest formuła:

$$\varphi := (p \vee q) \wedge (\sim q \vee r).$$

Sprawdź, czy jest tautologią.

Rozwiązanie:

Tabela prawdy (8 wierszy)

p	q	r	$p \vee q$	$\sim q$	$\sim q \vee r$	φ
T	T	T	T	F	T	T
T	T	F	T	F	F	F
T	F	T	T	T	T	T
T	F	F	T	T	T	T
F	T	T	T	F	T	T
F	T	F	T	F	F	F
F	F	T	F	T	T	F
F	F	F	F	T	T	F

Wniosek: formuła jest spełnialna, ale nie jest tautologią i nie jest sprzeczna.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Równoważna tabela decyzyjna (dla decyzji $D: = \varphi$)

p	q	r	D
T	T	T	T
T	T	F	F
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	F
F	F	T	F
F	F	F	F

Z tabeli można zauważyć, że:

- gdy $q = T$, to D zależy od r i trzeba mieć $p \vee q$ (czyli i tak prawda), więc $q = T \Rightarrow D \equiv r$,
- gdy $q = F$, to $\sim q = T$ więc drugi nawias zawsze prawdziwy, a zostaje $D \equiv p$.

Spostrzeżenia te można zapisać jako reguły:

- Jeżeli $q = F$, to $D = T$ wtedy i tylko wtedy, gdy $p = T$.
- Jeżeli $q = T$, to $D = T$ wtedy i tylko wtedy, gdy $r = T$.

Ćwiczenia samodzielne

Zadanie 4.1

Wykaż, że następujące wyrażenia są tautologiami:

- $p \Rightarrow p$,
- $p \Rightarrow (q \Rightarrow p)$,
- $p \Rightarrow (q \Rightarrow p \wedge q)$,
- $[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$,
- $p \vee \sim p$,



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- f) $p \Rightarrow (p \vee q)$,
g) $(p \wedge q \Rightarrow r) \Leftrightarrow [p \Rightarrow (q \Rightarrow r)]$,
h) $[p \vee (q \vee r)] \Leftrightarrow [(p \vee q) \vee r]$,
i) $[(p \Rightarrow q) \wedge p] \Rightarrow q$.

Zadanie 4.2

Sprawdzić, czy następujące wyrażenia są tautologiami:

- a) $[(p \vee q) \wedge \sim p \Rightarrow q]$,
b) $(p \Rightarrow q) \Rightarrow [(p \wedge r) \Rightarrow q]$,
c) $(p \Rightarrow q) \Rightarrow [p \Rightarrow (q \vee r)]$,
d) $p \vee [(\sim p \wedge q) \vee (\sim p \wedge \sim q)]$,
e) $p \Rightarrow [(\sim q \wedge q) \Rightarrow r]$.

Zadanie 4.3

Czy prawdziwe jest zdanie:

*„Jeżeli liczba naturalna **a** jest liczbą pierwszą, to o ile **a** jest liczbą złożoną, to **a** równa się 4.”*

Zadanie 4.4

Czy prawdziwe jest następujące zdanie:

*„Jeżeli figura **A** jest czworokątem i **A** ma wszystkie kąty równe, to z faktu, iż **A** jest czworokątem, wynika iż **A** ma boki równe.”*

Zadanie 4.5

Rozważ wyrażenie:

$$(p \wedge \sim p) \vee q$$

Czy wyrażenie jest:

- a) sprzeczne,
b) tautologią,
c) czy tylko spełnialne.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 4.6

Przekształć wyrażenie

$$\sim(p \vee q) \vee r$$

do postaci bez negacji złożonych stosując prawa de Morgana.

Zadanie 4.7

Dany jest system decyzyjny opisany zmiennymi logicznymi:

- p – użytkownik jest zalogowany
- q – użytkownik ma uprawnienia administratora
- r – zasób jest dostępny
- Decyzja D – dostęp przyznany

Tabela decyzyjna:

p	q	r	D
T	T	T	T
T	F	T	T
T	F	F	F
F	T	T	F
F	F	T	F

Zapisz decyzję D jako formułę logiczną.

Uprość otrzymaną formułę.

Zadanie 4.8

Dana jest formuła:

$$\varphi := (p \vee q) \wedge (\sim q \vee r)$$

Zbuduj tabelę prawdy dla φ .

Na jej podstawie skonstruuj równoważną tabelę decyzyjną.

Wskaż minimalny zbiór reguł decyzyjnych opisujących działanie formuły.

Oceń, czy φ jest tautologią, sprzecznością czy formułą spełnialną.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Pytania pomocnicze

- 1) Co odróżnia zdanie logiczne od wypowiedzi, której nie można przypisać wartości logicznej?
- 2) Ile wierszy zawiera tabela prawdy dla formuły z trzema zmiennymi logicznymi?
- 3) Jaka jest różnica między tautologią a formułą spełnialną?
- 4) Kiedy dwie formuły logiczne są równoważne?
- 5) Jakie znaczenie mają prawa de Morgana w upraszczaniu wyrażeń logicznych?
- 6) W jaki sposób tabela decyzyjna odpowiada tabeli prawdy formuły logicznej?
- 7) Dlaczego uproszczenie formuły decyzyjnej jest istotne w projektowaniu systemów decyzyjnych?

Podsumowanie

W trakcie ćwiczeń omówiono podstawowe pojęcia rachunku zdań oraz narzędzia umożliwiające formalną analizę wyrażeń logicznych. Studenci nauczyli się konstruować i interpretować tabele prawdy, rozpoznawać tautologie, sprzeczności i formuły spełnialne, a także badać równoważność logiczną formuł.

Szczególne uwagę poświęcono prawom de Morgana oraz ich zastosowaniu w przekształceniach logicznych. Przedstawiono również ideę tabel decyzyjnych jako praktycznego narzędzia opisu reguł decyzyjnych, wykorzystywanego m.in. w analizie algorytmów i systemach ekspertowych.

Zdobyte umiejętności stanowią podstawę do dalszego studiowania logiki matematycznej, teorii algorytmów oraz projektowania systemów informatycznych.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.



Fundusze Europejskie
dla Rozwoju Społecznego



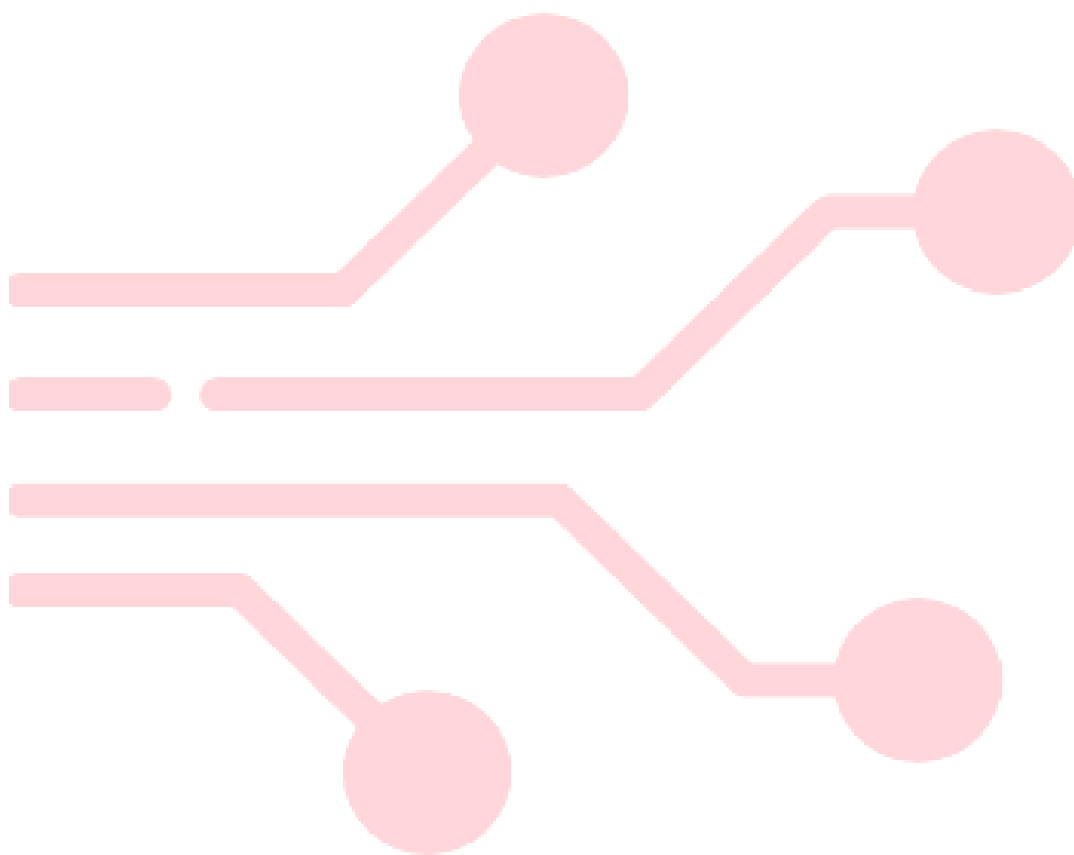
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



[3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.

[4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 5

Algorytmy generowania permutacji, kombinacji i wariacji. Implementacja i wizualizacja diagramów drzewkowych

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



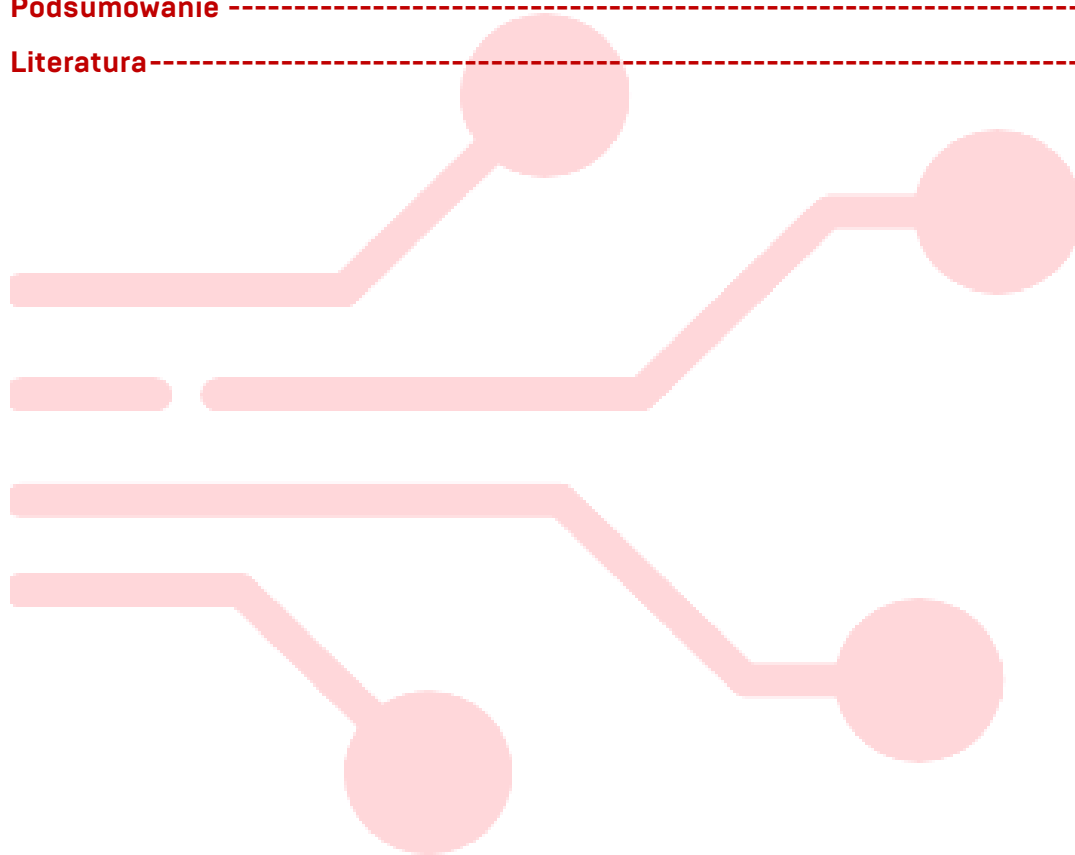
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	69
Cel ćwiczenia/laboratorium	70
Instrukcja laboratoryjna/ćwiczeniowa	70
Ćwiczenia samodzielne	76
Pytania pomocnicze	80
Podsumowanie	81
Literatura	81



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Permutacje

Niech A będzie zbiorem n -elementowym. Permutacją zbioru A nazywamy każde uporządkowanie wszystkich elementów zbioru A , w którym każdy element występuje dokładnie raz.

Liczba wszystkich permutacji n -elementowego zbioru dana jest wzorem

$$P(n) = n!.$$

Na pierwszym miejscu można wybrać dowolny z n elementów, na drugim dowolny z pozostałych $n - 1$, itd., aż do ostatniego miejsca, na którym pozostaje jeden element. Z zasady mnożenia otrzymujemy

$$n \cdot (n - 1) \cdot (n - 2) \cdots 1 = n!$$

Wariacje bez powtórzeń

Niech A będzie zbiorem n -elementowym, a $k \leq n$. Wariacją k -elementową bez powtórzeń zbioru A nazywamy uporządkowany ciąg k różnych elementów zbioru A .

Liczba wariacji k -elementowych bez powtórzeń dana jest wzorem

$$V(n, k) = P(n, k) = \frac{n!}{(n - k)!}.$$

Wariacje z powtórzeniami

Niech A będzie zbiorem n -elementowym. Wariacją k -elementową z powtórzeniami zbioru A nazywamy uporządkowany ciąg długości k , w którym każdy element pochodzi ze zbioru A i może się powtarzać.

Liczba takich wariacji dana jest wzorem

$$V'(n, k) = n^k.$$

Kombinacje bez powtórzeń

Niech A będzie zbiorem n -elementowym, a $k \leq n$. Kombinacją k -elementową zbioru A nazywamy k -elementowy podzbiór zbioru A , w którym kolejność elementów nie ma znaczenia.

Liczba kombinacji k -elementowych dana jest wzorem

$$\binom{n}{k} = \frac{n!}{k! (n - k)!}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Kombinacje z powtórzeniami

Niech A będzie zbiorem n -elementowym. Kombinacją k -elementową z powtórzeniami nazywamy wybór k elementów ze zbioru A , przy czym kolejność nie ma znaczenia, a elementy mogą się powtarzać.

Liczba takich kombinacji dana jest wzorem

$$\binom{n+k-1}{k}.$$

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest zapoznanie studentów z podstawowymi pojęciami kombinatoryki oraz rozwinięcie umiejętności ich praktycznego zastosowania, w szczególności:

- pojęciem permutacji, wariacji i kombinacji (z powtórzeniami oraz bez powtórzeń),
- metodami obliczania liczby struktur kombinatorycznych,
- projektowaniem algorytmów generujących struktury kombinatoryczne,
- analizą działania algorytmów generujących,
- interpretowaniem algorytmów generujących jako przeszukiwania drzew decyzyjnych.

Ćwiczenia mają na celu rozwinięcie umiejętności algorytmicznego i kombinatorycznego myślenia oraz przygotowanie do dalszych zagadnień matematyki dyskretnej i informatyki.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 5.1

Dany jest zbiór

$$A = \{a, b, c, d, e\}.$$

Obliczyć liczbę wszystkich permutacji zbioru A .

Rozwiązanie



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Liczba wszystkich permutacji n -elementowego zbioru dana jest wzorem

$$P(n) = n!$$

W rozpatrywanym przypadku zbiór A ma $n = 5$ elementów, zatem

$$P(5) = 5! = 120.$$

Liczba wszystkich permutacji zbioru A wynosi 120.

Przykład 5.2

Dany jest zbiór

$$B = \{1, 2, 3, 4, 5, 6\}.$$

Obliczyć liczbę permutacji 3-elementowych zbioru B .

Rozwiązanie

Liczba permutacji k -elementowych zbioru n -elementowego (czyli wariacji bez powtórzeń) dana jest wzorem

$$P(n, k) = \frac{n!}{(n - k)!}.$$

Dla $n = 6$ oraz $k = 3$ otrzymujemy

$$P(6, 3) = \frac{6!}{3!} = \frac{720}{6} = 120.$$

Zatem liczba permutacji 3-elementowych zbioru B wynosi 120.

Przykład 5.3

Dany jest zbiór

$$C = \{x, y, z, u, v\}.$$

Obliczyć liczbę wszystkich kombinacji 3-elementowych zbioru C .

Rozwiązanie

Liczba kombinacji k -elementowych zbioru n -elementowego dana jest wzorem



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$\binom{n}{k} = \frac{n!}{k! (n-k)!}$$

W rozpatrywanym przypadku $n = 5$ oraz $k = 3$, więc

$$\binom{5}{3} = \frac{5!}{3! 2!} = \frac{120}{12} = 10.$$

Zbiór C ma dokładnie 10 kombinacji 3-elementowych.

Przykład 5.4

Dany jest zbiór

$$D = \{a, b, c, d\}.$$

Obliczyć liczbę wariacji 5-elementowych z powtórzeniami.

Rozwiązanie

Liczba wariacji k -elementowych z powtórzeniami zbioru n -elementowego dana jest wzorem

$$V'(n, k) = n^k.$$

Dla $n = 4$ oraz $k = 5$ otrzymujemy

$$V'(4, 5) = 4^5 = 1024.$$

Liczba wszystkich wariacji 5-elementowych z powtórzeniami wynosi 1024.

Przykład 5.4

Dany jest zbiór

$$E = \{1, 2, 3, 4, 5, 6, 7\}.$$

Oblicz liczbę 4-elementowych podzbiorów zbioru E .

Rozwiązanie

Liczba k -elementowych podzbiorów zbioru n -elementowego dana jest wzorem

$$\binom{n}{k}.$$

Dla $n = 7$ oraz $k = 4$ mamy

$$\binom{7}{4} = \frac{7!}{4! 3!} = \frac{5040}{144} = 35.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zatem zbiór E ma 35 podzbiorów 4-elementowych.

Przykład 5.5

Dany jest zbiór $A = \{a, b, c\}$. Wygenerować wszystkie permutacje.

Permutacje zbioru S budujemy wybierając element $x \in S$ jako pierwszy, a następnie doklejając do niego każdą permutację zbioru $S \setminus \{x\}$.

Przypadek bazowy: $|S| = 0$ (zwracamy permutację pustą) albo $|S| = 1$ (zwracamy pojedynczy element).

Pseudokod.

```
PERMUTACJE(S):  
  jeśli S jest puste:  
    wypisz []  
    zakończ  
  
  dla każdego x w S:  
    T := S \ {x}  
    dla każdej p z PERMUTACJE_LISTA(T):  
      wypisz [x] + p  
  
PERMUTACJE_LISTA(S):  
  jeśli S puste: zwróć listę zawierającą tylko []  
  wynik := []  
  dla każdego x w S:  
    T := S \ {x}  
    dla każdej p w PERMUTACJE_LISTA(T):  
      dołącz ([x] + p) do wynik  
  zwróć wynik
```

Przykład działania dla $\{a, b, c\}$.

Wyniki (kolejność zgodna z wyborem pierwszego elementu w pętli):

$(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$.

Przykład 5.6

Dany jest zbiór $B = \{1, 2, 3, 4, 5\}$. Wygenerować wszystkie kombinacje 3-elementowe w porządku leksykograficznym (rosnąco).



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Trzymamy częściową kombinację X oraz parametr start mówiący, od którego indeksu wolno dalej wybierać, aby zachować porządek rosnący i nie generować duplikatów.

Pseudokod.

```
KOMB(S[1..n], k):  
  X := pusta lista  
  GEN(start=1)  
  
GEN(start):  
  jeśli |X| = k:  
    wypisz X  
    zakończ  
  
  dla i od start do n - (k - |X|) + 1:  
    dołącz S[i] do X  
    GEN(i+1)  
    usuń ostatni element z X
```

Przykład działania dla $S = (1,2,3,4,5)$, $k = 3$.

Kolejne wypisywane kombinacje:

$(1,2,3), (1,2,4), (1,2,5), (1,3,4), (1,3,5), (1,4,5), (2,3,4), (2,3,5), (2,4,5), (3,4,5)$.

Przykład 5.7

Dany jest zbiór $C = \{x, y, z\}$. Wygenerować wszystkie wariacje 4-elementowe z powtórzeniami.

Budujemy słowo pozycyjnie: na każdej pozycji mamy dowolny wybór z C . To jest klasyczne przeszukiwanie drzewa o rozgałęzieniu $|C|$ i głębokości k .

Pseudokod.

```
WARIACJE_Z_POWT(S[1..n], k):  
  X[1..k] := tablica  
  GEN(pos=1)  
  
GEN(pos):  
  jeśli pos = k+1:  
    wypisz (X[1], ..., X[k])  
    zakończ  
  dla i od 1 do n:  
    X[pos] := S[i]  
    GEN(pos+1)
```



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład działania [pierwsze 10 wyników dla $S = (x, y, z)$, $k = 4$].

$(x, x, x, x), (x, x, x, y), (x, x, x, z), (x, x, y, x), (x, x, y, y),$
 $(x, x, y, z), (x, x, z, x), (x, x, z, y), (x, x, z, z), (x, y, x, x), \dots$

Przykład 5.8

Dany jest zbiór $D = \{a, b, c, d, e\}$. Wygenerować wszystkie permutacje 3-elementowe [czyli wariacje bez powtórzeń].

Budujemy wynik X długości k . Na każdym kroku wybieramy element jeszcze nieużyty. Używamy tablicy $used[i]$.

Pseudokod.

```
K_PERM(S[1..n], k):
    used[1..n] := fałsz
    X := pusta lista
    GEN()

GEN():
    jeśli |X| = k:
        wypisz X
        zakończ
    dla i od 1 do n:
        jeśli used[i] = fałsz:
            used[i] := prawda
            dołącz S[i] do X
            GEN()
            usuń ostatni element z X
            used[i] := fałsz
```

Przykład działania [dla $S = (a, b, c, d, e)$, $k = 3$, pierwszych 12 wyników].

$(a, b, c), (a, b, d), (a, b, e), (a, c, b), (a, c, d), (a, c, e), (a, d, b), (a, d, c),$
 $(a, d, e), (a, e, b), (a, e, c), (a, e, d), \dots$

Należy zauważyć, że łącznie będzie $\frac{5!}{(5-3)!} = 60$ wyników.

Przykład 5.9

Dany jest zbiór $E = \{p, q, r, s\}$. Wygenerować wszystkie podzbiory.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Każdemu podzbiorowi odpowiada wektor bitów długości n : bit 1 oznacza „element należy”, bit 0 – „nie należy”. Przechodzimy przez wszystkie liczby od 0 do $2^n - 1$.

Pseudokod.

```

PODZBIORY(S[1..n]):
  dla mask od 0 do 2^n - 1:
    T := pusty zbiór
    dla i od 1 do n:
      jeśli (mask >> (i-1)) & 1 = 1:
        dodaj S[i] do T
    wypisz T
  
```

Przykład działania dla $S = (p, q, r, s)$.

Kolejne maski i zbiory:

0000 $\rightarrow \emptyset$

0001 $\rightarrow \{p\}$

0010 $\rightarrow \{q\}$

0011 $\rightarrow \{p, q\}$

0100 $\rightarrow \{r\}$

...

1111 $\rightarrow \{p, q, r, s\}$

Ćwiczenia samodzielne

Zadanie 5.1

Dany jest zbiór

$$A = \{a, b, c, d, e, f, g\}.$$

Oblicz liczbę wszystkich permutacji zbioru A .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 5.2

Dany jest zbiór

$$B = \{1, 2, 3, 4, 5, 6\}.$$

Oblicz liczbę permutacji 4-elementowych zbioru B .

Zadanie 5.3

Dany jest zbiór

$$C = \{x, y, z, u, v\}.$$

Oblicz liczbę wszystkich kombinacji 3-elementowych zbioru C .

Zadanie 5.4

Dany jest zbiór

$$D = \{a, b, c, d, e, f\}.$$

Oblicz liczbę kombinacji 2-elementowych oraz 4-elementowych tego zbioru i porównaj otrzymane wyniki.

Zadanie 5.5

Dany jest zbiór

$$E = \{0, 1, 2, 3, 4\}.$$

Oblicz liczbę wariacji 3-elementowych bez powtórzeń, w których pierwszym elementem nie jest zero.

Zadanie 5.6

Dany jest zbiór

$$F = \{a, b, c, d\}.$$

Oblicz liczbę wszystkich wariacji 5-elementowych z powtórzeniami.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 5.7

Dany jest zbiór

$$G = \{a, b, c, d, e\}.$$

Ile różnych słów długości 4 można utworzyć z elementów zbioru G , jeżeli litera a nie może występować więcej niż jeden raz?

Zadanie 5.8

Dany jest zbiór

$$H = \{1, 2, 3, 4, 5, 6, 7\}.$$

Oblicz liczbę wszystkich 3-elementowych podzbiorów zbioru H , które zawierają liczbę 1.

Zadanie 5.9

Dany jest zbiór

$$I = \{a, b, c, d, e, f\}.$$

Oblicz liczbę permutacji zbioru I , w których element a nie znajduje się na pierwszej pozycji.

Zadanie 5.10

Dany jest zbiór

$$J = \{x, y, z\}.$$

Ile różnych słów długości 6 można utworzyć z elementów zbioru J , jeżeli każdy element musi wystąpić co najmniej raz?

Zadanie 5.11

Dany jest zbiór

$$K = \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Oblicz liczbę wszystkich 4-elementowych kombinacji zbioru K , w których nie występują jednocześnie liczby 1 i 2.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 5.12

Dany jest zbiór

$$L = \{a, b, c, d, e\}.$$

Oblicz liczbę wszystkich permutacji zbioru L , w których elementy a oraz b nie występują obok siebie.

Zadanie 5.13

Dany jest zbiór

$$M = \{a, b, c, d\}.$$

Zaprojektuj algorytm rekurencyjny generujący wszystkie permutacje zbioru M . Opisz przypadek bazowy, krok rekurencyjny oraz kolejność generowania wyników.

Zadanie 5.14

Dany jest zbiór

$$N = \{1, 2, 3, 4, 5\}.$$

Zaprojektuj algorytm generowania wszystkich kombinacji 3-elementowych zbioru N w porządku leksykograficznym.

Zadanie 5.15

Dany jest zbiór

$$P = \{x, y, z\}.$$

Zaprojektuj algorytm generowania wszystkich wariacji 4-elementowych z powtórzeniami. Przedstaw strukturę drzewa generowania.

Zadanie 5.16

Dany jest zbiór

$$R = \{a, b, c, d, e\}.$$

Zaprojektuj algorytm typu backtracking generujący wszystkie permutacje 3-elementowe zbioru R bez powtórzeń.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 5.17

Dany jest zbiór

$$S = \{1, 2, 3, 4\}.$$

Zaprojektuj algorytm iteracyjny generujący wszystkie kombinacje 2-elementowe zbioru S . Opisz sposób przechodzenia do następnej kombinacji.

Zadanie 5.18

Dany jest zbiór

$$T = \{a, b, c\}.$$

Zaprojektuj algorytm generowania wszystkich słów długości 5 z elementów zbioru T . Zinterpretuj algorytm jako przeszukiwanie drzewa decyzyjnego.

Zadanie 5.19

Dany jest zbiór

$$U = \{1, 2, 3, 4, 5\}.$$

Zaprojektuj algorytm generowania wszystkich kombinacji zbioru U (wszystkich podzbiorów), wykorzystując reprezentację binarną.

Zadanie 5.20

Dany jest zbiór

$$W = \{a, b, c, d\}.$$

Zaprojektuj algorytm generowania wszystkich permutacji zbioru W , w którym każda kolejna permutacja różni się od poprzedniej możliwie najmniejszą zmianą.

Pytania pomocnicze

- 1) Jaka jest różnica pomiędzy permutacją a wariacją bez powtórzeń?
- 2) W jakich sytuacjach stosujemy kombinacje z powtórzeniami zamiast kombinacji bez powtórzeń?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- 3) Dlaczego liczba wariacji z powtórzeniami zbioru -elementowego równa się n^k ?
- 4) Na czym polega metoda backtracking i dlaczego jest ona wygodna przy generowaniu permutacji?
- 5) W jaki sposób algorytm generowania podzbiorów można powiązać z reprezentacją binarną liczb naturalnych?
- 6) Jakie są zalety i wady algorytmów rekurencyjnych w porównaniu z algorytmami iteracyjnymi?

Podsumowanie

W trakcie ćwiczeń omówiono podstawowe zagadnienia kombinatoryki oraz przedstawiono metody obliczania liczby permutacji, wariacji i kombinacji. Zdobyta wiedza stanowi podstawę do dalszego studiowania algorytmów dyskretnych oraz analizy ich złożoności obliczeniowej.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 6

Implementacja i analiza algorytmów rekurencyjnych

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	84
Cel ćwiczenia/laboratorium	86
Instrukcja laboratoryjna/ćwiczeniowa	87
Ćwiczenia samodzielne	91
Pytania pomocnicze	95
Podsumowanie	95
Literatura	96



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt współfinansowany ze środków Unii Europejskiej w ramach: FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS) "POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Wprowadzenie, tematyka zajęć

Definicja ciągu rekurencyjnego

Ciągiem rekurencyjnym nazywamy ciąg $(a_n)_{n \geq 0}$, którego wyrazy są określone za pomocą zależności rekurencyjnej postaci:

$$a_n = F(n, a_{n-1}, a_{n-2}, \dots, a_{n-k}),$$

gdzie:

- F jest daną funkcją,
- $k \in \mathbb{N}$ oznacza rząd rekurencji,
- podane są odpowiednie warunki początkowe $a_0, a_1, \dots, a_{k-1}$.

Rekurencje liniowe pierwszego rzędu

Rekurencję liniową pierwszego rzędu nazywamy zależność postaci:

$$a_{n+1} = \alpha a_n + \beta,$$

gdzie $\alpha, \beta \in \mathbb{R}$.

Przypadek jednorodny ($\beta = 0$)

$$a_{n+1} = \alpha a_n$$

Rozwiązaniem jest ciąg geometryczny:

$$a_n = a_0 \alpha^n.$$

Przypadek niejednorodny ($\beta \neq 0$)

$$a_{n+1} = \alpha a_n + \beta$$

Jeżeli $\alpha \neq 1$, to wzór jawny ma postać:

$$a_n = \left(a_0 + \frac{\beta}{\alpha - 1}\right) \alpha^n - \frac{\beta}{\alpha - 1}.$$

Alternatywnie stosuje się podstawienie pomocnicze:

$$b_n = a_n + C,$$

gdzie stała C jest dobrana tak, aby zredukować rekurencję do postaci jednorodnej.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Rekurencje liniowe drugiego rzędu (jednorodne)

Rekurencją liniową drugiego rzędu nazywamy zależność:

$$a_n = pa_{n-1} + qa_{n-2},$$

gdzie $p, q \in \mathbb{R}$.

Rekurencji odpowiada następujące równanie charakterystyczne:

$$r^2 - pr - q = 0.$$

W zależności od pierwiastków równania charakterystycznego otrzymujemy następujące wzory na postać ogólną:

Dwa różne pierwiastki rzeczywiste $r_1 \neq r_2$:

$$a_n = C_1 r_1^n + C_2 r_2^n.$$

Pierwiastek podwójny r :

$$a_n = (C_1 + C_2 n) r^n.$$

Stałe C_1, C_2 wyznacza się z warunków początkowych.

Rekurencje niejednorodne typu sumacyjnego

Jeżeli rekurencja ma postać:

$$a_n = a_{n-1} + f(n),$$

to rozwiązanie można zapisać jako sumę:

$$a_n = a_0 + \sum_{k=1}^n f(k).$$

W szczególności:

$$\sum_{k=1}^n k = \frac{n(n+1)}{2}, \quad \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Rekurencje z częścią całkowitą i interpretacja algorytmiczna

Rekurencje postaci:

$$a_n = a_{\lfloor n/2 \rfloor} + c$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



opisują procesy iteracyjne, w których argument zmniejsza się przez dzielenie przez 2.

Liczba iteracji potrzebnych do osiągnięcia wartości początkowej jest równa:

$$\lfloor \log_2 n \rfloor + 1.$$

Stąd:

$$a_n = a_0 + c(\lfloor \log_2 n \rfloor + 1).$$

Własności pomocnicze

- Ciąg (a_n) jest rosnący, jeżeli $a_{n+1} \geq a_n$ dla każdego n .
- Ciąg (a_n) jest malejący, jeżeli $a_{n+1} \leq a_n$ dla każdego n .
- Ciąg (a_n) jest geometryczny, jeżeli $a_{n+1} = qa_n$.
- Ciąg (a_n) jest arytmetyczny, jeżeli $a_{n+1} = a_n + r$.

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest:

- nabycie umiejętności rozwiązywania prostych i średnio zaawansowanych rekurencji,
- wyznaczanie wzorów jawnych ciągów rekurencyjnych,
- rozumienie związku między postacią rekurencji a własnościami ciągu,
- przygotowanie studentów do samodzielnej analizy rekurencji pojawiających się w zadaniach algorytmicznych.

Po zakończeniu ćwiczenia student potrafi dobrać odpowiednią metodę rozwiązania rekurencji oraz poprawnie zinterpretować otrzymany wynik.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Instrukcja laboratoryjna/ćwiczeniowa

Przykład 6.1

Dany jest ciąg określony rekurencyjnie:

$$a_0 = 3,$$
$$a_{n+1} = a_n + 2 \text{ dla } n > 0.$$

Wyznacz wzór jawny ciągu a_n .

Rozwiązanie.

Rekurencja opisuje ciąg arytmetyczny o różnicy 2.

Obliczmy kilka pierwszych wyrazów:

$$a_0 = 3, a_1 = 5, a_2 = 7, a_3 = 9.$$

Łatwo zauważyć, że:

$$a_n = 3 + 2n.$$

Przykład 6.2

Dany jest ciąg:

$$a_0 = 1,$$
$$a_{n+1} = 3a_n, \text{ dla } n > 0$$

Wyznacz jego wzór jawny.

Rozwiązanie.

Obliczamy początkowe wyrazy ciągu:

$$a_0 = 1, a_1 = 3, a_2 = 9, a_3 = 27.$$

Jest to ciąg geometryczny o ilorazie 3, zatem wzór jawny ma postać:

$$a_n = 3^n.$$

Przykład 6.3

Dany jest ciąg:

$$a_0 = 0,$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$a_{n+1} = a_n + 3, \text{ dla } n > 0$$

Wyznacz wzór jawny.

Rozwiązanie.

Jest to ciąg arytmetyczny o różnicy 3:

$$a_1 = 3, a_2 = 6, a_3 = 9.$$

Zatem:

$$a_n = 3n.$$

Przykład 6.4

Dany jest ciąg:

$$a_0 = 2,$$

$$a_{n+1} = 2a_n, \text{ dla } n > 0$$

Wyznacz wzór jawny.

Rozwiązanie.

Wypisujemy kolejne wyrazy ciągu

$$a_1 = 4, a_2 = 8, a_3 = 16.$$

Zauważamy, że są to potęgi liczby 2:

$$a_n = 2^{n+1}.$$

Przykład 6.5

Rozwiąż rekurencję:

$$a_0 = 1,$$

$$a_{n+1} = 2a_n + 1, \text{ dla } n > 0$$

Rozwiązanie.

Najpierw zgadujemy postać rozwiązania szczególnego. Szukamy stałej A , takiej że:

$$A = 2A + 1 \Rightarrow A = -1.$$

Definiujemy:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$b_n = a_n + 1.$$

Wtedy:

$$b_{n+1} = 2b_n,$$

$$b_0 = 2.$$

Zatem:

$$b_n = 2^{n+1},$$

$$a_n = 2^{n+1} - 1.$$

Przykład 6.6

Dany jest ciąg:

$$a_0 = 0, a_1 = 1,$$

$$a_n = a_{n-1} + a_{n-2}, \text{ dla } n > 1$$

Podaj pierwsze wyrazy ciągu.

Rozwiązanie.

Obliczamy kolejne wyrazy:

$$a_2 = 1, a_3 = 2, a_4 = 3, a_5 = 5, a_6 = 8.$$

Jest to klasyczny ciąg Fibonacciego.

Przykład 6.7

Rozwiąż rekurencję:

$$a_0 = 1, a_1 = 2,$$

$$a_n = 3a_{n-1} - 2a_{n-2}.$$

Rozwiązanie.

Równanie charakterystyczne powyższego równania ma postać:

$$r^2 - 3r + 2 = 0.$$

Rozkład tego równania wynosi:

$$(r - 1)(r - 2) = 0 \Rightarrow r_1 = 1, r_2 = 2.$$

Postać ogólna ciągu:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$a_n = C_1 \cdot 1^n + C_2 \cdot 2^n.$$

Uwzględniamy warunki początkowe:

$$\begin{cases} C_1 + C_2 = 1, \\ C_1 + 2C_2 = 2. \end{cases}$$

Stąd $C_2 = 1$, $C_1 = 0$, więc:

$$a_n = 2^n.$$

Przykład 6.8

Rozwiąż rekurencję:

$$\begin{aligned} a_0 &= 1, a_1 = 2, \\ a_n &= 2a_{n-1} - a_{n-2}, \text{ dla } n > 1 \end{aligned}$$

Rozwiązanie.

Równanie charakterystyczne ma postać:

$$r^2 - 2r + 1 = 0 \Rightarrow (r - 1)^2 = 0.$$

Zatem postać ogólna rozwiązania dana jest wzorem:

$$a_n = (C_1 + C_2 n) \cdot 1^n = C_1 + C_2 n.$$

Warunki początkowe:

$$\begin{cases} C_1 = 1, \\ C_1 + C_2 = 2. \end{cases}$$

Stąd $C_2 = 1$, zatem wzór ogólny ma postać:

$$a_n = 1 + n.$$

Przykład 6.9

Rozwiąż rekurencję:

$$a_n = a_{n-1} + n, a_0 = 0.$$

Rozwiązanie.

Wypisujemy pierwsze wyrazy ciągu:

$$a_1 = 1, a_2 = 3, a_3 = 6, a_4 = 10.$$

Zauważamy, że są to sumy kolejnych liczb naturalnych, zatem



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$a_n = 1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

Przykład 6.10

Dana jest rekurencja:

$$a_0 = 1, a_n = a_{\lfloor n/2 \rfloor} + 1 \text{ dla } n \geq 1.$$

Znajdź interpretację i wzór tej rekurencji.

Rozwiązanie.

Rekurencja zmniejsza argument przez dzielenie przez 2. Liczba kroków potrzebnych do zejścia do zera to liczba bitów w zapisie binarnym n .

Zatem:

$$a_n = \lfloor \log_2 n \rfloor + 1.$$

Ćwiczenia samodzielne

Zadanie 6.1.

Dany jest ciąg:

$$a_0 = 5,$$

$$a_{n+1} = a_n + 4, \text{ dla } n > 0$$

Wyznacz wzór jawny ciągu a_n .

Zadanie 6.2.

Dany jest ciąg:

$$a_0 = 2,$$

$$a_{n+1} = 5a_n, \text{ dla } n > 0$$

Podaj wzór jawny oraz oblicz a_4 .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 6.3.

Dany jest ciąg:

$$a_1 = 7,$$

$$a_{n+1} = a_n - 3, \text{ dla } n > 0$$

Wyznacz wzór jawny oraz sprawdź, czy ciąg jest monotoniczny.

Zadanie 6.4.

Rozwiąż rekurencję:

$$a_0 = 1,$$

$$a_{n+1} = 2a_n + 2, \text{ dla } n > 0$$

Zadanie 6.5.

Dany jest ciąg:

$$a_0 = 0,$$

$$a_{n+1} = a_n + 2n + 1, \text{ dla } n > 0$$

Wyznacz wzór jawny ciągu.

Zadanie 6.6.

Rozwiąż rekurencję:

$$a_0 = 3,$$

$$a_{n+1} = 3a_n - 6, \text{ dla } n > 0$$

Zadanie 6.7.

Dany jest ciąg:

$$a_0 = 1,$$

$$a_{n+1} = 4a_n + 3, \text{ dla } n > 0$$

Wyznacz wzór jawny metodą podstawienia pomocniczego.

Zadanie 6.8.

Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Dany jest ciąg:

$$a_0 = 10,$$
$$a_{n+1} = \frac{1}{2}a_n, \text{ dla } n > 0$$

Wyznacz wzór jawny i granicę ciągu.

Zadanie 6.9.

Dany jest ciąg:

$$a_0 = 1, a_1 = 1,$$
$$a_n = a_{n-1} + a_{n-2}, \text{ dla } n > 1$$

Oblicz pierwsze 8 wyrazów ciągu.

Zadanie 6.10.

Rozwiąż rekurencję:

$$a_0 = 1, a_1 = 3,$$
$$a_n = 2a_{n-1} - a_{n-2}, \text{ dla } n > 1$$

Zadanie 6.11.

Dany jest ciąg:

$$a_0 = 2, a_1 = 5,$$
$$a_n = 3a_{n-1} - 2a_{n-2}, \text{ dla } n > 1$$

Wyznacz wzór jawny tego ciągu

Zadanie 6.12.

Rozwiąż rekurencję:

$$a_0 = 0, a_1 = 1,$$
$$a_n = 4a_{n-1} - 4a_{n-2}, \text{ dla } n > 0$$

Zadanie 6.13.

Dany jest ciąg:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$a_0 = 1, a_1 = 3,$$

$$a_n = 2a_{n-1} - a_{n-2}, \text{ dla } n > 1$$

Wyznacz wzór jawny ciągu a_n .

Zadanie 6.14.

Rozwiąż rekurencję:

$$a_0 = 2, a_1 = 4, a_2 = 6$$

$$a_n = a_{n-1} + a_{n-2} - a_{n-3}, \text{ dla } n > 2$$

Zadanie 6.15.

Dany jest ciąg:

$$a_0 = 0,$$

$$a_n = a_{n-1} + n^2, \text{ dla } n > 0$$

Wyznacz wzór jawny.

Zadanie 6.16.

Rozwiąż rekurencję:

$$a_1 = 2,$$

$$a_n = a_{n-1} + 3n - 2, \text{ dla } n > 0$$

Zadanie 6.17.

Dany jest ciąg:

$$a_0 = 1,$$

$$a_n = a_{\lfloor n/2 \rfloor} + 2, \text{ dla } n > 0$$

Znajdź wzór w zależności od n .

Zadanie 6.18.

Dany jest ciąg:

$$a_1 = 0,$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$a_n = a_{n-1} + \lfloor \log_2 n \rfloor, \text{ dla } n > 0$$

Zinterpretuj znaczenie ciągu i opisz jego monotoniczność.

Zadanie 6.19.

Rozwiąż rekurencję:

$$a_1 = 1, a_n = 2a_{\lfloor n/2 \rfloor}.$$

Zadanie 6.20.

Dany jest ciąg:

$$a_0 = 0,$$

$$a_n = a_{n-1} + (-1)^n, \text{ dla } n > 0$$

Wyznacz wzór jawny tego ciągu.

Pytania pomocnicze

- 1) Jaka jest różnica między rekurencją liniową jednorodną a niejednorodną?
- 2) Kiedy rekurencję można rozwiązać metodą iteracji, a kiedy należy użyć równania charakterystycznego?
- 3) Jaką postać ma rozwiązanie rekurencji drugiego rzędu z podwójnym pierwiastkiem?
- 4) W jaki sposób interpretować rekurencje zawierające funkcję $\lfloor n/2 \rfloor$?
- 5) Jakie znaczenie mają warunki początkowe dla jednoznaczności rozwiązania rekurencji?

Podsumowanie

W trakcie ćwiczeń studenci poznali podstawowe techniki rozwiązywania rekurencji i wyznaczania wzorów jawnych ciągów. Omówione przykłady i zadania pozwalają zrozumieć, w jaki sposób rekurencje opisują procesy iteracyjne oraz algorytmiczne.

Umiejętność pracy z rekurencjami jest kluczowa w dalszych zagadnieniach matematyki dyskretnej, w szczególności w analizie algorytmów oraz struktur danych.



Fundusze Europejskie
dla Rozwoju Społecznego



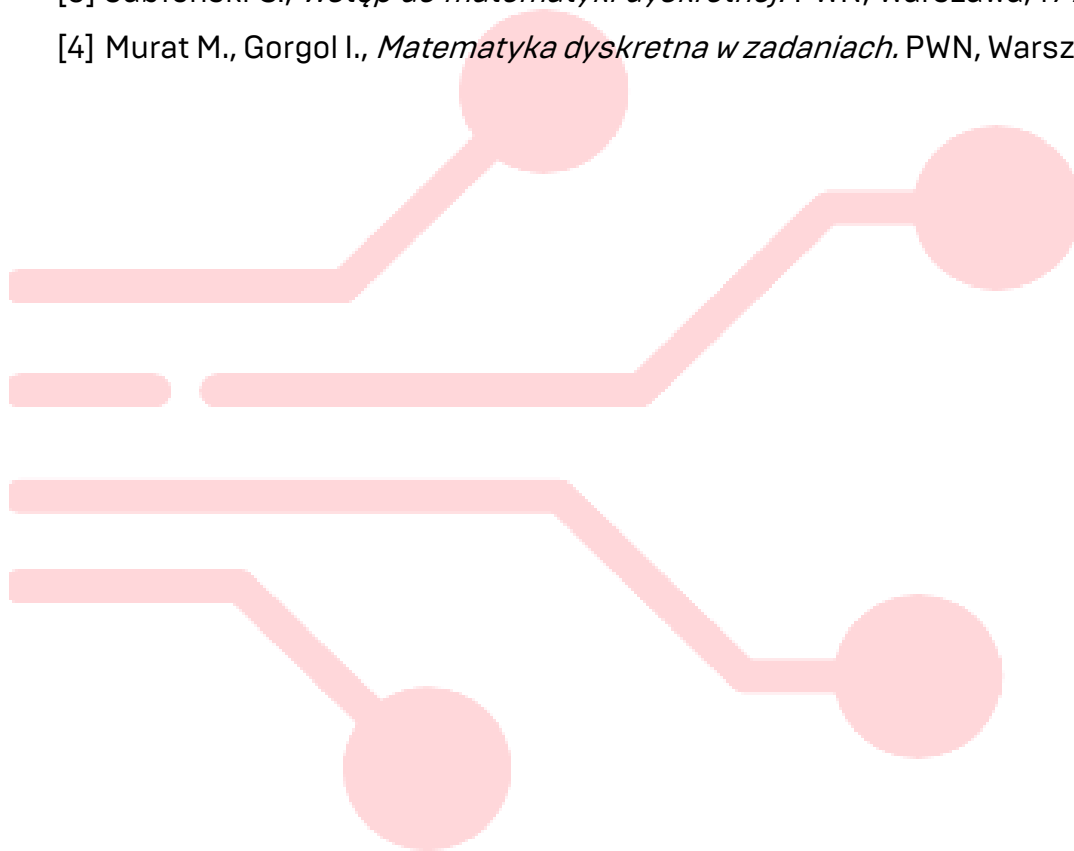
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 7

Prawdopodobieństwo klasyczne i geometryczne, prawdopodobieństwo warunkowe i całkowite. Dyskretne zmienne losowe. Zastosowanie prawa wielkich liczb

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



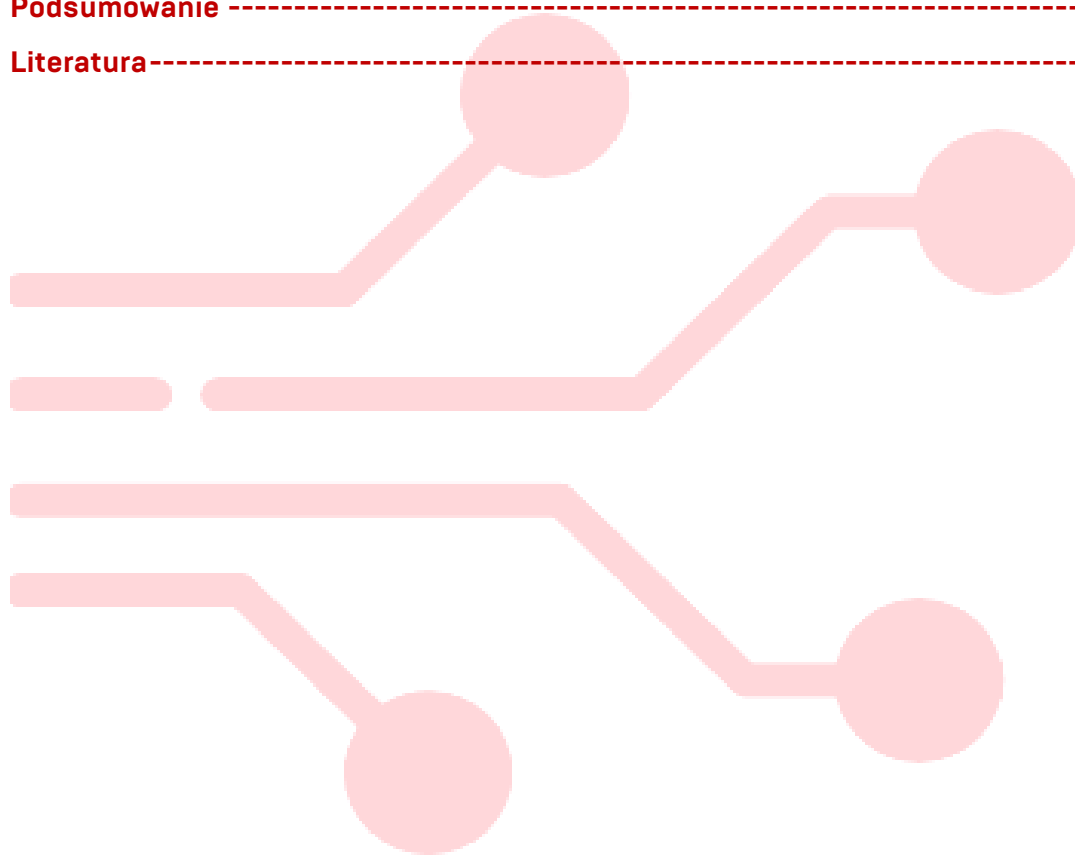
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć -----	99
Cel ćwiczenia/laboratorium -----	102
Instrukcja laboratoryjna/ćwiczeniowa -----	103
Ćwiczenia samodzielne -----	110
Pytania pomocnicze -----	116
Podsumowanie -----	117
Literatura -----	117



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Przestrzeń probabilistyczna i prawdopodobieństwo klasyczne

Przestrzeń probabilistyczną opisujemy przez trójkę

$$(\Omega, \mathcal{F}, P),$$

gdzie:

Ω – zbiór wszystkich możliwych wyników (przestrzeń prób),

$\mathcal{F} \subseteq 2^\Omega$ – σ – ciało,

$P: \mathcal{F} \rightarrow [0,1]$ – miara probabilistyczna.

Prawdopodobieństwo klasyczne

Jeżeli Ω jest skończona i wszystkie wyniki są jednakowo prawdopodobne, to dla zdarzenia $A \subseteq \Omega$:

$$P(A) = \frac{|A|}{|\Omega|}.$$

Własności prawdopodobieństwa, w ujęciu klasycznym.

Dla dowolnych zdarzeń A, B zachodzą następujące własności:

$$P(\Omega) = 1, P(\emptyset) = 0,$$

$$P(A^c) = 1 - P(A),$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Prawdopodobieństwo geometryczne

Jeżeli przestrzeń prób Ω jest obszarem geometrycznym (np. odcinek, prostokąt, koło), a punkt losowane są jednorodnie, to:

$$P(A) = \frac{\mu(A)}{\mu(\Omega)}.$$

Prawdopodobieństwo warunkowe

Dla zdarzeń A, B takich, że $P(B) > 0$, prawdopodobieństwo warunkowe zdarzenia A pod warunkiem zajścia B definiujemy jako:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$P(A | B) = \frac{P(A \cap B)}{P(B)}.$$

Niezależność zdarzeń

Zdarzenia A, B są niezależne, gdy:

$$P(A \cap B) = P(A)P(B),$$

równoważnie:

$$P(A | B) = P(A).$$

Prawo całkowite prawdopodobieństwa

Jeżeli zdarzenia $B_1, B_2, \dots, B_n$ tworzą rozbięcie przestrzeni:

$$B_i \cap B_j = \emptyset \ (i \neq j), \bigcup_{i=1}^n B_i = \Omega,$$

to dla dowolnego zdarzenia A zachodzi:

$$P(A) = \sum_{i=1}^n P(A | B_i) P(B_i).$$

Prawo to stosujemy m.in. gdy:

- losujemy maszynę, a potem produkt,
- wybieramy zestaw egzaminacyjny,
- losujemy hurtownię, a potem wyrób.

Wzór Bayesa

Jeżeli $B_1, \dots, B_n$ jest rozbięciem Ω oraz $P(A) > 0$, to:

$$P(B_k | A) = \frac{P(A | B_k) P(B_k)}{\sum_{i=1}^n P(A | B_i) P(B_i)}.$$

Wzór Bayesa pozwala:

- odwrócić warunek,
- obliczyć prawdopodobieństwo przyczyny przy znanym skutku.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zmienna losowa dyskretna

Zmienna losowa X jest dyskretna, jeżeli przyjmuje co najwyżej przeliczalnie wiele wartości:

$$X: \Omega \rightarrow \{x_1, x_2, \dots\}.$$

Rozkład zmiennej losowej określony jest przez funkcję:

$$P(X = x_k) = p_k,$$

która posiada następujące własności:

$$p_k \geq 0, \sum_k p_k = 1.$$

Wartość oczekiwana i wariancja

Wartość oczekiwana

$$E(X) = \sum_k x_k P(X = x_k).$$

Drugi moment

$$E(X^2) = \sum_k x_k^2 P(X = x_k).$$

Wariancja

$$\text{Var}(X) = E(X^2) - [E(X)]^2.$$

Własności wartości oczekiwanej i wariancji:

$$\begin{aligned} E(aX + b) &= aE(X) + b, \\ \text{Var}(aX + b) &= a^2 \text{Var}(X). \end{aligned}$$

Transformacja zmiennej losowej

Jeżeli $Y = g(X)$, to:

- wyznaczamy wszystkie możliwe wartości Y ,
- sumujemy prawdopodobieństwa tych wartości X , które dają to samo Y .

W szczególności:

$$E(g(X)) = \sum g(x_k) P(X = x_k).$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ciągi zmiennych losowych i prawo wielkich liczb

Niech $X_1, X_2, \dots$ będą niezależnymi zmiennymi losowymi o tym samym rozkładzie (i.i.d.), takimi że:

$$E(X_i) = \mu, \text{Var}(X_i) = \sigma^2 < \infty.$$

Definiujemy średnią:

$$\bar{X}_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

Dla tak zdefiniowanej średniej mamy:

$$E(\bar{X}_n) = \mu, \text{Var}(\bar{X}_n) = \frac{\sigma^2}{n}.$$

Prawo wielkich liczb (słaba wersja)

Dla każdego $\varepsilon > 0$:

$$P(|\bar{X}_n - \mu| > \varepsilon) \xrightarrow{n \rightarrow \infty} 0.$$

Interpretacja: średnia z dużej liczby obserwacji stabilizuje się wokół wartości oczekiwanej.

Nierówność Czebyszewa

Dla dowolnej zmiennej losowej X o skończonej wariancji:

$$P(|X - E(X)| \geq \varepsilon) \leq \frac{\text{Var}(X)}{\varepsilon^2}.$$

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest zapoznanie studentów z podstawowymi pojęciami rachunku prawdopodobieństwa oraz rozwinięcie umiejętności ich praktycznego zastosowania, w szczególności:

- pojęciem przestrzeni probabilistycznej,
- pojęciem prawdopodobieństwa klasycznego, geometrycznego oraz warunkowego,
- pojęciem niezależności zdarzeń losowych,



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- stosowaniem prawa całkowitego prawdopodobieństwa oraz wzoru Bayesa,
- rozwiązywaniem typowych zadań probabilistycznych,
- pojęciem dyskretnej zmiennej losowej i jej rozkładu,
- obliczaniem wartości oczekiwanej i wariancji,
- transformacjami zmiennych losowych,
- zastosowaniem prawa wielkich liczb oraz nierówności Czebyszewa w analizie zachowania ciągów zmiennych losowych.

Ćwiczenia mają na celu rozwinięcie umiejętności probabilistycznego i analitycznego myślenia oraz przygotowanie do dalszych zagadnień matematyki i informatyki.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 7.1

Rzucamy dwiema uczciwymi kostkami. Niech S oznacza sumę oczek.

- Oblicz $P(S = 9)$.
- Oblicz $P(\min \{X_1, X_2\} \geq 4)$.

Rozwiązanie:

- Przestrzeń ma 36 równoprawdopodobnych wyników (i, j) .
Suma 9 zachodzi dla: $(3,6), (4,5), (5,4), (6,3)$ – 4 przypadki. Zatem

$$P(S = 9) = \frac{4}{36} = \frac{1}{9}.$$

- Warunek $\min \geq 4$ oznacza: obie kostki mają wyniki należące do zbioru $\{4,5,6\}$
Moc tego zbioru wynosi $3 \cdot 3 = 9$. Zatem

$$P(\min \geq 4) = \frac{9}{36} = \frac{1}{4}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 7.2

W urnie jest 7 kul białych i 5 czarnych. Losujemy 4 kule bez zwracania. Niech

X – liczba wylosowanych kul białych.

a) Oblicz $P(X = 3)$.

b) Oblicz $P(X \geq 1)$.

Rozwiązanie:

a) To rozkład hipergeometryczny:

$$P(X = 3) = \frac{\binom{7}{3} \binom{5}{1}}{\binom{12}{4}} = \frac{35 \cdot 5}{495} = \frac{175}{495} = \frac{35}{99}.$$

b) Prawdopodobieństwo to najprościej jest obliczyć poprzez zastosowanie wzoru na dopełnienie:

$$P(X \geq 1) = 1 - P(X = 0) = 1 - \frac{\binom{7}{0} \binom{5}{4}}{\binom{12}{4}} = 1 - \frac{1 \cdot 5}{495} = 1 - \frac{1}{99} = \frac{98}{99}.$$

Przykład 7.3

Punkt (X, Y) losujemy jednorodnie z kwadratu $[0, 2] \times [0, 2]$. Losowanie jednorodne oznacza, że każdy element ma jednakowe szanse wylosowania. Oblicz:

$$P(X + Y \leq 2).$$

Rozwiązanie:

Skorzystamy ze wzoru na prawdopodobieństwo geometryczne. Musimy zatem obliczyć pole całej przestrzeni oraz pole ograniczone przez zadany warunek.

Pole całego kwadratu wynosi 4. Nierówność $x + y \leq 2$ w tym kwadracie wycina trójkąt prostokątny o przyprostokątnych długości 2 oraz 2, więc pole:

$$P(\text{obszaru}) = \frac{1}{2} \cdot 2 \cdot 2 = 2.$$

Zatem:

$$P(X + Y \leq 2) = \frac{2}{4} = \frac{1}{2}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 7.4

Losujemy niezależnie $X, Y \sim U(0,1)$. Oblicz:

$$P(Y \leq X^2).$$

Rozwiązanie:

W kwadracie jednostkowym $(x, y) \in [0,1]^2$ obszar $y \leq x^2$ ma pole:

$$\int_0^1 x^2 dx = \left[\frac{x^3}{3} \right]_0^1 = \frac{1}{3}.$$

Zatem:

$$P(Y \leq X^2) = \frac{1}{3}.$$

Przykład 7.5

W urnie jest 5 białych i 3 czarne. Losujemy 2 kule bez zwracania. Oblicz $P(\text{pierwsza biała} \mid \text{druga czarna})$.

Rozwiązanie:

Niech A : „pierwsza biała”, B : „druga czarna”.

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}.$$

Liczymy:

$$P(A \cap B) = P(1. \text{ biała}) \cdot P(2. \text{ czarna} \mid 1. \text{ biała}) = \frac{5}{8} \cdot \frac{3}{7} = \frac{15}{56}.$$

$$P(B) = P(2. \text{ czarna}) = \frac{3}{8}$$

Stąd

$$P(A \mid B) = \frac{\frac{15}{56}}{\frac{3}{8}} = \frac{15}{56} \cdot \frac{8}{3} = \frac{120}{168} = \frac{5}{7}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 7.6

Z talii 52 kart losujemy 2 karty bez zwracania.

Oblicz:

$$P(\text{obie piki} \mid \text{pierwsza pik}).$$

Rozwiązanie:

Jeśli pierwsza jest piką, w talii zostaje 51 kart, z czego pików 12.

$$P(\text{obie piki} \mid \text{pierwsza pika}) = P(\text{druga pika} \mid \text{pierwsza pika}) = \frac{12}{51} = \frac{4}{17}.$$

Przykład 7.7

Trzy maszyny: M_1, M_2, M_3 produkują odpowiednio 50%, 30%, 20% elementów. Odsetek wadliwych elementów produkowanych przez poszczególne maszyny wynosi: $P(W \mid M_1) = 0.01$, $P(W \mid M_2) = 0.02$, $P(W \mid M_3) = 0.05$. Oblicz $P(W)$.

Rozwiązanie:

Prawdopodobieństwo całkowite:

$$P(W) = \sum_{i=1}^3 P(W \mid M_i)P(M_i) = 0.01 \cdot 0.5 + 0.02 \cdot 0.3 + 0.05 \cdot 0.2.$$

$$P(W) = 0.005 + 0.006 + 0.01 = 0.021.$$

Przykład 7.8

Student wybiera zestaw: A, B, C z prawdopodobieństwem 0.4, 0.4, 0.2 odpowiednio. Zdawalność egzaminu dla poszczególnych zestawów wynosi:

$$P(Z \mid A) = 0.9, P(Z \mid B) = 0.7, P(Z \mid C) = 0.5.$$

Oblicz $P(Z)$ oraz $P(\bar{Z})$.

Rozwiązanie:

$$P(Z) = 0.9 \cdot 0.4 + 0.7 \cdot 0.4 + 0.5 \cdot 0.2 = 0.36 + 0.28 + 0.10 = 0.74.$$

$$P(\bar{Z}) = 1 - P(Z) = 1 - 0.74 = 0.26.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 7.9

Hurtownie: H_1, H_2, H_3 mają następujące udziały w rynku 0.5, 0.3, 0.2. Odsetek wadliwych elementów w poszczególnych hurtowniach wynosi: $P(W | H_1) = 0.01$, $P(W | H_2) = 0.02$, $P(W | H_3) = 0.06$. Oblicz $P(H_3 | W)$.

Rozwiązanie:

Najpierw obliczamy prawdopodobieństwo całkowite.

$$P(W) = 0.01 \cdot 0.5 + 0.02 \cdot 0.3 + 0.06 \cdot 0.2 = 0.005 + 0.006 + 0.012 = 0.023.$$

Następnie korzystamy ze wzoru Bayes'a:

$$P(H_3 | W) = \frac{P(W | H_3)P(H_3)}{P(W)} = \frac{0.06 \cdot 0.2}{0.023} = \frac{0.012}{0.023} \approx 0.5217.$$

Przykład 7.10

Choroba wystąpienia choroby wynosi $P(C) = 0.02$. Test ma czułość $P(+ | C) = 0.95$ oraz swoistość $P(- | \bar{C}) = 0.97$, więc $P(+ | \bar{C}) = 0.03$. Oblicz $P(C | +)$.

Rozwiązanie:

Korzystamy jak poprzednio z prawdopodobieństwa całkowitego i wzoru Bayes'a.

$$P(+)=P(+|C)P(C)+P(+|\bar{C})P(\bar{C})=0.95\cdot0.02+0.03\cdot0.98=0.019+0.0294=0.0484.$$

$$P(C|+)=\frac{0.95\cdot0.02}{0.0484}=\frac{0.019}{0.0484}\approx0.3926.$$

Przykład 7.11

Zmienna $X \in \{0, 1, 2, 3\}$ ma rozkład określony wzorem

$$P(X = k) = c(k + 1), k = 0, 1, 2, 3.$$

a) Wyznacz stałą c .

$$\sum_{k=0}^3 c(k+1) = c(1+2+3+4) = 10c = 1 \Rightarrow c = \frac{1}{10}.$$

b) Wyznacz rozkład zmiennej losowej X

$$P(0) = \frac{1}{10}, P(1) = \frac{2}{10}, P(2) = \frac{3}{10}, P(3) = \frac{4}{10}.$$

c) Oblicz wartość oczekiwaną $E(X)$:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$E(X) = \sum kP(X = k) = 0 \cdot \frac{1}{10} + 1 \cdot \frac{2}{10} + 2 \cdot \frac{3}{10} + 3 \cdot \frac{4}{10} = \frac{2 + 6 + 12}{10} = 2.$$

d) Oblicz drugi moment $E(X^2)$:

$$E(X^2) = 0^2 \cdot \frac{1}{10} + 1^2 \cdot \frac{2}{10} + 2^2 \cdot \frac{3}{10} + 3^2 \cdot \frac{4}{10} = \frac{2 + 12 + 36}{10} = 5$$

e) Oblicz wariancję

$$\text{Var}(X) = E(X^2) - [E(X)]^2 = 5 - 2^2 = 1.$$

Przykład 7.12

Dana jest zmienna losowa X o rozkładzie:

$$P(X = -1) = 0.3, P(X = 0) = 0.4, P(X = 2) = 0.3.$$

Niech $Y = X^2$.

a) Wyznaczyć rozkład zmiennej losowej Y .

b) Obliczyć wartość oczekiwaną zmiennej losowej Y

Rozwiązanie:

a) Zmienna losowa Y może przyjmować następujące wartości:

$$Y = 0 \Leftrightarrow X = 0 \Rightarrow P(Y = 0) = 0.4$$

$$Y = 1 \Leftrightarrow X = -1 \Rightarrow P(Y = 1) = 0.3$$

$$Y = 4 \Leftrightarrow X = 2 \Rightarrow P(Y = 4) = 0.3$$

b) Wartość oczekiwana wynosi:

$$E(Y) = 0 \cdot 0.4 + 1 \cdot 0.3 + 4 \cdot 0.3 = 0 + 0.3 + 1.2 = 1.5.$$

Przykład 7.13

Niech $X_1, X_2, \dots, i.i.d.$, (czyli ciąg niezależnych zmiennych losowych o identycznych rozkładach) takim, że $E(X_i) = 10, \text{Var}(X_i) = 9$.

$$\bar{X}_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

Dobierz n , tak by $P(|\bar{X}_n - 10| \geq 0.5) \leq 0.04$.

Rozwiązanie:

$$E(\bar{X}_n) = 10, \text{Var}(\bar{X}_n) = \frac{\text{Var}(X_i)}{n} = \frac{9}{n}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Na mocy nierówności Czebyszewa:

$$P(|\bar{X}_n - 10| \geq 0.5) \leq \frac{Var(\bar{X}_n)}{0.5^2} = \frac{\frac{9}{n}}{0.25} = \frac{36}{n}.$$

Chcemy $\frac{36}{n} \leq 0.04 \Rightarrow n \geq \frac{36}{0.04} = 900$.

Przykład 7.14

Niech dany będzie ciąg X_i niezależnych prób Bernoulliego z $P(X_i = 1) = p = 0.4$.

Przyjmijmy

$$\bar{X}_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

a) Obliczyć $E(\bar{X}_n), Var(\bar{X}_n)$.

b) Dobierz n , by $P(|\bar{X}_n - 0.4| \geq 0.05) \leq 0.01$.

Rozwiązanie:

a) Dla rozkładu Bernoulliego mamy: $E(X_i) = p, Var(X_i) = p(1 - p) = 0.4 \cdot 0.6 = 0.24$.

$$E(\bar{X}_n) = 0.4, Var(\bar{X}_n) = \frac{0.24}{n}.$$

b) Na mocy nierówności Czebyszewa:

$$P(|\bar{X}_n - 0.4| \geq 0.05) \leq \frac{0.24/n}{0.05^2} = \frac{0.24/n}{0.0025} = \frac{96}{n}.$$

Warunek $\frac{96}{n} \leq 0.01 \Rightarrow n \geq 9600$.

Przykład 7.15

W jednej grze:

- z prawdopodobieństwem 0.7 gracz wygrana +1,
- z prawdopodobieństwem 0.3 gracz przegrana -2.

Niech Y oznacza zysk z jednej gry, zaś $S_n = \sum_{i=1}^n Y_i$ zysk po n grach

a) Obliczyć $E(Y)$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$E(Y) = 1 \cdot 0.7 + (-2) \cdot 0.3 = 0.7 - 0.6 = 0.1.$$

b) Obliczyć $Var(Y)$.

Najpierw:

$$E(Y^2) = 1^2 \cdot 0.7 + (-2)^2 \cdot 0.3 = 0.7 + 4 \cdot 0.3 = 0.7 + 1.2 = 1.9.$$

$$Var(Y) = E(Y^2) - [E(Y)]^2 = 1.9 - 0.1^2 = 1.9 - 0.01 = 1.89.$$

c) Zbadać granicę $\frac{S_n}{n}$.

Z prawa wielkich liczb mamy:

$$\frac{S_n}{n} \xrightarrow{P} E(Y) = 0.1.$$

Zatem można stwierdzić, że przy dużej liczbie gier średni zysk na grę stabilizuje się w pobliżu 0.1 zł, czyli gra jest „opłacalna” w sensie wartości oczekiwanej (choć wahania mogą być duże dla małych n).

Ćwiczenia samodzielne

Zadanie 7.1

Rzucamy dwiema uczciwymi kostkami. Niech S oznacza sumę oczek. Obliczyć

- a) $P(S = 7)$
- b) $P(S \geq 10)$
- c) $P(\max\{X_1, X_2\} = 5)$
- d) $P(\min\{X_1, X_2\} \geq 3)$

Zadanie 7.2

Rzucamy 3 razy uczciwą monetą. Obliczyć

- a) $P(\text{dokładnie 2 orły})$
- b) $P(\text{co najmniej 1 orzeł})$
- c) $P(\text{pierwszy orzeł w 2. rzucie})$
- d) $P(\text{nie ma dwóch kolejnych orłów})$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 7.3

W urnie jest 6 kul białych i 4 czarne. Losujemy 3 kule bez zwracania. Obliczyć

- a) $P(\text{dokładnie 2 białe})$
- b) $P(\text{wszystkie tego samego koloru})$
- c) $P(\text{co najmniej 1 czarna})$
- d) $P(\text{pierwsza biała, a wśród trzech dokładnie 1 czarna})$

Zadanie 7.4

W urnie jest 3 kule czerwone i 2 zielone. Losujemy 4 razy po jednej kuli ze zwracaniem. Obliczyć

- a) $P(\text{dokładnie 2 czerwone})$
- b) $P(\text{co najmniej 1 zielona})$
- c) $P(\text{pierwsza zielona i ostatnia zielona})$

Zadanie 7.5

Z talii 52 kart losujemy 2 karty bez zwracania. Obliczyć

- a) $P(\text{obie figury: J, Q, K, A})$
- b) $P(\text{dokładnie jedna kier})$
- c) $P(\text{co najmniej jeden as})$

Zadanie 7.6

Losujemy 5 kart z talii 52 kart.

- a) $P(\text{dokładnie 2 asy})$
- b) $P(\text{dokładnie 3 karty w tym samym kolorze (czarne/czerwone)})$
- c) $P(\text{dokładnie 1 para i nic więcej})$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 7.7

W pudełku jest 10 losów ponumerowanych 1–10. Losujemy 3 bez zwracania. Obliczyć:

- a) $P(\text{suma wylosowanych} = 15)$
- b) $P(\text{wszystkie parzyste})$
- c) $P(\text{dokładnie 2 liczby większe od 6})$

Zadanie 7.8

Losowo ustawiamy litery słowa **MATEMATYKA**.

- a) Jakie jest prawdopodobieństwo, że wyraz zaczyna się od M?
- b) Jakie jest prawdopodobieństwo, że dwie litery A stoją obok siebie?
- c) Jakie jest prawdopodobieństwo, że wszystkie samogłoski są obok siebie (tworzą blok)?

Zadanie 7.9

W grupie jest 8 kobiet i 6 mężczyzn. Losowo wybieramy 4 osoby. Obliczyć:

- a) $P(\text{dokładnie 2 kobiety})$
- b) $P(\text{co najmniej 1 mężczyzna})$
- c) $P(\text{same kobiety})$

Zadanie 7.10

Na 10 miejscach w rzędzie siada 6 osób (pozostałe 4 miejsca puste), losowo. Obliczyć:

- a) $P(\text{dwie wskazane osoby siedzą obok siebie})$
- b) $P(\text{żadne dwie osoby nie siedzą obok siebie})$

Zadanie 7.11

Punkt wybierany jest losowo i jednorodnie z kwadratu o wierzchołkach $(0,0)$, $(2,0)$, $(2,2)$, $(0,2)$.

- a) Oblicz prawdopodobieństwo, że punkt spełnia nierówność



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$x + y \leq 2.$$

b) Oblicz prawdopodobieństwo, że odległość punktu od środka kwadratu (1,1) jest mniejsza niż 1.

Zadanie 7.12

Losujemy niezależnie i jednorodnie dwie liczby $X, Y \sim U(0,1)$.

- a) Oblicz $P(X < Y)$.
- b) Oblicz $P(X + Y > 1.2)$.

Zadanie 7.13

W urnie znajduje się 5 kul białych i 3 czarne. Losujemy kolejno 2 kule bez zwracania.

- a) Oblicz prawdopodobieństwo, że druga kula jest biała, jeśli wiadomo, że pierwsza była czarna.
- b) Oblicz prawdopodobieństwo, że pierwsza kula była biała, jeśli wiadomo, że druga jest czarna.

Zadanie 7.14

Z talii 52 kart losujemy kolejno 2 karty bez zwracania.

- a) Oblicz $P(\text{druga karta jest asem} \mid \text{pierwsza jest figurą})$.
- b) Oblicz $P(\text{obie karty są pikami} \mid \text{pierwsza jest pikiem})$.

Zadanie 7.15

Trzy maszyny M_1, M_2, M_3 produkują odpowiednio 40%, 35% i 25% wyrobów.

Prawdopodobieństwa wady:

$$P(W \mid M_1) = 0.01, P(W \mid M_2) = 0.02, P(W \mid M_3) = 0.04.$$

- a) Oblicz prawdopodobieństwo, że losowo wybrany wyrób jest wadliwy.
- b) Oblicz prawdopodobieństwo, że wyrób pochodzi z maszyny M_2 .

Zadanie 7.16



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Student losowo wybiera jeden z trzech zestawów zadań:

$$P(A) = 0.5, P(B) = 0.3, P(C) = 0.2.$$

Prawdopodobieństwo zdania egzaminu:

$$P(Z | A) = 0.9, P(Z | B) = 0.7, P(Z | C) = 0.6.$$

a) Oblicz $P(Z)$.

b) Oblicz $P(\bar{Z})$.

Zadanie 7.17

Towar pochodzi z trzech hurtowni:

$$P(H_1) = 0.5, P(H_2) = 0.3, P(H_3) = 0.2.$$

Odsetek wadliwych wyrobów:

$$P(W | H_1) = 0.01, P(W | H_2) = 0.02, P(W | H_3) = 0.05.$$

a) Oblicz $P(W)$.

b) Oblicz $P(H_3 | W)$.

Zadanie 7.18

Zmienna losowa X przyjmuje wartości 1,2,3,4 z prawdopodobieństwami

$$P(X = k) = c(5 - k), k = 1, 2, 3, 4.$$

a) Wyznacz stałą c .

b) Sporządź tablicę rozkładu zmiennej X .

c) Oblicz $E(X)$ oraz $Var(X)$.

d) Oblicz $P(X \geq 3)$.

Zadanie 7.19

Rzucamy trzykrotnie uczciwą monetą. Niech X oznacza liczbę orłów.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- a) Wyznacz rozkład prawdopodobieństwa zmiennej X .
- b) Oblicz $E(X)$ oraz $Var(X)$.
- c) Oblicz $P(X \leq 1)$.

Zadanie 7.20

Rzucamy uczciwą monetą aż do uzyskania pierwszego orła.

Niech X oznacza liczbę rzutów.

- a) Zapisz rozkład prawdopodobieństwa zmiennej X .
- b) Oblicz $P(X > 4)$.
- c) Oblicz wartość oczekiwaną i wariancję zmiennej X .

Zadanie 7.21

Dana jest zmienna losowa X o rozkładzie:

x	-1	0	2
$P(X = x)$	0.2	0.5	0.3

Niech $Y = X^2$.

- a) Wyznacz rozkład zmiennej losowej Y .
- b) Oblicz $E(Y)$.
- c) Porównaj $E(Y)$ oraz $E(X^2)$.

Zadanie 7.22

Niech $X_1, X_2, \dots$ będą niezależnymi zmiennymi losowymi o tym samym rozkładzie, takimi że:

$$E(X_i) = 5, \quad Var(X_i) = 9.$$

Niech

$$\bar{X}_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

- a) Sformułuj prawo wielkich liczb dla ciągu $\bar{X}_n$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



b) Oblicz $E(\bar{X}_n)$ oraz $Var(\bar{X}_n)$.

Zadanie 7.23

Wykonujemy niezależnie n prób Bernoulliego z prawdopodobieństwem sukcesu $p = 0.4$. Niech X_i oznacza wynik i -tej próby [1 – sukces, 0 – porażka], a

$$\bar{X}_n = \frac{1}{n} \sum_{i=1}^n X_i.$$

a) Oblicz $E(\bar{X}_n)$ i $Var(\bar{X}_n)$.

b) Wyjaśnij, dlaczego $\bar{X}_n$ jest estymatorem p .

c) Dobierz n tak, aby

$$P(|\bar{X}_n - 0.4| \geq 0.05) \leq 0.01.$$

Zadanie 7.24

W każdej grze gracz:

- z prawdopodobieństwem 0.7 wygrywa 1 zł,
- z prawdopodobieństwem 0.3 przegrywa 2 zł.

Niech Y oznacza zysk z jednej gry, a S_n – łączny zysk po n grach.

a) Wyznacz $E(Y)$ i $Var(Y)$.

b) Zastosuj prawo wielkich liczb do ciągu $\frac{S_n}{n}$.

c) Zinterpretuj otrzymany wynik w kontekście „opłacalności” gry.

Pytania pomocnicze

1. Co nazywamy przestrzenią probabilistyczną i jakie elementy ją definiują?
2. Na czym polega różnica pomiędzy prawdopodobieństwem klasycznym a geometrycznym?
3. Jak interpretować prawdopodobieństwo warunkowe w kontekście zawężenia przestrzeni prób?
4. Kiedy zdarzenia losowe nazywamy niezależnymi?
5. W jakich sytuacjach stosujemy prawo całkowite prawdopodobieństwa?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



6. Jaka interpretację ma wzór Bayesa i jakie problemy pozwala rozwiązywać?
7. Co to jest zmienna losowa dyskretna i w jaki sposób opisuje się jej rozkład?
8. Jak obliczamy wartość oczekiwaną i wariancję zmiennej losowej?
9. Jakie znaczenie praktyczne ma prawo wielkich liczb?
10. Jak interpretować nierówność Czebyszewa?

Podsumowanie

W trakcie ćwiczeń studenci poznali podstawowe narzędzia rachunku prawdopodobieństwa i teorii zmiennych losowych dyskretnych. Przeanalizowane zostały zarówno klasyczne problemy probabilistyczne, jak i zadania wykorzystujące prawdopodobieństwo warunkowe, niezależność zdarzeń oraz wzór Bayesa.

Omówiono również własności wartości oczekiwanej i wariancji oraz ich zastosowanie do analizy losowych procesów powtarzalnych. Wprowadzenie prawa wielkich liczb i nierówności Czebyszewa pozwoliło na zrozumienie zachowania średnich z dużej liczby prób losowych i ocenę koncentracji wyników wokół wartości oczekiwanej.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 8

Reprezentacja grafów: listy sąsiedztwa, macierz incydencji. Implementacja i analiza algorytmów przeszukiwania grafów. Rozwiązanie problemu komiwojażera

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



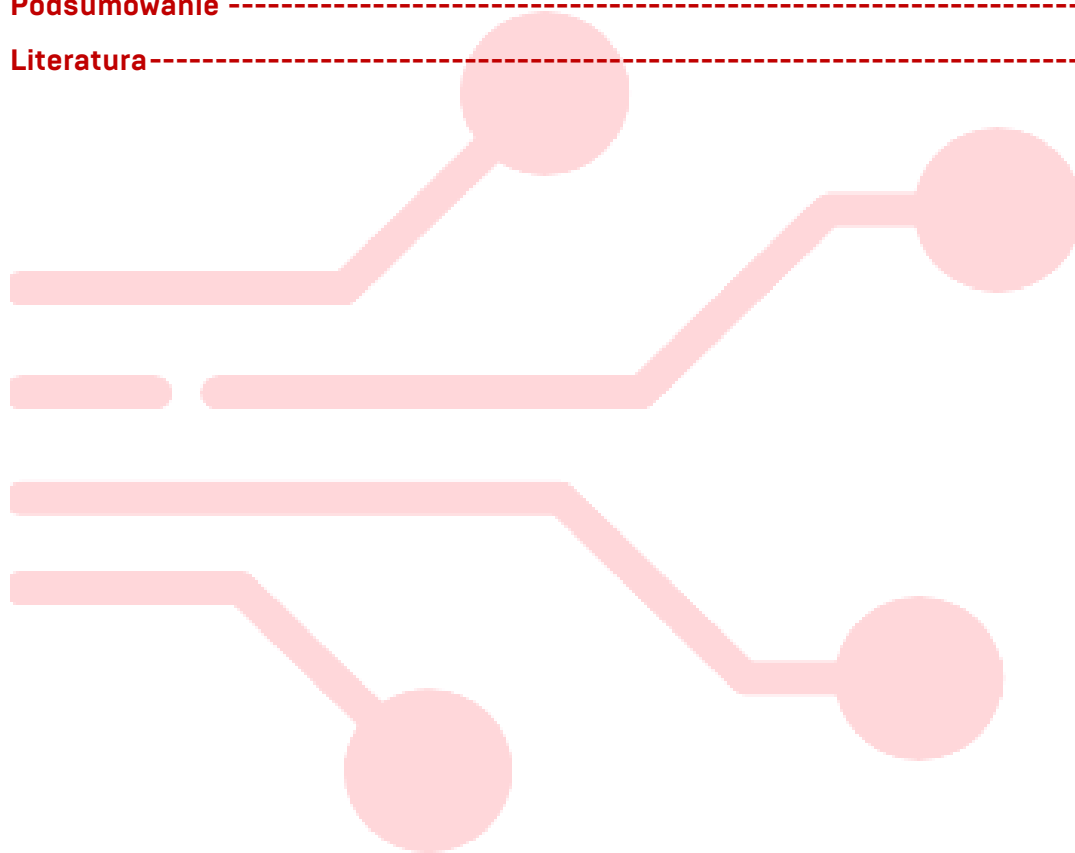
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	120
Cel ćwiczenia/laboratorium	123
Instrukcja laboratoryjna/ćwiczeniowa	123
Ćwiczenia samodzielne	130
Pytania pomocnicze	133
Podsumowanie	134
Literatura	134



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Podstawowe pojęcia teorii grafów

Grafem nazywamy parę

$$G = (V, E),$$

gdzie V jest niepustym, skończonym zbiorem wierzchołków, a E jest zbiorem krawędzi [graf nieskierowany] lub łuków [graf skierowany].

- W grafie nieskierowanym krawędź jest parą nieuporządkowaną $\{u, v\}$.
- W grafie skierowanym łuk jest parą uporządkowaną (u, v) .
- Dwa wierzchołki połączone krawędzią (lub łukiem) nazywamy sąsiednimi.

Stopnie wierzchołków i podstawowe własności

Stopniem wierzchołka v nazywamy liczbę krawędzi incydentnych z v i oznaczamy przez $\deg(v)$.

Zachodzi zależność:

$$\sum_{v \in V} \deg(v) = 2 |E|.$$

W graf skierowanym wyróżniamy

- stopień wejściowy: $\deg^-(v)$ – liczba łuków wchodzących do v ,
- stopień wyjściowy: $\deg^+(v)$ – liczba łuków wychodzących z v .

Grafy eulerowskie

Graf nieskierowany:

- jest eulerowski, gdy jest spójny i każdy wierzchołek ma stopień parzysty,
- jest półeulerowski, gdy jest spójny i dokładnie dwa wierzchołki mają stopień nieparzysty.

Kryterium to opiera się wyłącznie na stopniach wierzchołków.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Reprezentacje grafów

Listy sąsiedztwa

Każdemu wierzchołkowi przypisujemy listę jego sąsiadów.

Reprezentacja ta:

- jest czytelna tablicowo,
- pozwala łatwo wyznaczać stopnie,
- jest naturalna przy BFS i DFS.

Macierz sąsiedztwa

Dla grafu o n wierzchołkach definiujemy macierz:

$$A = (a_{ij}), a_{ij} = \begin{cases} 1 & \text{jeśli istnieje krawędź/łuk } i \rightarrow j, \\ 0 & \text{w przeciwnym razie.} \end{cases}$$

Dla grafu nieskierowanego macierz jest symetryczna.

Macierz incydencji

Dla grafu nieskierowanego:

$$B_{v,e} = \begin{cases} 1 & \text{jeśli wierzchołek } v \text{ jest końcem krawędzi } e, \\ 0 & \text{w przeciwnym razie.} \end{cases}$$

Każda kolumna zawiera dokładnie dwie jedynki.

Dla grafu skierowanego (konwencja $-1, +1$):

$$B_{v,e} = \begin{cases} -1 & \text{jeśli łuk } e \text{ wychodzi z } v, \\ +1 & \text{jeśli łuk } e \text{ wchodzi do } v, \\ 0 & \text{w przeciwnym razie.} \end{cases}$$

Suma elementów w każdej kolumnie wynosi 0.

Przeszukiwanie grafów

BFS [Breadth-First Search] polega na odwiedzaniu wierzchołków warstwami, według rosnącej odległości od wierzchołka startowego.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Własności BFS:

- wyznacza najkrótsze ścieżki w grafie nieważonym,
- buduje drzewo BFS,
- umożliwia sprawdzanie spójności grafu,
- pozwala badać dwudzielność grafu.

Odległość w BFS oznacza liczbę krawędzi na najkrótszej ścieżce.

DFS (Depth-First Search) polega na przechodzeniu w głąb grafu, dopóki jest to możliwe, a następnie cofania się (backtracking).

Własności DFS:

- buduje drzewo DFS,
- umożliwia wykrywanie cykli,
- służy do wyznaczania porządku topologicznego,
- pozwala wykrywać mosty i punkty artykulacji.

Kolejność odwiedzin w DFS zależy od kolejności sąsiadów.

Cykle Hamiltona i problem komiwojażera (TSP)

Cyklem Hamiltona nazywamy cykl przechodzący przez każdy wierzchołek grafu dokładnie jeden raz.

Problem komiwojażera (TSP) polega na znalezieniu najkrótszego cyklu Hamiltona w pełnym grafie ważonym.

Własności:

- cykl i jego odwrócenie mają tę samą długość,
- liczba możliwych tras rośnie bardzo szybko $((n - 1)!)$,
- dla małych grafów możliwe jest ręczne przeglądanie permutacji z wykorzystaniem prostych kryteriów odrzucania tras.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cel ćwiczenia/laboratorium

Celem ćwiczenia jest:

- zapoznanie się z podstawowymi reprezentacjami grafów,
- nabycie umiejętności ręcznego wykonywania algorytmów BFS i DFS,
- analiza własności grafów na podstawie ich struktury,
- rozwiązanie prostych instancji problemu komiwojażera metodami tablicowymi.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 8.1

Dany jest graf nieskierowany $G = (V, E)$, gdzie

$$V = \{1, 2, 3, 4, 5, 6\}$$

oraz

$$E = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 5\}, \{4, 5\}, \{4, 6\}\}.$$

- Zapisz listę sąsiedztwa (w porządku rosnącym).
- Oblicz stopnie wszystkich wierzchołków.
- Sprawdź, czy graf jest eulerowski / półeulerowski.

Rozwiązanie

1) Dla badanego grafu lista sąsiedztwa ma postać:

1: 2,3

2: 1,3,4

3: 1,2,5

4: 2,5,6

5: 3,4

6: 4

2) W oparciu o listę sąsiedztwa wyznaczamy stopnie poszczególnych wierzchołków:

$$\deg(1) = 2, \deg(2) = 3, \deg(3) = 3, \deg(4) = 3, \deg(5) = 2, \deg(6) = 1.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Suma stopni: $2 + 3 + 3 + 3 + 2 + 1 = 14$, więc $|E| = \frac{14}{2} = 7$ [zgodnie z danymi].

3) Sprawdzenie, czy graf jest eulerowski.

Graf eulerowski $\Leftrightarrow$ wszystkie stopnie parzyste. W naszym przypadku, własność ta nie jest spełniona.

Graf półeulerowski (istnieje droga Eulera) $\Leftrightarrow$ dokładnie dwa wierzchołki nieparzyste.

W naszym grafie wierzchołki nieparzyste: 2,3,4,6, więc nie jest półeulerowski.

Przykład 8.2

Dla grafu z Przykładu 8.1 numerujemy krawędzie:

$$\begin{aligned} e_1 &= \{1,2\}, e_2 = \{1,3\}, \\ e_3 &= \{2,3\}, e_4 = \{2,4\}, \\ e_5 &= \{3,5\}, e_6 = \{4,5\}, \\ e_7 &= \{4,6\}. \end{aligned}$$

Zapisz macierz incydencji B rozmiaru 6×7 , gdzie

$$B_{v,e} = \begin{cases} 1 & \text{gdy } v \text{ jest końcem krawędzi } e, \\ 0 & \text{w p.p.} \end{cases}$$

Rozwiązanie

Wiersze: 1, ..., 6. Kolumny: $e_1, \dots, e_7$.

Wierzchołek 1 jest incydentny z e_1, e_2 . Podobnie dla pozostałych wierzchołków:

2 z e_1, e_3, e_4 .

3 z e_2, e_3, e_5 .

4 z e_4, e_6, e_7 .

5 z e_5, e_6 .

6 z e_7 .

Zatem macierz ma postać:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	1	0	0	0	0	0
2	1	0	1	1	0	0	0
3	0	1	1	0	1	0	0
4	0	0	0	1	0	1	1
5	0	0	0	0	1	1	0
6	0	0	0	0	0	0	1

Przykład 8.3

Rozważ graf nieskierowany G o wierzchołkach $V = \{A, B, C, D, E, F, G\}$ i krawędziach:

$\{A, B\}, \{A, C\}, \{B, D\}, \{B, E\}, \{C, F\}, \{E, F\}, \{D, G\}, \{F, G\}$.

- Wykonaj przeszukiwanie wszerz (BFS) od A przy założeniu, że sąsiadów przeglądamy alfabetycznie.
- Podaj kolejność zdejmowania z kolejki.
- Podaj warstwy $L_0, L_1, L_2, \dots$
- Zapisz drzewo BFS (krawędzie rodzic–dziecko).

Rozwiązanie

Listy sąsiedztwa (alfabetycznie):

$A: B, C$

$B: A, D, E$

$C: A, F$

$D: B, G$

$E: B, F$

$F: C, E, G$

$G: D, F$

Algorytm BST:

Start: kolejka $[A]$, A odwiedzony, $\text{dist}(A) = 0$.

Krok po kroku (zdejmowanie z kolejki):

Zdejmij A . Dodaj nieodwiedzonych sąsiadów B, C . Kolejka $[B, C]$.

Rodzice: $B \leftarrow A$, $C \leftarrow A$. Odległości: 1.

Zdejmij B . Sąsiedzi: A (już odwiedzony), D (nowy), E (nowy). Kolejka $[C, D, E]$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Rodzice: $D \leftarrow B, E \leftarrow B$. Odległości: 2.

Zdejmij C . Sąsiedzi: A (już odwiedzony), F (nowy). Kolejka $[D, E, F]$.

Rodzic: $F \leftarrow C$. Odległość: 2.

Zdejmij D . Sąsiedzi: B (już odwiedzony), G (nowy). Kolejka $[E, F, G]$.

Rodzic: $G \leftarrow D$. Odległość: 3.

Zdejmij E . Sąsiedzi: B (już odwiedzony), F (już odwiedzony). Kolejka $[F, G]$.

Zdejmij F . Sąsiedzi: C, E, G (wszyscy już odwiedzani). Kolejka $[G]$.

Zdejmij G . Koniec.

1) Kolejność zdejmowania:

A, B, C, D, E, F, G .

2) Warstwy (odległości od A):

$$L_0 = \{A\}$$

$$L_1 = \{B, C\}$$

$$L_2 = \{D, E, F\}$$

$$L_3 = \{G\}$$

3) Drzewo BFS (krawędzie rodzic–dziecko):

$(A, B), (A, C), (B, D), (B, E), (C, F), (D, G)$.

Przykład 8.4

Dany jest graf skierowany o wierzchołkach $V = \{1, 2, 3, 4, 5, 6\}$ oraz łukach:

$1 \rightarrow 2, 1 \rightarrow 3, 2 \rightarrow 4, 2 \rightarrow 5, 3 \rightarrow 5, 4 \rightarrow 6, 5 \rightarrow 6$.

- Wykonaj przeszukiwanie w głąb (DFS) startując od 1, a sąsiadów odwiedzaj w porządku rosnącym.
- Podaj kolejność pierwszych odwiedzin wierzchołków.
- Podaj krawędzie drzewa DFS.

Rozwiązanie

Wyznaczamy listę sąsiedztwa

1: 2,3



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



2: 4,5

3: 5

4: 6

5: 6

6: $\emptyset$

Start DFS[1]:

Odwiedzamy 1, idziemy do 2.

W 2: idziemy do 4.

W 4: idziemy do 6.

6 kończy się (brak wyjść), wracamy do 4, potem do 2.

W 2 kolejny sąsiad to 5: wchodzimy do 5.

W 5 sąsiad 6 już odwiedzony.

Wracamy do 1, teraz sąsiad 3: wchodzimy do 3.

W 3 sąsiad 5 już odwiedzony.

1) Kolejność pierwszych odwiedzin:

1, 2, 4, 6, 5, 3.

2) Krawędzie drzewa DFS (te, którymi weszliśmy do nowego wierzchołka):

$1 \rightarrow 2, 2 \rightarrow 4, 4 \rightarrow 6, 2 \rightarrow 5, 1 \rightarrow 3.$

Przykład 8.5

Dla digrafu z Przykładu 8.4 zbuduj macierz incydencji B rozmiaru 6×7 przy konwencji:

$$B_{v,e} = \begin{cases} -1 & \text{gdy łuk } e \text{ wychodzi z } v, \\ +1 & \text{gdy łuk } e \text{ wchodzi do } v, \\ 0 & \text{wpp.} \end{cases}$$

Przyjmij kolejność łuków:

$e_1: 1 \rightarrow 2, e_2: 1 \rightarrow 3, e_3: 2 \rightarrow 4, e_4: 2 \rightarrow 5, e_5: 3 \rightarrow 5, e_6: 4 \rightarrow 6, e_7: 5 \rightarrow 6.$

Rozwiązanie



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wpisujemy w każdej kolumnie dokładnie jedno -1 (w wierszu źródła) i jedno $+1$ (w wierszu celu):

$$B = \begin{array}{c|ccccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\ \hline 1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 2 & +1 & 0 & -1 & -1 & 0 & 0 & 0 \\ 3 & 0 & +1 & 0 & 0 & -1 & 0 & 0 \\ 4 & 0 & 0 & +1 & 0 & 0 & -1 & 0 \\ 5 & 0 & 0 & 0 & +1 & +1 & 0 & -1 \\ 6 & 0 & 0 & 0 & 0 & 0 & +1 & +1 \end{array}$$

Kontrola: suma w każdej kolumnie to 0. To jest typowa własność takiej macierzy incydencji.

Przykład 8.6

Dane są miasta $\{A, B, C, D, E\}$ oraz symetryczna macierz odległości (km):

	A	B	C	D	E
A	0	2	9	10	7
B	2	0	6	4	3
C	9	6	0	8	5
D	10	4	8	0	6
E	7	3	5	6	0

Znajdź najkrótszy cykl Hamiltona (problem komiwojażera) startujący i kończący w mieście A.

Wskazówka: możesz przeglądać permutacje B, C, D, E , ale pamiętaj, że cykl i jego odwrócenie mają tę samą długość.

Rozwiązanie

Szukamy minimalnej długości trasy:

$$A \rightarrow (\text{permutacja } B, C, D, E) \rightarrow A.$$

Ponieważ graf jest symetryczny, cykl

$$A \rightarrow x_1 \rightarrow x_2 \rightarrow x_3 \rightarrow x_4 \rightarrow A$$

ma tę samą długość co odwrócony

$$A \rightarrow x_4 \rightarrow x_3 \rightarrow x_2 \rightarrow x_1 \rightarrow A.$$

Możemy więc liczyć tylko te permutacje, w których np. $x_1 < x_4$ w jakimś ustalonym porządku literowym; ale tu policzymy rozsądny podzbiór i wskażemy minimum.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Policzmy długości kilku wybranych dróg

Droga $A - B - D - E - C - A$ ma długość $2 + 4 + 6 + 5 + 9 = 26$.

Droga $A - B - E - C - D - A$ ma długość $2 + 3 + 5 + 8 + 10 = 28$

Droga $A - B - E - D - C - A$ ma długość $2 + 3 + 6 + 8 + 9 = 28$

Droga $A - B - D - C - E - A$ ma długość $2 + 4 + 8 + 5 + 7 = 26$

Droga $A - E - B - D - C - A$ ma długość $7 + 3 + 4 + 8 + 9 = 31$

$A - E - B - D - C - A$ już jest niewłaściwe (31), więc patrzymy na trasy oparte na małowartościowych krawędziach: z tabeli widać, że najtańsze są m.in. $A - B = 2$, $B - E = 3$, $B - D = 4$, $C - E = 5$, $B - C = 6$, $D - E = 6$.

Sprawdźmy jeszcze drogi:

$$A - C - E - B - D - A: 9 + 5 + 3 + 4 + 10 = 31$$

$$A - D - B - E - C - A: 10 + 4 + 3 + 5 + 9 = 31$$

Widzimy, że 26 pojawia się już rozważanych trasach. Upewnijmy się, czy da się zejść poniżej wartości 26.

Żeby mieć < 26 , suma pięciu krawędzi musiałaby być ≤ 25 . Ponieważ zawsze musimy użyć dwóch krawędzi incydentnych z A , a najtaniej z A jest do $B(2)$ oraz do $E(7)$ lub do $C(9)$ lub do $D(10)$. Najlepszy „start” to więc $2 + 7 = 9$ (czyli A łączy się z B i E).

Wtedy pozostałe trzy krawędzie (łącznie C, D i spinające środek trasy) musiałby dać $\leq 25 - 9 = 16$.

Ale trzy krawędzie w środku, nawet bardzo dobre, to np. $B - D = 4$, $D - C = 8$, $C - E = 5$ daje 17 (już za dużo), albo $B - E = 3$, $E - C = 5$, $C - D = 8$ też 16, ale wtedy trzeba sprawdzić spójność cyklu (czy nie dublujemy stopni w wierzchołkach). Przy strukturze cyklu z A do B i E typowy kandydat to:

$$A - B - D - C - E - A = 2 + 4 + 8 + 5 + 7 = 26$$

albo

$$A - B - E - C - D - A = 2 + 3 + 5 + 8 + 10 = 28.$$

Żeby uzyskać 25 lub mniej, musielibyśmy unikać „drogich” $C - A = 9$ i $D - A = 10$ na końcu, ale jeśli A jest połączone z B i E , to końcówki są właśnie $A - B$ i $A - E$, co jest już ustalone (najlepsze). Wtedy w środku musimy połączyć C i D w cykl tak, by każdy miał stopień 2. W praktyce wymusza to użycie jednej z krawędzi $C - D =$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$8, C - B = 6, C - E = 5, D - B = 4, D - E = 6$. Minimalny rdzeń pasujący do cyklu daje co najmniej $4 + 8 + 5 = 17$ (jak wyżej) lub inne kombinacje nie schodzące poniżej 17 bez łamania stopni. Zatem <26 nie da się uzyskać.

Wniosek: minimalna długość to 26 km, a przykładowe optymalne cykle:

$A \rightarrow B \rightarrow D \rightarrow C \rightarrow E \rightarrow A[26]$

$A \rightarrow B \rightarrow D \rightarrow E \rightarrow C \rightarrow A[26]$

Ćwiczenia samodzielne

Zadanie 8.1

Dany jest graf nieskierowany

$V = \{1, 2, 3, 4\}$,

$E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$.

- Zapisz listy sąsiedztwa grafu.
- Oblicz stopnie wierzchołków.
- Sprawdź, czy graf jest spójny.

Zadanie 8.2

Dany jest graf nieskierowany

$V = \{A, B, C, D, E\}$,

$E = \{\{A, B\}, \{A, C\}, \{B, C\}, \{C, D\}, \{D, E\}\}$.

- Zapisz macierz sąsiedztwa.
- Oblicz liczbę krawędzi na podstawie macierzy.
- Wskaż wszystkie trójki wierzchołków tworzące trójkąt.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 8.3

Dany jest graf nieskierowany o macierzy incydencji:

	e_1	e_2	e_3	e_4
1	1	1	0	0
2	1	0	1	0
3	0	1	1	1
4	0	0	0	1

- Opisz zbiór krawędzi.
- Narysuj graf.
- Podaj stopnie wierzchołków.

Zadanie 8.4

Dany jest graf nieskierowany

$$V = \{1, 2, 3, 4, 5, 6\},$$

$$E = \{\{1, 2\}, \{1, 3\}, \{2, 4\}, \{2, 5\}, \{3, 6\}\}.$$

- Zapisz listy sąsiedztwa.
- Zapisz macierz incydencji.
- Wskaż wszystkie liście grafu.

Zadanie 8.5

Dany jest graf skierowany

$$V = \{A, B, C, D\},$$

$$E = \{A \rightarrow B, A \rightarrow C, B \rightarrow D, C \rightarrow D\}.$$

- Zapisz macierz sąsiedztwa.
- Zapisz macierz incydencji w konwencji $-1, +1$.
- Podaj stopnie wejściowe i wyjściowe wierzchołków.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 8.6

Dany jest graf nieskierowany.

$$V = \{A, B, C, D\},$$

$$E = \{A \rightarrow B, A \rightarrow C, B \rightarrow D, C \rightarrow D\}.$$

- Podaj zależność między sumą stopni wierzchołków a liczbą krawędzi.
- Uzasadnij tę zależność.
- Zastosuj ją do dowolnego przykładu grafu o co najmniej 6 wierzchołkach.

Zadanie 8.7

Dany jest graf nieskierowany:

$$V = \{A, B, C, D, E\}$$

$$E = \{\{A, B\}, \{A, C\}, \{B, D\}, \{C, E\}\}.$$

- Wykonaj BFS od wierzchołka A , przyjmując porządek alfabetyczny sąsiadów.
- Podaj kolejność odwiedzin.
- Wyznacz warstwy BFS.
- Zapisz drzewo BFS.

Zadanie 8.8

Dany jest graf nieskierowany.

$$V = \{A, B, C, D\},$$

$$E = \{A \rightarrow B, A \rightarrow C, B \rightarrow D, C \rightarrow D\}.$$

- Wyjaśnij, kiedy BFS może posłużyć do sprawdzenia spójności grafu.
- Jakie wnioski można wyciągnąć, jeśli BFS nie odwiedzi wszystkich wierzchołków?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 8.9

Dany jest graf nieskierowany:

$$V = \{1,2,3,4,5,6\}$$

$$E = \{\{1,2\}, \{1,3\}, \{2,4\}, \{3,4\}, \{4,5\}, \{5,6\}\}.$$

- Wykonaj BFS od wierzchołka 1.
- Podaj najkrótszą ścieżkę (w liczbie krawędzi) z 1 do 6.
- Podaj długość tej ścieżki.

Zadanie 8.10

Dany jest graf nieskierowany.

$$V = \{1,2,3,4,5,6\}$$

$$E = \{\{1,2\}, \{1,3\}, \{2,4\}, \{3,4\}, \{4,5\}, \{5,6\}\}.$$

- Wyjaśnij, w jaki sposób BFS może służyć do sprawdzania, czy graf jest dwudzielny.
- Podaj przykład grafu dwudzielnego i niedwudzielnego.

Zadanie 8.11

Dany jest graf skierowany:

$$1 \rightarrow 2, 1 \rightarrow 3, 2 \rightarrow 4, 3 \rightarrow 4.$$

- Wykonaj DFS od wierzchołka 1 (sąsiedzi rosnąco).
- Podaj kolejność odwiedzin.
- Zapisz drzewo DFS.

Pytania pomocnicze

1. Jaka jest różnica pomiędzy BFS a DFS?
2. Dlaczego BFS wyznacza najkrótsze ścieżki w grafie nieważonym?
3. Od czego zależy kolejność odwiedzin w DFS?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



4. Dlaczego w TSP można pominąć cykl i jego odwrócenie?

Podsumowanie

Podczas ćwiczeń omówiono podstawowe pojęcia teorii grafów, sposoby ich reprezentacji oraz algorytmy przeszukiwania grafów. Przedstawione metody umożliwiają analizę struktury grafów oraz rozwiązywanie klasycznych problemów, takich jak problem komiwojażera, dla niewielkich instancji.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 9

Implementacja drzew binarnych i operacji na nich. Eksperymentalna analiza różnych metod wyszukiwania

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



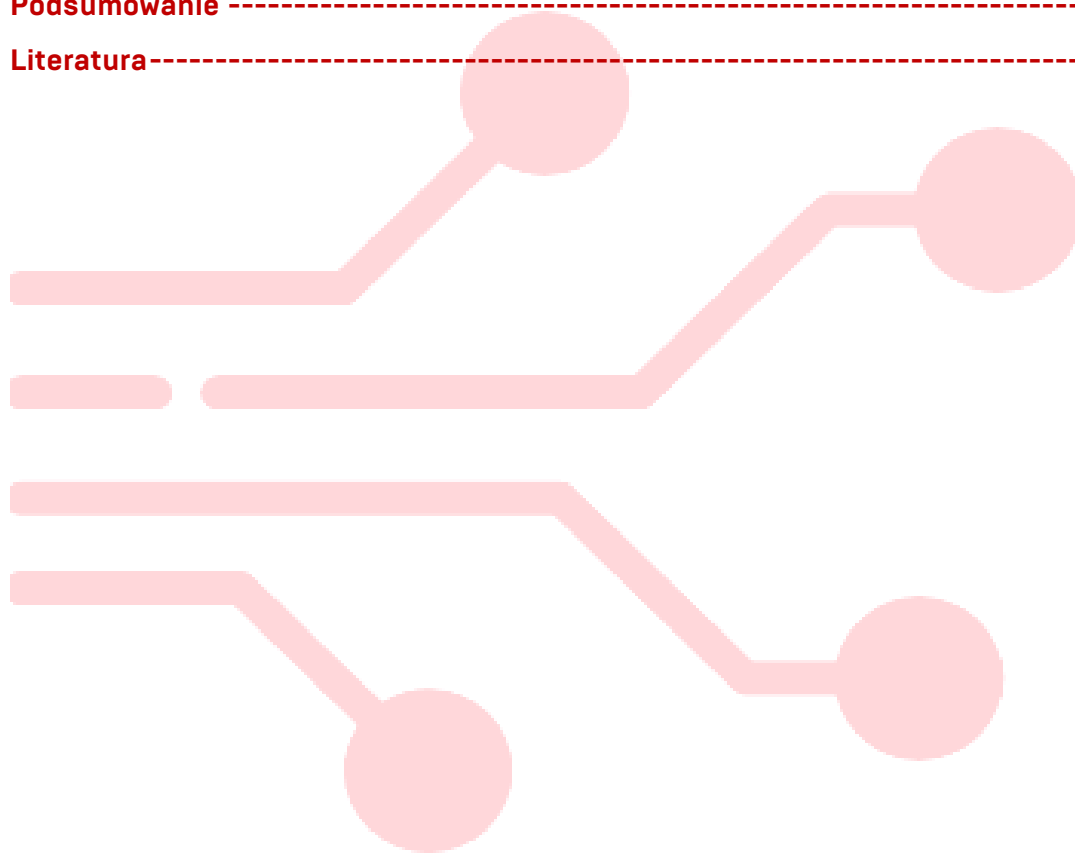
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	137
Cel ćwiczenia/laboratorium	138
Instrukcja laboratoryjna/ćwiczeniowa	138
Ćwiczenia samodzielne	145
Pytania pomocnicze	151
Podsumowanie	151
Literatura	151



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Drzewo binarne

Drzewem binarnym nazywamy uporządkowaną strukturę:

$$T = (V, E)$$

gdzie:

- V jest skończonym zbiorem węzłów,
- $E \subseteq V \times V$ jest zbiorem krawędzi,

każdy węzeł ma co najwyżej dwoje dzieci, wyróżnionych jako lewe i prawe.

Pojęcia podstawowe:

- korzeń – węzeł bez rodzica,
- liść – węzeł bez dzieci,
- wysokość drzewa – liczba krawędzi na najdłuższej ścieżce od korzenia do liścia,
- poziom węzła – liczba krawędzi od korzenia do danego węzła.

Przechodzenie drzewa

DFS (Depth First Search):

- preorder (NLR): węzeł $\rightarrow$ lewy $\rightarrow$ prawy,
- inorder (LNR): lewy $\rightarrow$ węzeł $\rightarrow$ prawy,
- postorder (LRN): lewy $\rightarrow$ prawy $\rightarrow$ węzeł.

BFS (Breadth First Search):

- przechodzenie poziomami,
- implementowane z użyciem kolejki FIFO.

Binarne drzewo wyszukiwań (BST)

BST jest drzewem binarnym spełniającym warunek:

$$\forall v \in V: \text{klucze}(L(v)) < \text{klucz}(v) < \text{klucze}(R(v))$$

gdzie $L(v)$ oraz $R(v)$ oznaczają odpowiednio lewe i prawe poddrzewo węzła v .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Własności BST:

- inorder zawsze generuje ciąg kluczy w porządku rosnącym,
- koszt wyszukiwania jest proporcjonalny do wysokości drzewa,
- w najgorszym przypadku BST może ulec degeneracji do listy.

Usuwanie węzłów w BST

Rozróżniamy trzy przypadki:

- usuwany węzeł jest liściem,
- usuwany węzeł ma jedno dziecko,
- usuwany węzeł ma dwoje dzieci – stosuje się następnik lub poprzednik inorder.

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest:

- zapoznanie studentów z formalną definicją drzew binarnych i BST,
- praktyczne opanowanie algorytmów przechodzenia drzew,
- zrozumienie wpływu struktury drzewa na efektywność wyszukiwania,
- rozwijanie umiejętności analizy algorytmów na podstawie prostych eksperymentów,
- kształtowanie umiejętności rysowania i interpretacji struktur drzewiastych.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 9.1.

Dane jest drzewo binarne:

```
A
 / \
B   C
/\   \
D E   F
```



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- Zapisz drzewo jako strukturę węzłów: (klucz, lewy, prawy).
- Podaj: liczbę węzłów, liczbę liści, wysokość (liczba krawędzi na najdłuższej ścieżce od korzenia do liścia).

Rozwiązanie.

Reprezentacja węzłowa:

A: [A, B, C]

B: [B, D, E]

C: [C, $\emptyset$, F]

D: [D, $\emptyset$, $\emptyset$]

E: [E, $\emptyset$, $\emptyset$]

F: [F, $\emptyset$, $\emptyset$]

Analizowane drzewo ma następujące własności:

- Liczba węzłów wynosi 6 [A,B,C,D,E,F].
- Liczba liści wynosi 3: D, E, F .
- Wysokość drzewa, czyli najdłuższa ścieżka wynosi 2, bowiem: A–B–D lub A–B–E lub A–C–F ma 2 krawędzie

Przykład 9.2.

Dla drzewa z Przykładu 9.1 wypisz kolejno węzły w porządkach: preorder, inorder, postorder.

Rozwiązanie.

Drzewo:

```

  A
 / \
B   C
/\  \
D E  F

```

Preorder (NLR),czyli najpierw węzeł, potem lewy, następnie prawy. W takim przypadku mamy:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



A, B, D, E, C, F

Inorder (LNR), czyli lewy, węzeł, prawy. W takim przypadku mamy: D, B, E, A, C, F

Postorder (LRN), czyli lewy, prawy, węzeł. W takim przypadku mamy: D, E, B, F, C, A

Przykład 9.3

Zbuduj drzewo BST (Binary Search Tree) przez wstawianie kluczy w kolejności:

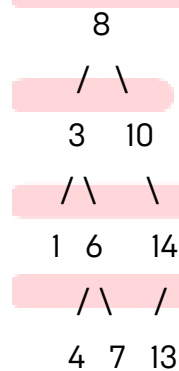
8, 3, 10, 1, 6, 14, 4, 7, 13.

Narysuj drzewo końcowe i podaj inorder.

Rozwiązanie.

Wstawiamy po kolei zgodnie z regułą BST: lewo < węzeł < prawo.

Końcowe drzewo ma postać:



Inorder w BST daje klucze w kolejności rosnącej: 1, 3, 4, 6, 7, 8, 10, 13, 14.

Przykład 9.4

Dla BST z Przykładu 9.3 wykonaj wyszukiwanie klucza 7 oraz 2.

Policz liczbę porównań typu „czy szukany < aktualny?” / „czy szukany > aktualny?”



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Rozwiązanie.

BST:

```

      8
     / \
    3   10
   /\   \
  1 6   14
   /\   /
  4 7  13
  
```

Szukanie elementu 7

Ścieżka: $8 \rightarrow 3 \rightarrow 6 \rightarrow 7$.

Odwiedzone węzły: 4, więc odnotowujemy 4 porównania/wizyty.

Szukanie elementu 2

Ścieżka: $8 \rightarrow 3 \rightarrow 1 \rightarrow \{\text{prawy syn } \emptyset\}$ bo:

$2 < 8 \rightarrow \text{lewo}$

$2 < 3 \rightarrow \text{lewo}$

$2 > 1 \rightarrow \text{pravo (brak)}$

Odwiedzone węzły: 3 (8,3,1), potem koniec na $\emptyset$.

Przykład 9.6.

W BST z Przykładu 9.4 usuń kolejno:

- 7 (liść)
- 14 (węzeł z jednym dzieckiem)
- 3 (węzeł z dwoma dziećmi) – użyj następnik inorder.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Rozwiązanie.

a) Element 7 jest liściem, zatem po prostu odpinamy ten element i otrzymujemy drzewo:

```

      8
     / \
    3   10
   /\   \
  1 6   14
   /    \
  4     13
  
```

b) Element 14 ma jedno dziecko (element 13), zatem zastępujemy 14 jego jedynym dzieckiem:

```

      8
     / \
    3   10
   /\   \
  1 6   13
   /
  4
  
```

c) Element 3 ma dwoje dzieci: 1 oraz 6

Następnik inorder dla 3 to najmniejszy w prawym poddrzewie 3, czyli 4 (bo w prawym poddrzewie jest 6 z lewym dzieckiem 4). Wykonujemy następujące kroki:

Zamień wartość węzła 3 na 4. Usuń „stare” 4 z miejsca, gdzie było (liść pod 6).

Otrzymujemy następujący wynik (z wersji po b):

```

      8
     / \
    4   10
   /\   \
  1 6   13
  
```



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 9.7.

Rozważ dwa BST zawierające te same klucze: 1,2,3,4,5,6,7.

BST zbudowane przez wstawianie w kolejności rosnącej: 1,2,3,4,5,6,7.

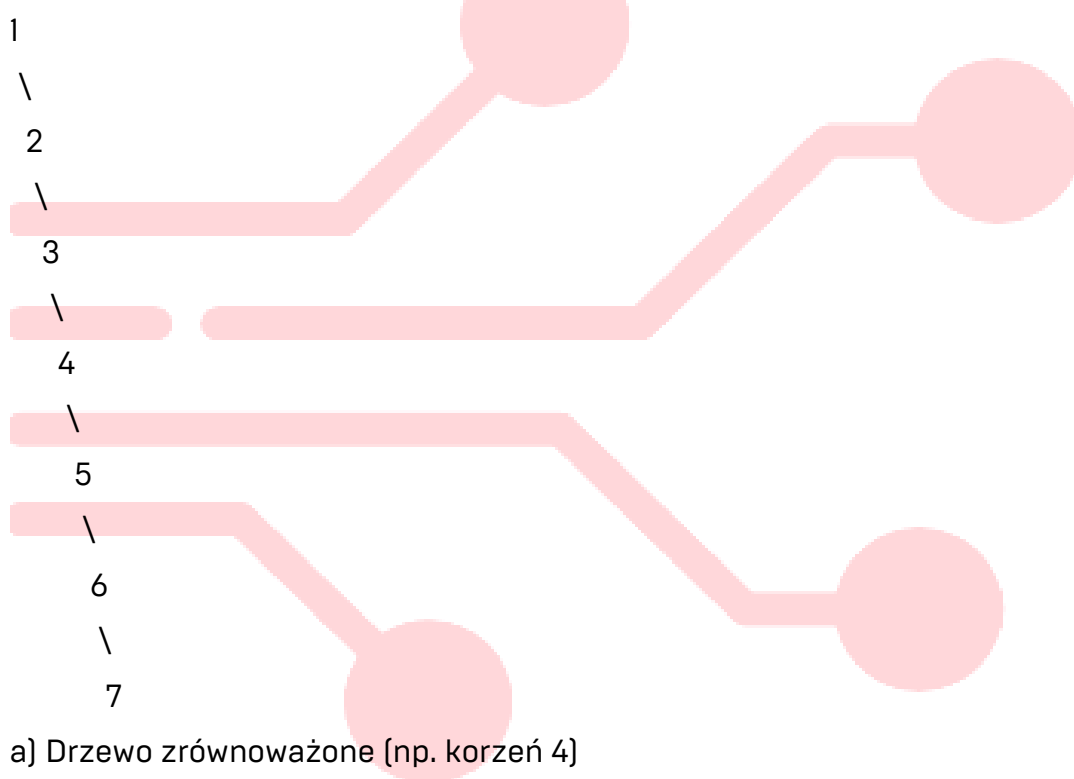
BST idealnie zrównoważone (minimalna wysokość).

a) Narysuj oba drzewa.

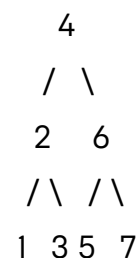
b) Dla każdego drzewa policz liczbę wizyt węzłów przy wyszukiwaniu 7 oraz 4.

Rozwiązanie.

a) Drzewo zdegenerowane (rosnące wstawianie) o wysokości 6:



a) Drzewo zrównoważone (np. korzeń 4)



Wysokość tego drzewa wynosi jedynie 2.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



b) Wyznaczamy liczbę wizyt przy wyszukiwaniu elementu 7:

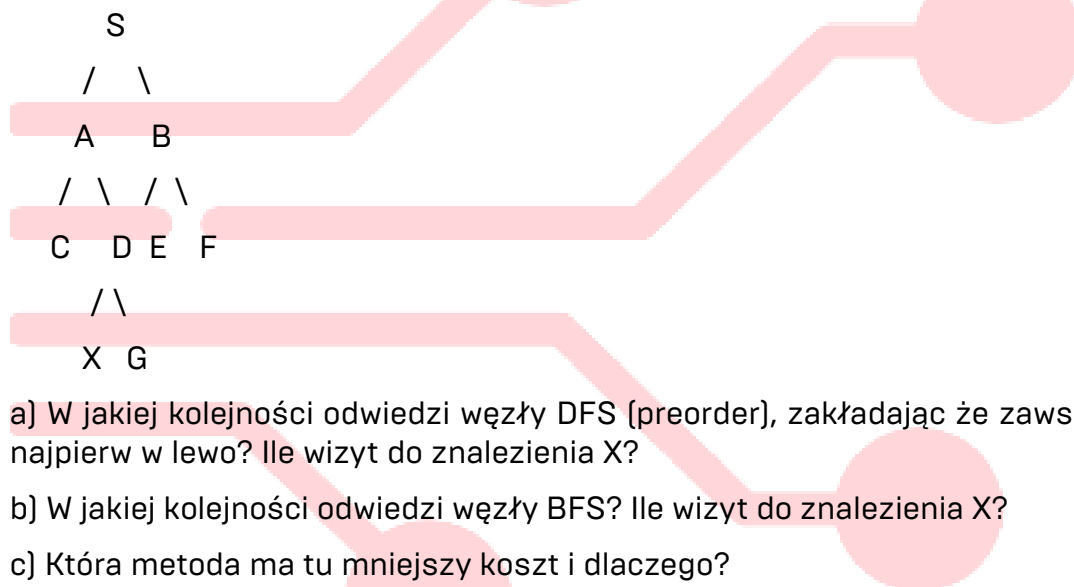
- Drzewo zdegenerowane odwiedzamy kolejno: 1,2,3,4,5,6,7 zatem mamy 7 wizyt
- Drzewo zrównoważone: $4 \rightarrow 6 \rightarrow 7$. Liczba wizyt ogranicza się do 3.

Podobnie przy wyszukiwaniu elementu 4:

- Drzewo zdegenerowane: $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$, aż 4 wizyty
- Drzewo zrównoważone: 4, tylko 1 wizyta

Przykład 9.8.

Dane jest drzewo (każdy węzeł to „stan”), szukamy pierwszego węzła z etykietą X:



a) W jakiej kolejności odwiedzi węzły DFS (preorder), zakładając że zawsze idziesz najpierw w lewo? Ile wizyt do znalezienia X?

b) W jakiej kolejności odwiedzi węzły BFS? Ile wizyt do znalezienia X?

c) Która metoda ma tu mniejszy koszt i dlaczego?

Rozwiązanie.

a) DFS preorder (lewo przed prawym)

Kolejność: S, A, C, D, X, ...

Znalezienie X po wizytach: S[1], A[2], C[3], D[4], X[5], czyli potrzeba 5 wizyt.

b) BFS (poziomami)

Poziomami: S, A, B, C, D, E, F, X, ...

Znalezienie X po wizytach: S[1], A[2], B[3], C[4], D[5], E[6], F[7], X[8], zatem odnotowujemy aż 8 wizyt.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



c) Wniosek

Tu DFS wygrywa, bo cel X leży „głęboko, ale w lewym poddrzewie”, a DFS szybko schodzi w głąb. BFS jest korzystny, gdy spodziewasz się celu płytko (mały poziom)

Ćwiczenia samodzielne

Zadanie 9.1

Dane jest drzewo binarne:

A

/ \

B C

a) Podaj liczbę węzłów oraz liści.

b) Podaj wysokość drzewa.

c) Zapisz drzewo w postaci (klucz, lewy, prawy).

Zadanie 9.2

Dla drzewa:

A

/

B

/

C

a) Określ, czy jest to drzewo zdegenerowane.

b) Podaj jego wysokość.

c) Podaj liczbę liści.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 9.3

Dla drzewa:

```

1
 / \
2   3

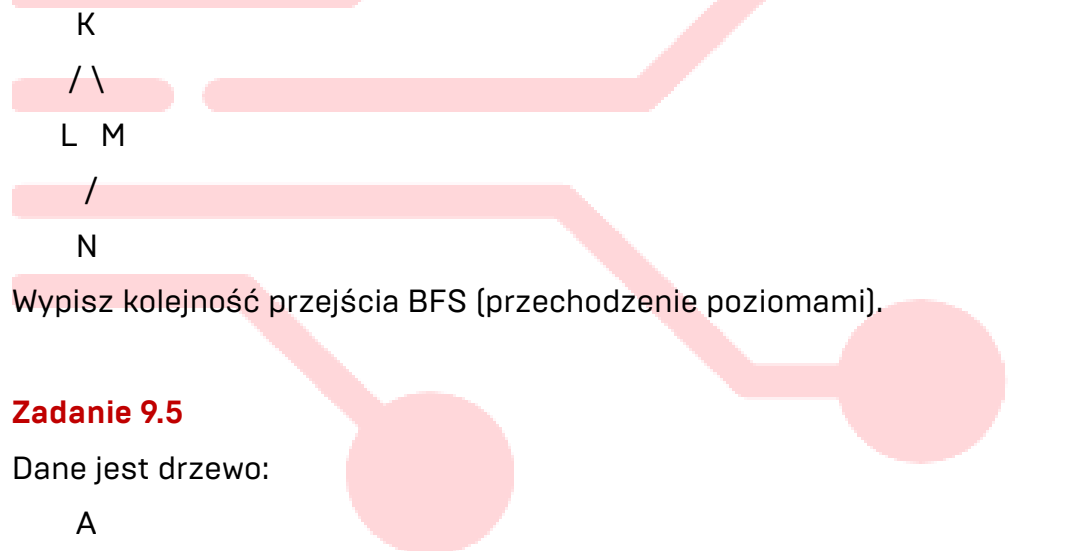
```

Wypisz kolejność węzłów dla:

- a) preorder
- b) inorder
- c) postorder

Zadanie 9.4

Dla drzewa:



Wypisz kolejność przejścia BFS (przechodzenie poziomami).

Zadanie 9.5

Dane jest drzewo:

```

A
 / \
B   C
 / \ /
D  E F

```

Wypisz kolejność:

- a) preorder



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- b) inorder
- c) postorder

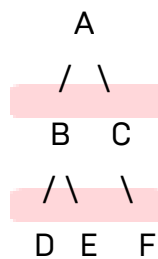
Zadanie 9.6

Dla drzewa z Zadania 9.5:

- a) Wypisz kolejność BFS.
- b) Podaj stan kolejki po każdym kroku algorytmu BFS.

Zadanie 9.7

Dla tego samego drzewa:



Podaj:

- a) liczbę węzłów odwiedzonych przez DFS preorder do momentu znalezienia węzła E,
- b) liczbę węzłów odwiedzonych przez BFS do momentu znalezienia węzła E.

Zadanie 9.8

Zbuduj BST, wstawiając kolejno klucze:

5, 2, 8.

- a) Narysuj drzewo końcowe.
- b) Podaj jego wysokość.
- c) Podaj inorder.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 9.9

Zbuduj BST przez wstawianie kluczy:

7, 4, 9, 1, 6.

- a) Narysuj drzewo.
- b) Wypisz inorder.
- c) Podaj liczbę liści.

Zadanie 9.10

Zbuduj BST dla ciągu:

10, 5, 15, 3, 7, 12.

- a) Narysuj drzewo.
- b) Podaj wysokość drzewa.
- c) Podaj węzły na poziomie 2 (korzeń na poziomie 0).

Zadanie 9.11

Dla BST zbudowanego z kluczy:

8, 3, 10, 1, 6, 14

- a) Podaj ścieżkę wyszukiwania klucza 6.
- b) Policz liczbę odwiedzonych węzłów.
- c) Czy wyszukiwanie zakończyło się sukcesem?

Zadanie 9.12

Dla tego samego BST [Zadanie 9.11]:

- a) Wykonaj wyszukiwanie klucza 2.
- b) Podaj liczbę porównań.
- c) W którym momencie algorytm kończy działanie?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 9.13

Dane są dwa BST zawierające klucze {1,2,3,4,5}:
jedno zbudowane przez wstawianie w kolejności rosnącej,
drugie zbudowane w kolejności: 3,1,5,2,4.

- Narysuj oba drzewa.
- Porównaj wysokości.
- Porównaj liczbę wizyt przy wyszukiwaniu klucza 4.

Zadanie 9.14

Dla BST:



Usuń klucz 3.

- Narysuj drzewo po usunięciu.
- Określ, który przypadek usuwania wystąpił.

Zadanie 9.15

Dla BST:



Usuń klucz 10.

- Narysuj drzewo wynikowe.
- Podaj, jak zmieniła się wysokość drzewa.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 9.16

Dla BST:

```

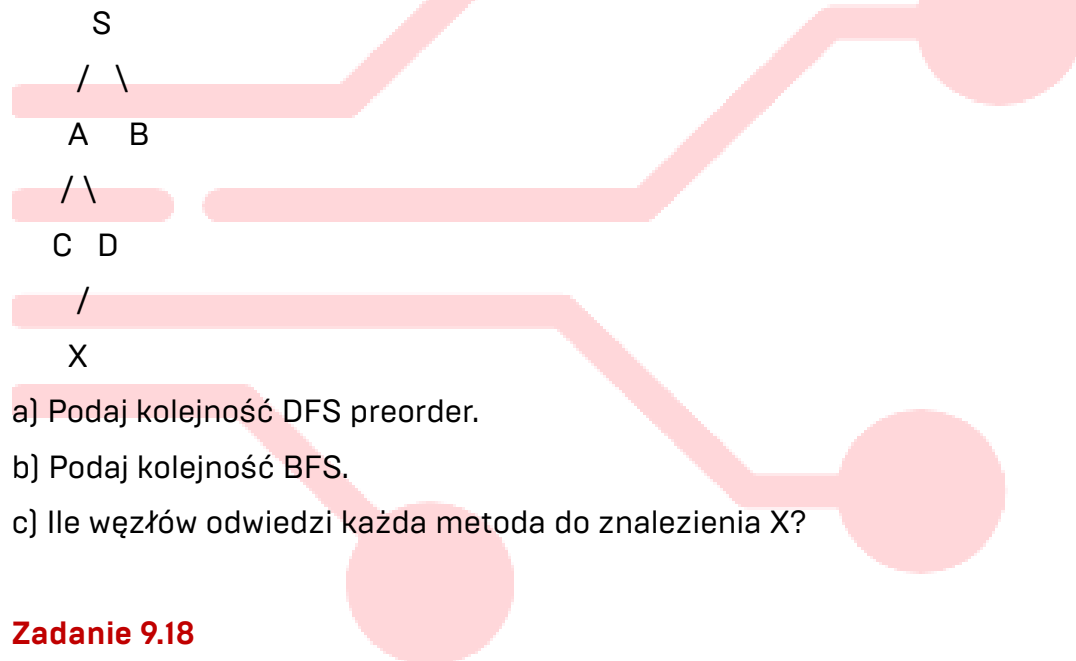
    6
   /\
  3  9
 /\  \
1  4 10

```

Usuń klucz 3, stosując następnik inorder.

Zadanie 9.17

Dane jest drzewo:



- Podaj kolejność DFS preorder.
- Podaj kolejność BFS.
- Ile węzłów odwiedzi każda metoda do znalezienia X?

Zadanie 9.18

Dla drzewa:

```

    R
   /\
  P  Q
   /
  X

```



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



a) Która metoda (DFS czy BFS) znajdzie X szybciej?

b) Uzasadnij odpowiedź, licząc odwiedzone węzły.

Zadanie 9.19

Dane są klucze: 1,2,3,4,5,6,7.

a) Zbuduj BST z minimalną możliwą wysokością.

b) Podaj jego wysokość.

c) Podaj maksymalną liczbę porównań przy wyszukiwaniu elementu.

Pytania pomocnicze

1. Czym różni się drzewo binarne od binarnego drzewa wyszukiwań?
2. Dlaczego inorder w BST generuje ciąg uporządkowany?
3. Od czego zależy koszt wyszukiwania w BST?
4. W jakich sytuacjach BFS jest lepszy od DFS?
5. Jakie są konsekwencje degeneracji BST?
6. Dlaczego usuwanie węzła z dwoma dziećmi jest bardziej złożone?

Podsumowanie

W trakcie ćwiczeń studenci poznali drzewa binarne jako fundamentalną strukturę matematyczno-algorytmiczną. Przećwiczano zarówno podstawowe operacje strukturalne, jak i algorytmy wyszukiwania oraz modyfikacji BST. Analiza liczby odwiedzonych węzłów pozwoliła empirycznie potwierdzić wpływ wysokości drzewa na efektywność algorytmów oraz zilustrować różnicę pomiędzy zachowaniem struktur zrównoważonych i zdegenerowanych.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.



Fundusze Europejskie
dla Rozwoju Społecznego

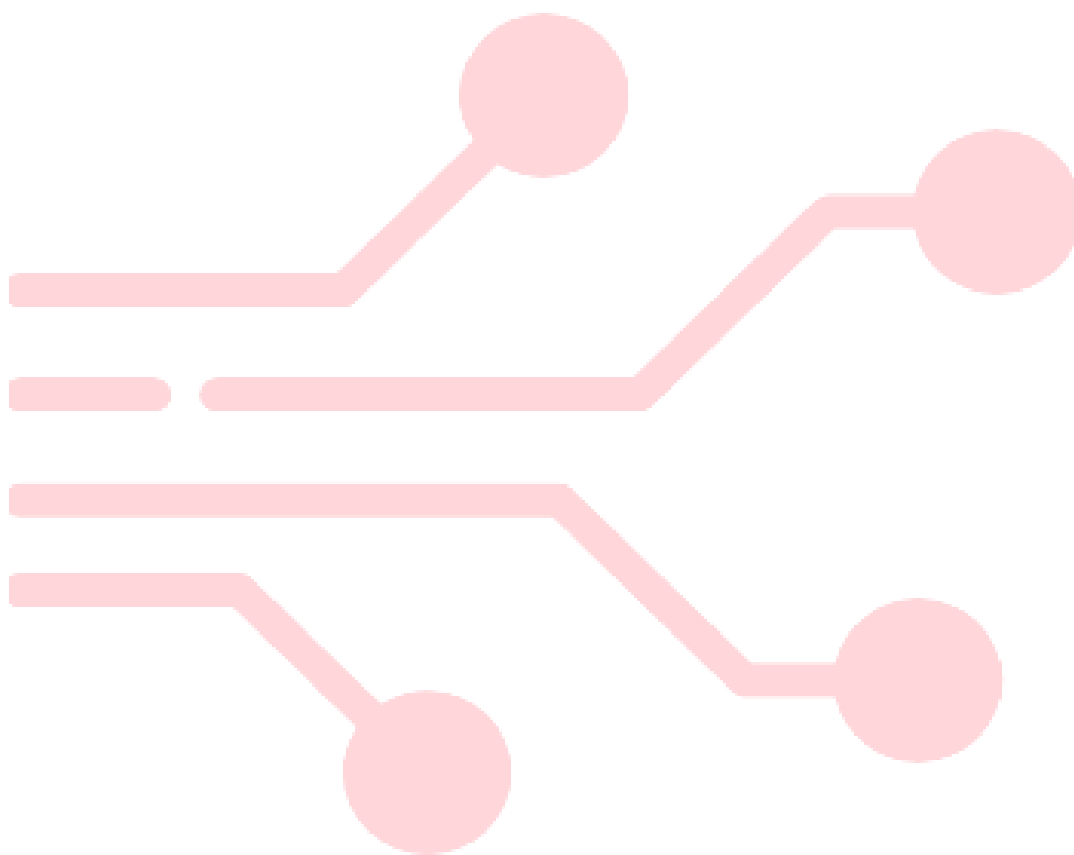


Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 10

Implementacja i analiza struktur matematycznych. Eksperymentalna weryfikacja twierdzeń matematyki dyskretnej

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



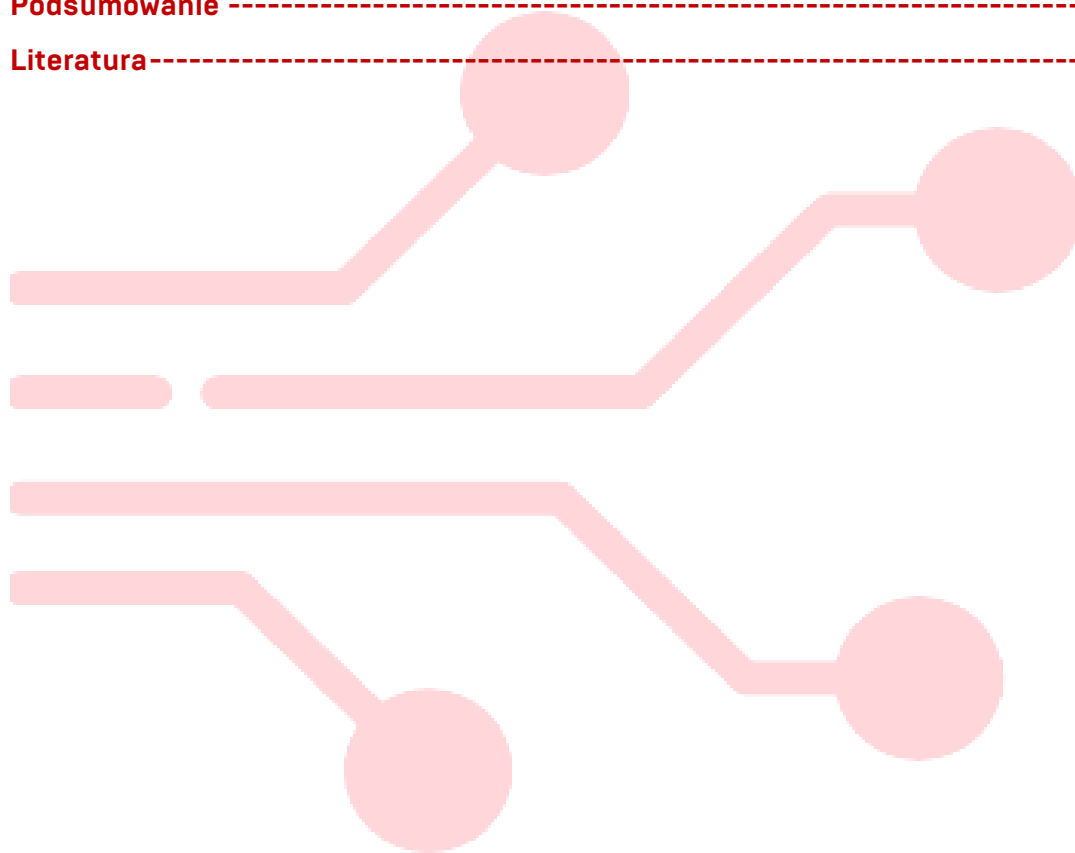
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć -----	155
Cel ćwiczenia/laboratorium -----	156
Instrukcja laboratoryjna/ćwiczeniowa -----	157
Ćwiczenia samodzielne -----	162
Pytania pomocnicze -----	164
Podsumowanie -----	165
Literatura -----	165



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Zbiory i operacje na zbiorach

Niech U będzie skończonym uniwersum

Dla zbiorów $A, B \subseteq U$ definiujemy:

$$A \cup B = \{x \in U: x \in A \vee x \in B\},$$

$$A \cap B = \{x \in U: x \in A \wedge x \in B\}.$$

Reprezentacja bitowa zbioru:

Jeśli $U = \{0, 1, \dots, n-1\}$, to zbiór $A \subseteq U$ reprezentujemy jako wektor bitowy długości n , gdzie:

$$\text{bit}_i = \begin{cases} 1 & \text{gdy } i \in A, \\ 0 & \text{gdy } i \notin A. \end{cases}$$

Przy takich założeniach

- suma zbiorów $\leftrightarrow$ operacja OR,
- część wspólna $\leftrightarrow$ operacja AND.

Relacje i ich własności

Relacja $R \subseteq X \times X$ jest:

- zwrotna, gdy $\forall x \in X: (x, x) \in R$,
- symetryczna, gdy $\forall x, y \in X: ((x, y) \in R \Rightarrow (y, x) \in R)$,
- przechodnia, gdy $\forall x, y, z \in X: ((x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R)$.

Macierz relacji M_R to macierz binarna, gdzie:

$$(M_R)_{ij} = \begin{cases} 1 & \text{gdy } (i, j) \in R, \\ 0 & \text{w przeciwnym razie.} \end{cases}$$

Domknięcie przechodnie R^+ to zbiór wszystkich par (x, y) , dla których istnieje ścieżka długości ≥ 1 pomiędzy liczbą x oraz liczbą y .



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Relacje równoważności

Relacja $\sim$ jest relacją równoważności, gdy jest zwrotna, symetryczna i przechodnia.

Dla $x \in X$ klasa abstrakcji:

$$[x] = \{y \in X : y \sim x\}.$$

Zbiór wszystkich klas abstrakcji oznaczamy przez $X/\sim$ i nazywamy zbiorem ilorazowym.

Zasada szufladkowa

Jeżeli n obiektów umieścimy w k szufladkach i $n > k$, to istnieje szufladka zawierająca co najmniej dwa obiekty.

Ciągi rekurencyjne i indukcja

Ciąg Fibonacciego:

$$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}.$$

Indukcja matematyczna:

- baza indukcyjna,
- krok indukcyjny: $P(n) \Rightarrow P(n+1)$.

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest utrwalenie i usystematyzowanie wiadomości zdobytych podczas poprzednich zajęć, w szczególności:

- powtórzenie kluczowych pojęć i metod omawianych we wcześniejszych ćwiczeniach,
- uporządkowanie zdobytej wiedzy w spójną całość,
- utrwalenie umiejętności rozwiązywania zadań z dotychczasowego zakresu materiału.

Ćwiczenia mają na celu zamknięcie pierwszej części materiału oraz przygotowanie do dalszych zagadnień z zakresu teorii liczb.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Instrukcja laboratoryjna/ćwiczeniowa

Przykład 10.1

Dane są zbiory w uniwersum $U = \{0,1,2,3,4,5,6,7\}$:

$A = \{0,1,3,6\}$, $B = \{1,2,3,5\}$, $C = \{3,4,5,6\}$.

Zaimplementuj operacje $\cup$, $\cap$ przez maski bitowe długości 8.

Oblicz obie strony tożsamości

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

i potwierdź równość.

Rozwiązanie.

Krok 1: kodowanie maską bitową.

Indeks bitu = element z U . Bit = 1, gdy element należy do zbioru.

$$A = \{0,1,3,6\} \Rightarrow A = 11010010 \text{ (od 0 do 7)}$$

$$B = \{1,2,3,5\} \Rightarrow B = 01110100$$

$$C = \{3,4,5,6\} \Rightarrow C = 00011110$$

Operacje bitowe $\cap$ = AND, $\cup$ = OR pozwalające na przeprowadzenie dowodu.

Krok 2: lewa strona $A \cup (B \cap C)$.

Najpierw obliczamy $B \cap C$ [AND]:

$$B = 01110100$$

$$C = 00011110$$

$$\text{AND} = 00010100 \Rightarrow B \cap C = \{3,5\}$$

Następnie obliczamy $A \cup (B \cap C)$ [OR]:

$$A = 11010010$$

$$B \cap C = 00010100$$

$$\text{OR} = 11010110 \Rightarrow \{0,1,3,5,6\}$$

Krok 3: prawa strona $(A \cup B) \cap (A \cup C)$.

Na początku obliczamy $A \cup B$ [OR]:

$$A = 11010010$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$B = 01110100$$

$$OR = 11110110 \Rightarrow \{0,1,2,3,5,6\}.$$

Następnie obliczamy $A \cup C$ (OR):

$$A = 11010010$$

$$C = 00011110$$

$$OR = 11011110 \Rightarrow \{0,1,3,4,5,6\}$$

Kończąc obliczamy AND:

$$\{0,1,2,3,5,6\} \cap \{0,1,3,4,5,6\} = \{0,1,3,5,6\}$$

Podsumowując zauważamy, że obie strony dają $\{0,1,3,5,6\}$, więc prawo rozdzielności potwierdzone eksperymentalnie na danych.

Przykład 10.2

Niech $X = \{1,2,3,4\}$. Dana relacja $R \subseteq X \times X$:

$$R = \{(1,2), (2,3), (3,4), (1,3)\}.$$

- Zapisz R jako macierz M_R 4×4 .
- Sprawdź, czy R jest przechodnia.
- Wyznacz domknięcie przechodnie R^+ .

Rozwiązanie.

Krok 1: macierz relacji. Wiersz = pierwszy element pary, kolumna = drugi.

$$M_R = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Krok 2:

Przechodniość: $(a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$.

Mamy $(1,2) \in R$ oraz $(2,3) \in R$, więc powinno być $(1,3) \in R$. Para $(1,3) \in R$ zatem warunek jest spełniony.

Mamy $(2,3) \in R$ oraz $(3,4) \in R$, więc powinno być $(2,4) \in R$. Niestety para ta nie należy do badanej relacji. Zatem R nie jest przechodnia.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Krok 3:

Wyznaczamy domknięcie przechodnie R^+ .

Wyznaczamy pary osiągalne ścieżką długości ≥ 1 .

Z liczby 1 osiągalne są liczby: $1 \rightarrow 2$, $1 \rightarrow 3$, a także $1 \rightarrow 4$ (bo $1 \rightarrow 3 \rightarrow 4$ lub $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$).

Z liczby 2 osiągalne są liczby: $2 \rightarrow 3$, $2 \rightarrow 4$ (bo $2 \rightarrow 3 \rightarrow 4$).

Z liczby 3 osiągalne są liczby: $3 \rightarrow 4$.

Z liczby 4 nie jest osiągalna żadna liczba, zatem

$$R^+ = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}.$$

Należy zauważyć, że brak jednej pary $(2,4)$ łamie przechodność, ale pojawia się ona w R^+ .

Przykład 10.3

Na zbiorze $A = \{0,1,2,3,4,5\}$ zdefiniujmy relację

$$x \sim y \Leftrightarrow x \equiv y \pmod{3}.$$

- Sprawdź, że jest to relacja równoważności.
- Wyznacz klasy abstrakcji i zbiór ilorazowy $A/\sim$.

Rozwiązanie.

Sprawdzamy, czy relacja $\sim$ jest relacją równoważności, w tym celu sprawdzamy zwrotność, symetrię oraz przechodność.

Zwrotność: relacja $x \equiv x \pmod{3}$ jest zawsze spełniona.

Symetria: jest oczywiste, że $x \equiv y \pmod{3} \Rightarrow y \equiv x \pmod{3}$.

Przechodność: $x \equiv y \pmod{3}$ oraz $y \equiv z \pmod{3} \Rightarrow x \equiv z \pmod{3}$ – jest to podstawowa własność kongruencji.

Wyznaczamy klasy abstrakcji w A oraz zbiór ilorazowy.

Reszty mod 3 wynoszą odpowiednio

$$[0] = \{0,3\}$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$[1] = \{1,4\}$$

$$[2] = \{2,5\}$$

Zatem

$$A/\sim = \{\{0,3\}, \{1,4\}, \{2,5\}\}.$$

Przykład 10.4

Dany jest graf nieskierowany G o wierzchołkach $V = \{1,2,3,4,5\}$ i krawędziach

$$E = \{\{1,2\}, \{1,3\}, \{2,3\}, \{2,4\}, \{3,5\}\}.$$

- Zapisz listy sąsiedztwa oraz oblicz stopnie wierzchołków.
- Sprawdź, czy zachodzi własność:

$$\sum_{v \in V} \deg(v) = 2 |E|.$$

Rozwiązanie.

Wyznaczamy listy sąsiedztwa oraz obliczamy stopnie poszczególnych wierzchołków.

Dla wierzchołka 1 sąsiadami są wierzchołki $\{2,3\}$ stąd $\deg(1) = 2$.

Podobnie dla pozostałych wierzchołków:

$$2: \{1,3,4\} \rightarrow \deg(2) = 3$$

$$3: \{1,2,5\} \rightarrow \deg(3) = 3$$

$$4: \{2\} \rightarrow \deg(4) = 1$$

$$5: \{3\} \rightarrow \deg(5) = 1$$

Sprawdzamy, czy spełniona jest własność $\sum_{v \in V} \deg(v) = 2 |E|$.

Na początku stwierdzamy, że suma stopni: $2 + 3 + 3 + 1 + 1 = 10$.

Następnie zauważamy, że $|E| = 5$, więc $2 |E| = 10$.

Zatem równość zachodzi.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 10.6

Mamy 9 liczb całkowitych:

$$a = \{2, 5, 7, 11, 14, 17, 20, 23, 26\}.$$

Pokaż, że istnieją dwie liczby o tej samej reszcie z dzielenia przez 4.

Rozwiązanie.

Na wstępie zauważmy, że reszty mod 4 to tylko: 0, 1, 2, 3. Mamy zatem 4 szufladki. Z drugiej strony mamy 9 liczb. Jeśli rozdzielimy 9 obiektów do 4 szufladek, któraś szufladka ma co najmniej $\lceil 9/4 \rceil = 3$ elementy, więc na pewno są co najmniej dwie z tą samą resztą.

Sprawdźmy to obliczając wszystkie reszty mod 4:

$$2 \equiv 2$$

$$5 \equiv 1$$

$$7 \equiv 3$$

$$11 \equiv 3$$

$$14 \equiv 2$$

$$17 \equiv 1$$

$$20 \equiv 0$$

$$23 \equiv 3$$

$$26 \equiv 2$$

Widzimy np. reszta 3 jest osiągalna dla 3 liczb (7, 11, 23), reszta 2 jest również osiągalna dla 3 liczb: (2, 14, 26), reszta 1 jest osiągalna dla dwóch liczb: (5, 17).

Przykład 10.7

Niech $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$.

Oblicz iteracyjnie $F_2, \dots, F_{10}$.

Udowodnij, że



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$\sum_{k=0}^n F_k = F_{n+2} - 1$$

Rozwiązanie.

Wypisujemy początkowe wyrazy ciągu:

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

Badana teza ma postać: $P(n): \sum_{k=0}^n F_k = F_{n+2} - 1$

Zgodnie z zasadą indukcji sprawdzamy, czy własność jest prawdziwa dla $n = 0$:

$F_0 = 0$, natomiast $F_2 - 1 = 1 - 1 = 0$.

Teraz sprawdzamy krok indukcyjny. Zakładamy prawdziwość $P(n)$. Wówczas

$$\sum_{k=0}^{n+1} F_k = \left(\sum_{k=0}^n F_k \right) + F_{n+1} = (F_{n+2} - 1) + F_{n+1} = F_{n+3} - 1,$$

bo $F_{n+3} = F_{n+2} + F_{n+1}$.

Zatem $P(n+1)$ jest prawdziwe. Na mocy zasady indukcji matematycznej stwierdzamy, że badana własność jest prawdziwa dla dowolnego n .

Ćwiczenia samodzielne

Zadanie 10.1

Dane jest uniwersum $U = \{0,1,2,3,4,5,6,7\}$ oraz zbiory

$A = \{0,2,4,7\}$, $B = \{1,2,3,7\}$, $C = \{2,5,6,7\}$.

Zakoduj zbiory jako maski bitowe długości 8 (bit i oznacza przynależność elementu i). Następnie oblicz obie strony i sprawdź równość:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Zadanie 10.2

Niech $X = \{1,2,3,4,5\}$. Dana relacja:

$$R = \{(1,2), (2,3), (3,5), (1,3), (2,5)\} \subseteq X \times X.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zapisz R jako macierz M_R . Sprawdź, czy relacja jest przechodnia. Jeśli nie jest, podaj najmniejszy (w sensie liczby dodanych par) zbiór par, który trzeba dodać, by otrzymać relację przechodnią.

Zadanie 10.3

Na zbiorze $A = \{0,1,2,3,4,5,6,7,8\}$ zdefiniuj relację:

$$x \sim y \Leftrightarrow x \equiv y \pmod{4}.$$

Sprawdź, czy $\sim$ jest relacją równoważności. Wyznacz wszystkie klasy abstrakcji oraz zbiór ilorazowy $A/\sim$.

Zadanie 10.4

Wykonaj algorytm Euklidesa dla NWD (924,396). Zapisz wszystkie kroki dzielenia z resztą. Następnie odpowiedz:

- ile iteracji wykonał algorytm,
- jaką wartość ma NWD (924,396),

Zadanie 10.5

Dany jest graf nieskierowany G o wierzchołkach $V = \{1,2,3,4,5,6\}$ oraz krawędziach:

$$E = \{\{1,2\}, \{1,3\}, \{2,3\}, \{2,4\}, \{4,5\}, \{4,6\}, \{5,6\}\}.$$

Zapisz listy sąsiedztwa oraz stopnie wszystkich wierzchołków. Zweryfikuj na tym grafie twierdzenie:

$$\sum_{v \in V} \deg(v) = 2 |E|.$$

Zadanie 10.6

Mamy 11 liczb całkowitych:

$$\{3,6,10,15,18,22,27,31,35,39,43\}.$$

- Udowodnij (zasada szufladkowa), że istnieją dwie liczby o tej samej reszcie z dzielenia przez 5.
- Wskaż konkretną parę (lub kilka par) o tej samej reszcie.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 10.7

Dla $n \in \mathbb{N}$ zdefiniujmy funkcję:

$$s(n) = \{\text{suma cyfr liczby } n \text{ w zapisie dziesiętnym}\}.$$

Dla liczb $n \in \{1, 2, \dots, 30\}$ policz wartości $s(n)$ oraz sprawdź, czy prawdziwa jest teza:

$$n \equiv s(n) \pmod{9}.$$

Zadanie 10.8

Niech $A = \{a, b, c, d\}$. Zaimplementuj na papierze funkcję $f: \mathcal{P}(A) \rightarrow \{0, 1\}^4$, która każdemu podzbirowi przypisuje wektor bitowy obecności elementów (w ustalonej kolejności a, b, c, d).

Następnie:

- wypisz wszystkie elementy $\mathcal{P}(A)$ w tej reprezentacji,
- policz $|\mathcal{P}(A)|$ oraz porównaj z $2^{|A|}$,
- wskaż, jak wygląda operacja $\cup$ oraz $\cap$ na wektorach bitowych.

Zadanie 10.9

Niech $X = \{1, 2, 3, 4\}$. Dana jest relacja $R \subseteq X \times X$:

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 4), (1, 4)\}.$$

- Sprawdź, czy R jest porządkiem częściowym (zwrotność, antysymetria, przechodniość).
- Jeśli tak, narysuj diagram Hassego.
- Wyznacz elementy minimalne, maksymalne oraz (jeśli istnieją) element najmniejszy i największy.

Pytania pomocnicze

1. Jakie są zalety reprezentacji zbiorów i relacji w postaci struktur binarnych?
2. Dlaczego domknięcie przechodnie relacji odpowiada pojęciu osiągalności w grafie?
3. Na czym polega rola niezmiennika w dowodzeniu poprawności algorytmu?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



4. Dlaczego eksperymentalna weryfikacja twierdzeń nie zastępuje dowodu, ale jest użyteczna dydaktycznie?

Podsumowanie

W trakcie ćwiczenia pokazano, że struktury matematyki dyskretnej mogą być nie tylko formalnie definiowane, ale również implementowane i analizowane obliczeniowo. Eksperymentalne sprawdzanie własności na skończonych danych pozwala lepiej zrozumieć sens twierdzeń matematycznych i przygotowuje grunt pod analizę algorytmów w informatyce.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 11

Algorytmy podzielności i testowania pierwszości. Implementacja metod faktoryzacji liczb. Eksperymentalna analiza podzielności liczb

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



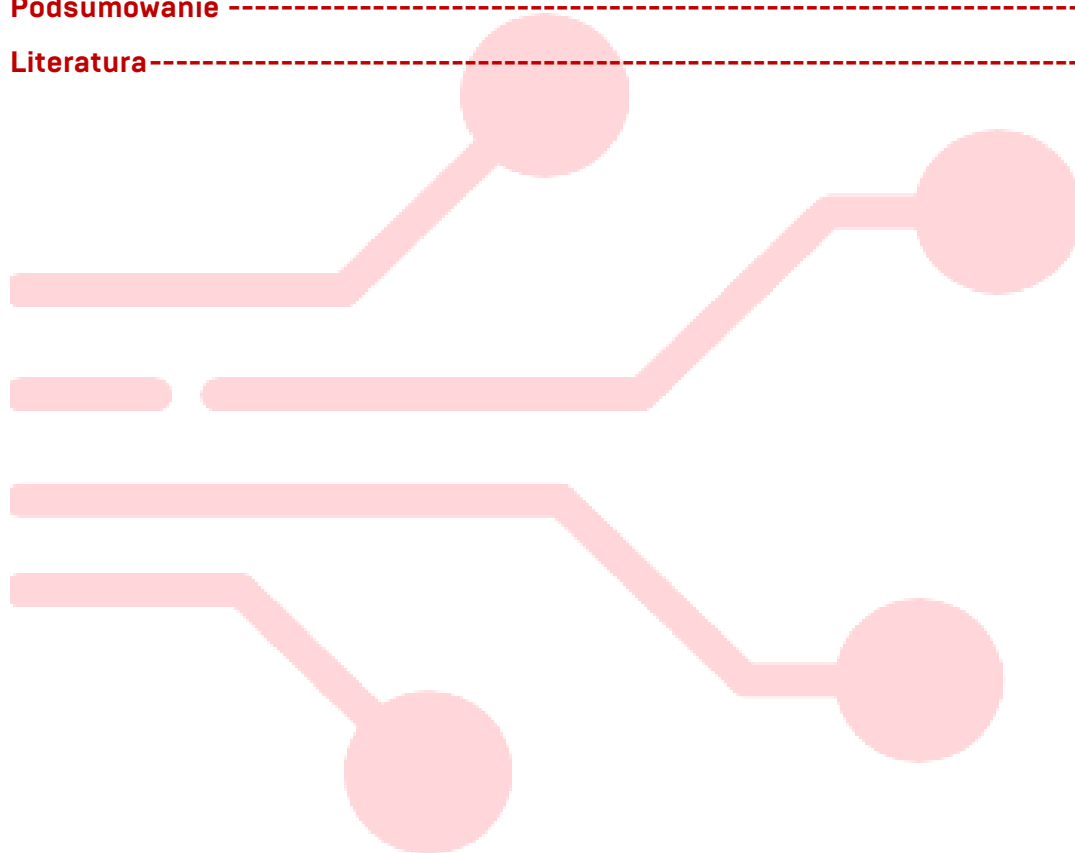
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	168
Cel ćwiczenia/laboratorium	171
Instrukcja laboratoryjna/ćwiczeniowa	171
Ćwiczenia samodzielne	176
Pytania pomocnicze	178
Podsumowanie	179
Literatura	179



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Podzielność liczb

Dla liczb całkowitych a, b , gdzie $a \neq 0$, mówimy, że

$$a \mid b \Leftrightarrow \exists k \in \mathbb{Z}: b = a \cdot k$$

Największy wspólny dzielnik (NWD)

Dla $a, b \in \mathbb{Z}$, różnych od zera, największym wspólnym dzielnikiem liczb a i b , oznaczanym przez

$$\text{NWD}(a, b),$$

nazywamy największą dodatnią liczbę całkowitą, która dzieli jednocześnie a i b .

Własności NWD

Dla dowolnych liczb całkowitych a, b, c zachodzą następujące własności:

$$\text{NWD}(a, b) = \text{NWD}(b, a)$$

$$\text{NWD}(a, 0) = |a|$$

$$\text{NWD}(a, b) = \text{NWD}(b, a \bmod b)$$

$$\text{NWD}(a, b) \mid a \text{ oraz } \text{NWD}(a, b) \mid b$$

$$\text{Jeśli } d \mid a \text{ oraz } d \mid b, \text{ to } d \mid \text{NWD}(a, b)$$

Algorytm Euklidesa

Algorytm Euklidesa opiera się na tożsamości:

$$\text{NWD}(a, b) = \text{NWD}(b, a \bmod b)$$

Procedura wyznaczania NWD:

Dla $a > b > 0$ obliczamy resztę z dzielenia $a \bmod b$,

- Zastępujemy parę (a, b) przez $(b, a \bmod b)$,



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- Powtarzamy ten krok, aż reszta z dzielenia wyniesie 0,
- Ostatnia niezerowa reszta jest równa NWD.

NWD wielu liczb

Dla $a_1, a_2, \dots, a_n$:

$$\text{NWD}(a_1, a_2, \dots, a_n) = \text{NWD}(\text{NWD}(a_1, a_2), a_3, \dots, a_n)$$

Liczby pierwsze

Liczbę naturalną $n > 1$ nazywamy liczbą pierwszą, jeżeli jedynymi dodatnimi dzielnikami liczby n są 1 oraz n .

Jeżeli liczba $n > 1$ nie jest pierwsza, to liczbę taką nazywamy ją złożoną.

Jeżeli liczba $n > 1$ jest złożona, to posiada dzielnik d taki, że:

$$2 \leq d \leq \sqrt{n}$$

Deterministyczne testy pierwszości

Aby sprawdzić, czy n jest pierwsza:

- Sprawdzamy, czy n dzieli się przez kolejne liczby naturalne
- $2, 3, 4, \dots, [\sqrt{n}]$
- Wystarczy sprawdzać liczby pierwsze.
- Jeśli żadna z nich nie dzieli n , to n jest pierwsza.

Test pierwszości z użyciem NWD

Jeżeli istnieje liczba k , taka że:

$$1 < \text{NWD}(n, k) < n,$$

to liczba n jest złożona.

Twierdzenie o jednoznaczności rozkładu

Każdą liczbę naturalną $n > 1$ można zapisać w postaci iloczynu liczb pierwszych:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

gdzie p_i są różnymi liczbami pierwszymi, a wykładniki $\alpha_i \geq 1$ są liczbami naturalnymi.

Rozkład ten jest jednoznaczny z dokładnością do kolejności czynników.

Faktoryzacja przez próbne dzielenie

Procedura:

- Dzielimy n przez kolejne liczby pierwsze 2,3,5,7, ...,
- Każdy znaleziony dzielnik zapisujemy,
- Dzielimy dalej otrzymany iloraz,
- Kończymy, gdy pozostała liczba jest równa 1 lub jest pierwsza.

Faktoryzacja z użyciem NWD

Jeżeli znamy liczbę k , dla której:

$$\text{NWD}(n, k) > 1,$$

to znaleźliśmy nietrywialny dzielnik n , który można dalej rozkładać.

Eksperymentalne sprawdzanie pierwszości

Sito Eratostenesa służy do wyznaczania wszystkich liczb pierwszych mniejszych od danej liczby N .

Algorytm sita Eratostenesa

- Tworzymy listę liczb od 2 do N ,
- Wybieramy najmniejszą niewykreśloną liczbę p (na początku $p = 2$),
- Wykreślamy wszystkie wielokrotności p większe od p ,
- Powtarzamy dla kolejnych niewykreślonych liczb $p \leq \sqrt{N}$,
- Pozostałe liczby są pierwsze.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Cel ćwiczenia/laboratorium

Celem ćwiczenia jest zapoznanie studentów z podstawowymi algorytmami teorii liczb wykorzystywanymi w matematyce dyskretniej oraz informatyce. W szczególności celem laboratorium jest:

- nabycie umiejętności wyznaczania największego wspólnego dzielnika liczb całkowitych z wykorzystaniem algorytmu Euklidesa,
- zrozumienie pojęcia liczby pierwszej oraz własności liczb złożonych,
- poznanie deterministycznych metod testowania pierwszości liczb naturalnych,
- opanowanie technik rozkładu liczb naturalnych na czynniki pierwsze,
- zapoznanie się z ideą eksperymentalnego sprawdzania pierwszości liczb za pomocą sita Eratostenesa,
- rozwijanie umiejętności analizy poprawności i efektywności prostych algorytmów arytmetycznych.

Realizacja ćwiczenia ma na celu także przygotowanie studentów do dalszych zagadnień związanych z algorytmami kryptograficznymi oraz teorią obliczeń.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 11.1

Wyznacz $NWD(252, 105)$.

Rozwiązanie.

Postępujemy zgodnie z algorytmem Euklidesa

$$252 = 2 \cdot 105 + 42$$

$$105 = 2 \cdot 42 + 21$$

$$42 = 2 \cdot 21 + 0$$

Kończymy rozkład otrzymując wynik

$$NWD(252, 105) = 21.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 11.2.

Wyznacz $NWD(1001, 143)$.

Rozwiązanie.

Ponownie wykorzystujemy algorytm Euklidesa.

$$1001 = 7 \cdot 143 + 0$$

Już po pierwszym kroku otrzymujemy wynik:

$$NWD(1001, 143) = 143$$

Przykład 11.3.

Wyznacz $NWD(360, 840, 1320)$.

Rozwiązanie.

Korzystamy z własności NWD dla wielu liczb. Na początku wyznaczamy NWD dwóch pierwszych liczb:

$$NWD(360, 840)$$

$$840 = 2 \cdot 360 + 120$$

$$360 = 3 \cdot 120 + 0 \Rightarrow NWD(360, 840) = 120$$

Następnie obliczamy NWD dla otrzymanej wartości oraz trzeciej liczby:

$$NWD(120, 1320)$$

$$1320 = 11 \cdot 120 + 0$$

Ostatecznie wynik końcowy wynosi:

$$NWD(360, 840, 1320) = 120$$

Przykład 11.4

Sprawdź, czy liczba $n = 97$ jest pierwsza.

Rozwiązanie.

Zauważmy, że

$$\sqrt{97} \approx 9,8$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



W związku z tym sprawdzamy jedynie dzielniki pierwsze mniejsze od wyznaczonego pierwiastka: 2,3,5,7

$$97 \bmod 2 \neq 0,$$

$$97 \bmod 3 \neq 0,$$

$$97 \bmod 5 \neq 0,$$

$$97 \bmod 7 \neq 0$$

Ponieważ żadna liczba pierwsza mniejsza od pierwiastka z 97 nie dzieli badanej liczby jest ona liczbą pierwszą.

Przykład 11.5

Sprawdź, czy liczba $n = 221$ jest pierwsza.

Rozwiązanie.

Ponownie obliczamy pierwiastek z badanej liczby

$$\sqrt{221} \approx 14,8$$

Następnie zauważamy, że

$$221 \bmod 13 = 0 \Rightarrow 221 = 13 \cdot 17$$

Zatem liczba 221 nie jest pierwsza.

Przykład 11.6

Sprawdź, czy liczba $n = 143$ jest pierwsza.

Rozwiązanie.

Na wstępie zauważmy, że

$$\text{NWD}(143, 11) = 11 > 1$$

Zatem należy stwierdzić, że liczba 143 nie jest pierwsza.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 11.7

Sprawdź, czy liczba $n = 101$ jest pierwsza.

Rozwiązanie.

$$\sqrt{101} < 11$$

Sprawdzamy NWD $(101, k)$ dla każdego $k = 2, \dots, 10$:

$$\text{NWD}(101, 2) = 1$$

$$\text{NWD}(101, 3) = 1$$

$$\text{NWD}(101, 4) = 1$$

$$\text{NWD}(101, 5) = 1$$

$$\text{NWD}(101, 6) = 1$$

$$\text{NWD}(101, 7) = 1$$

$$\text{NWD}(101, 8) = 1$$

$$\text{NWD}(101, 9) = 1$$

$$\text{NWD}(101, 10) = 1$$

Ponieważ dla wszystkich sprawdzonych liczb NWD wynosi jeden stwierdzamy, że liczba 101 jest pierwsza.

Przykład 11.8

Rozłóż liczbę 756 na czynniki pierwsze.

Rozwiązanie.

Zaczynamy od najmniejszych liczb pierwszych:

$$756 = 2 \cdot 378$$

$$378 = 2 \cdot 189$$

$$189 = 3 \cdot 63$$

$$63 = 3 \cdot 21$$

$$21 = 3 \cdot 7$$

Mamy zatem rozkład

$$756 = 2^2 \cdot 3^3 \cdot 7$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 11.9

Rozłóż liczbę $n = 8051$, wiedząc że

$$\text{NWD}(8051, 97) > 1$$

Rozwiązanie.

Opierając się na wskazówce zauważamy, że

$$\text{NWD}(8051, 97) = 97$$

$$8051 = 97 \cdot 83$$

Obie wartości są liczbami pierwszymi, zatem poszukiwany rozkład ma postać:

$$8051 = 97 \cdot 83$$

Przykład 11.10

Wyznacz wszystkie liczby pierwsze mniejsze od 50 metodą sita Eratostenesa.

Rozwiązanie.

Zaczynamy od liczb 2, ..., 49.

- wykreślamy wielokrotności 2 (oprócz 2),
- wykreślamy wielokrotności 3 (oprócz 3),
- wykreślamy wielokrotności 5,
- wykreślamy wielokrotności 7.

Ponieważ $8 > \sqrt{50}$ kończymy poszukiwania.

Pozostałe liczby są liczbami pierwszymi:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

Przykład 11.11

Ile liczb pierwszych znajduje się w przedziale $[1, 200]$?

Rozwiązanie

- Stosujemy sito Eratostenesa do 200, wykreślając wielokrotności liczb pierwszych $\leq \sqrt{200}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



- Po zakończeniu sita pozostaje 46 liczb pierwszych.
Zatem w przedziale $[1, 200]$ znajduje się 46 liczb pierwszych.

Ćwiczenia samodzielne

Zadanie 11.1

Wyznacz NWD(420,294) za pomocą algorytmu Euklidesa.

Zadanie 11.2.

Wyznacz NWD(1024,640).

Zadanie 11.3.

Wyznacz NWD(891,594).

Zadanie 11.4.

Wyznacz NWD(756,1050).

Zadanie 11.5.

Wyznacz NWD(540,810,1260).

Zadanie 11.6.

Wyznacz NWD(1001,143,77).

Zadanie 11.7.

Sprawdź, czy liczba 97 jest pierwsza, stosując test do $\sqrt{n}$.

Zadanie 11.8.

Sprawdź, czy liczba 169 jest pierwsza.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 11.9.

Sprawdź, czy liczba 221 jest pierwsza.

Zadanie 11.10.

Sprawdź, czy liczba 289 jest pierwsza.

Zadanie 11.11.

Sprawdź, czy liczba 391 jest pierwsza.

Zadanie 11.12.

Sprawdź, czy liczba 437 jest pierwsza, wykorzystując obliczenia NWD z wybranymi dzielnikami.

Zadanie 11.13.

Rozłóż liczbę 360 na czynniki pierwsze.

Zadanie 11.14.

Rozłóż liczbę 924 na czynniki pierwsze.

Zadanie 11.15.

Rozłóż liczbę 1001 na czynniki pierwsze.

Zadanie 11.16.

Rozłóż liczbę 1155 na czynniki pierwsze.

Zadanie 11.17.

Rozłóż liczbę 2024 na czynniki pierwsze.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 11.18.

Zastosuj sito Eratostenesa w celu wyznaczenia wszystkich liczb pierwszych mniejszych od 100.

Zadanie 11.19.

Ile liczb pierwszych znajduje się w przedziale $[1,300]$? Odpowiedź uzasadnij eksperymentalnie, stosując sito Eratostenesa.

Zadanie 11.20.

Korzystając z sita Eratostenesa, sprawdź, ile liczb pierwszych znajduje się w przedziale $[100,500]$.

Pytania pomocnicze

1. Na czym polega algorytm Euklidesa i dlaczego jest on efektywny obliczeniowo?
2. Dlaczego w algorytmie Euklidesa parę (a, b) można zastąpić parą $(b, a \bmod b)$ bez zmiany wartości NWD?
3. Dlaczego do sprawdzenia pierwszości liczby n wystarczy badać dzielniki nie większe niż $\sqrt{n}$?
4. W jaki sposób obliczanie NWD może pomóc w wykrywaniu liczb złożonych?
5. Na czym polega twierdzenie o jednoznaczności rozkładu liczb naturalnych?
6. Dlaczego faktoryzacja przez próbne dzielenie jest algorytmem nieefektywnym dla dużych liczb?
7. Jak działa sito Eratostenesa i czym różni się od testowania pierwszości pojedynczej liczby?
8. Jakie są zalety i ograniczenia metod eksperymentalnych w testowaniu pierwszości?
9. Jakie znaczenie praktyczne mają algorytmy NWD i testy pierwszości w informatyce?
10. W jaki sposób omawiane algorytmy mogą być wykorzystane w kryptografii?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Podsumowanie

W trakcie ćwiczeń zaprezentowano podstawowe algorytmy teorii liczb związane z podzielnością, wyznaczaniem największego wspólnego dzielnika, testowaniem pierwszości oraz faktoryzacją liczb naturalnych. Studenci poznali algorytm Euklidesa jako efektywną metodę obliczania NWD oraz wykorzystali jego własności w analizie pierwszości liczb.

Omówiono deterministyczne testy pierwszości oraz ich ograniczenia obliczeniowe, a także przedstawiono ideę faktoryzacji liczb naturalnych. Zastosowanie sita Eratostenesa umożliwiło eksperymentalne wyznaczanie zbiorów liczb pierwszych i analizę ich rozmieszczenia w zadanych przedziałach.

Zdobyta wiedza i umiejętności stanowią istotny element przygotowania do dalszych zagadnień z zakresu matematyki dyskretnej, algorytmiki oraz kryptografii, gdzie efektywne operacje na liczbach naturalnych odgrywają kluczową rolę.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 12

Operacje modularne i ich zastosowanie.

Implementacja twierdzenia Eulera i

rozwiązywanie równań kongruencyjnych.

Algorytmy obliczania odwrotności modularnej

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



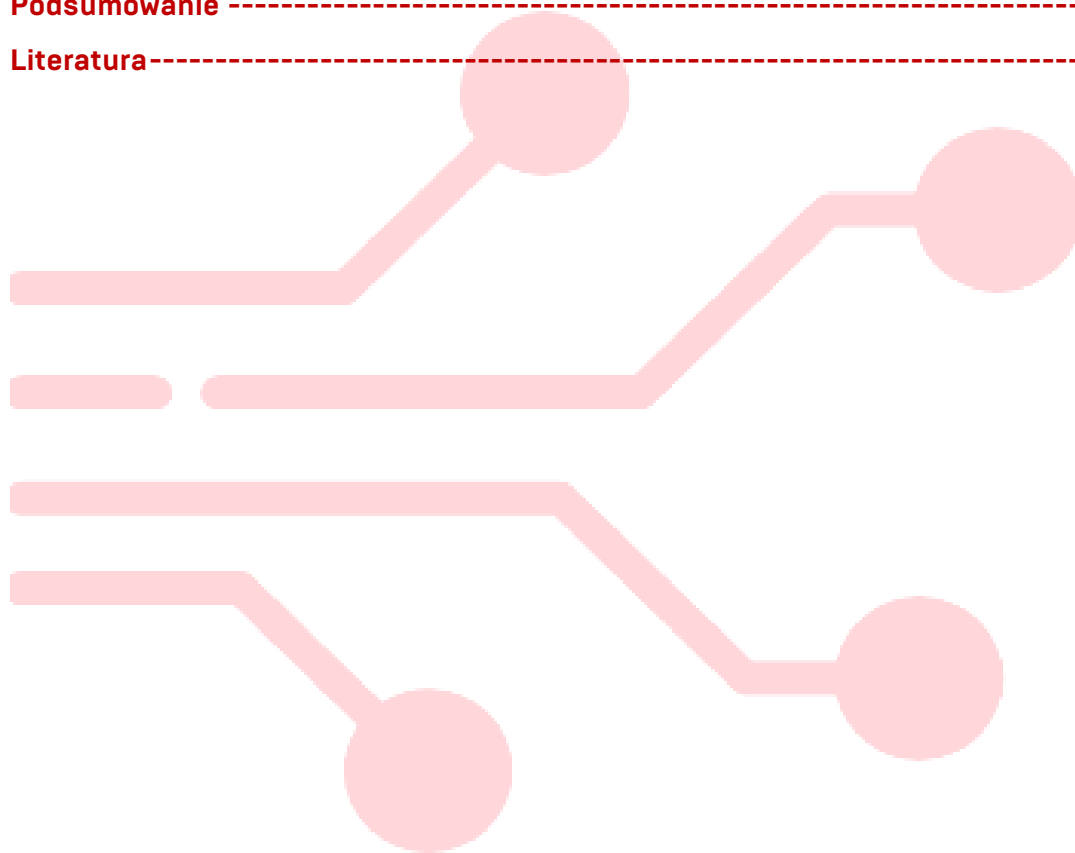
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	182
Cel ćwiczenia/laboratorium	183
Instrukcja laboratoryjna/ćwiczeniowa	184
Ćwiczenia samodzielne	188
Pytania pomocnicze	194
Podsumowanie	195
Literatura	196



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Projekt współfinansowany ze środków Unii Europejskiej w ramach: FUNDUSZE EUROPEJSKIE DLA ROZWOJU SPOŁECZNEGO 2021-2027 (FERS) "POLLUB z nami nowoczesne technologie" FERS.01.05-IP.08-0319/23-00

Wprowadzenie, tematyka zajęć

Kongruencje i arytmetyka modularna

Dla liczb całkowitych a, b oraz $n \geq 1$:

$$a \equiv b \pmod{n}$$

jeżeli

$$n \mid (a - b)$$

Własności kongruencji

Jeśli $a \equiv b \pmod{n}$ oraz $c \equiv d \pmod{n}$, to:

- $a + c \equiv b + d \pmod{n}$
- $a - c \equiv b - d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^k \equiv b^k \pmod{n}$ dla $k \in \mathbb{N}$

Potęgowanie modularne i okresy

Redukcja wykładnika

Jeżeli potęgi liczby a modulo n tworzą cykl (co zawsze zachodzi), to:

$$a^k \equiv a^{k \bmod t} \pmod{n},$$

gdzie t – długość okresu.

Funkcja Eulera $\varphi(n)$

$$\varphi(n) = \{1 \leq k \leq n: \gcd(k, n) = 1\}$$

Wzory:

- Jeżeli p jest liczbą pierwszą:

$$\varphi(p) = p - 1$$

- Jeżeli p^k :

$$\varphi(p^k) = p^k - p^{k-1}$$

- Jeżeli n jest liczbą złożoną postaci $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$:



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

Twierdzenie Eulera

Jeżeli $\text{NWD}(a, n) = 1$, to:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Wniosek:

$$a^k \equiv a^{k \bmod \varphi(n)} \pmod{n} \quad \text{dla } k \geq \varphi(n)$$

Odwrotność modularna

Liczba a^{-1} jest odwrotnością modularną a modulo n , jeżeli:

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

Warunek konieczny i dostateczny :

$$a^{-1} \text{ istnieje} \Leftrightarrow \text{NWD}(a, n) = 1$$

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest zapoznanie studentów z podstawowymi metodami arytmetyki modularnej oraz nabycie umiejętności praktycznego stosowania pojęcia kongruencji w obliczeniach. W szczególności ćwiczenia mają na celu:

- opanowanie rachunków w arytmetyce modularnej, w tym redukcji liczb i wykładników modulo n ,
- zrozumienie i stosowanie twierdzenia Eulera w obliczeniach potęg modularnych,
- nabycie umiejętności rozwiązywania równań kongruencyjnych liniowych wraz z analizą istnienia i liczby rozwiązań,
- opanowanie algorytmów wyznaczania odwrotności modularnej, w szczególności rozszerzonego algorytmu Euklidesa,
- zastosowanie odwrotności modularnej w rozwiązywaniu równań kongruencyjnych oraz układów kongruencji,
- zapoznanie się z chińskim twierdzeniem o resztach jako narzędziem do rozwiązywania układów kongruencji.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Instrukcja laboratoryjna/ćwiczeniowa

Przykład 12.1

Obliczyć $7^{222} \pmod{10}$.

Rozwiązanie.

Rozpatrzmy cykl potęg modulo 10:

$$\begin{aligned}7^1 &\equiv 7, \\7^2 &= 49 \equiv 9 \pmod{10}, \\7^3 &\equiv 9 \cdot 7 = 63 \equiv 3 \pmod{10}, \\7^4 &\equiv 3 \cdot 7 = 21 \equiv 1 \pmod{10}.\end{aligned}$$

Okres wynosi 4, więc

$$7^{222} \equiv 7^{222 \bmod 4} = 7^2 \equiv 9 \pmod{10}.$$

Szukana wartość wynosi 9.

Przykład 12.2

Obliczyć $3^{1234} \pmod{35}$.

Rozwiązanie.

Obliczamy wartość funkcji Eulera

$$\varphi(35) = \varphi(5 \cdot 7) = 35 \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24.$$

Ponieważ $\text{NWD}(3, 35) = 1$, z twierdzenia Eulera mamy:

$$3^{24} \equiv 1 \pmod{35}.$$

Redukujemy wykładnik otrzymujemy:

$$1234 = 24 \cdot 51 + 10 \Rightarrow 3^{1234} \equiv 3^{10} \pmod{35}.$$

Następnie obliczamy 3^{10} :

$$3^2 = 9, 3^4 = 81 \equiv 11, 3^8 \equiv 11^2 = 121 \equiv 16 \pmod{35}.$$

$$3^{10} = 3^8 \cdot 3^2 \equiv 16 \cdot 9 = 144 \equiv 4 \pmod{35}.$$

Szukana wartość wynosi 4.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 12.3

Rozwiązać:

$$14x \equiv 8 \pmod{22}.$$

Rozwiązanie.

Ponieważ $NWD(14, 22) = 2$. Warunek istnienia rozwiązań: $2 \mid 8$ jest spełniony.

Dzielimy równanie przez 2:

$$7x \equiv 4 \pmod{11}.$$

Teraz $NWD(7, 11) = 1$, więc istnieje odwrotność:

$$7^{-1} \pmod{11}$$

Szukamy 7^{-1} :

$$7 \cdot 8 = 56 \equiv 1 \pmod{11},$$

bo 55 jest wielokrotnością 11.

Mnożymy równanie przez 8:

$$x \equiv 4 \cdot 8 = 32 \equiv 10 \pmod{11}.$$

Należy pamiętać, że w module 22 będą 2 rozwiązania (bo dzieliliśmy przez $d = 2$):

$$x \equiv 10 \pmod{11} \Rightarrow x = 10 + 11k.$$

Dla $k = 0, 1$ otrzymujemy klasy modulo 22:

$$x \equiv 10 \pmod{22} \text{ lub } x \equiv 21 \pmod{22}.$$

Zatem $x \equiv 10$ lub $x \equiv 21 \pmod{22}$.

Przykład 12.4

Rozwiązać równanie:

$$12x \equiv 7 \pmod{18}.$$

Rozwiązanie.

Ponieważ $NWD(12, 18) = 6$. Warunek: $6 \mid 7$ nie jest spełniony.

Zatem analizowane równanie nie posiada rozwiązań.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 12.5

Obliczyć $17^{-1} \pmod{43}$.

Rozwiązanie.

Szukamy u, v takich, że:

$$17u + 43v = 1$$

Z algorytmu Euklidesa mamy:

$$43 = 2 \cdot 17 + 9$$

$$17 = 1 \cdot 9 + 8$$

$$9 = 1 \cdot 8 + 1$$

$$8 = 8 \cdot 1 + 0$$

Wykonujemy algorytm odwrotny otrzymujemy:

$$1 = 9 - 1 \cdot 8$$

$$8 = 17 - 1 \cdot 9 \Rightarrow 1 = 9 - (17 - 9) = 2 \cdot 9 - 17$$

$$9 = 43 - 2 \cdot 17 \Rightarrow 1 = 2(43 - 2 \cdot 17) - 17 = 2 \cdot 43 - 5 \cdot 17$$

Zatem:

$$-5 \cdot 17 \equiv 1 \pmod{43} \Rightarrow 17^{-1} \equiv -5 \equiv 38 \pmod{43}.$$

Szukana wartość wynosi zatem $17^{-1} \equiv 38 \pmod{43}$.

Przykład 12.6

Obliczyć $5^{-1} \pmod{14}$ korzystając z twierdzenia Eulera.

Rozwiązanie.

Ponieważ $\text{NWD}(5, 14) = 1$ z definicji funkcji Eulera otrzymujemy

$$\varphi(14) = \varphi(2 \cdot 7) = 14\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 6.$$

Na mocy twierdzenia Eulera mamy:

$$5^6 \equiv 1 \pmod{14} \Rightarrow 5^5 \equiv 5^{-1} \pmod{14}.$$

Stąd:

$$5^2 = 25 \equiv 11 \pmod{14},$$

$$5^4 \equiv 11^2 = 121 \equiv 9 \pmod{14},$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



$$5^5 \equiv 9 \cdot 5 = 45 \equiv 3 \pmod{14}.$$

Ostatecznie stwierdzamy, że $5^{-1} \equiv 3 \pmod{14}$.

Przykład 12.7

Rozwiąż:

$$37x \equiv 12 \pmod{101}.$$

Rozwiązanie.

Ponieważ 101 jest liczbą pierwszą i $37 \not\equiv 0$ to istnieje odwrotność. Obliczmy

$$37^{-1} \pmod{101}$$

Z algorytmu Euklidesa mamy:

$$101 = 2 \cdot 37 + 27$$

$$37 = 1 \cdot 27 + 10$$

$$27 = 2 \cdot 10 + 7$$

$$10 = 1 \cdot 7 + 3$$

$$7 = 2 \cdot 3 + 1$$

Następnie wykonujemy algorytm odwrotny:

$$1 = 7 - 2 \cdot 3$$

$$3 = 10 - 1 \cdot 7 \Rightarrow 1 = 7 - 2(10 - 7) = 3 \cdot 7 - 2 \cdot 10$$

$$7 = 27 - 2 \cdot 10 \Rightarrow 1 = 3(27 - 2 \cdot 10) - 2 \cdot 10 = 3 \cdot 27 - 8 \cdot 10$$

$$10 = 37 - 1 \cdot 27 \Rightarrow 1 = 3 \cdot 27 - 8(37 - 27) = 11 \cdot 27 - 8 \cdot 37$$

$$27 = 101 - 2 \cdot 37 \Rightarrow 1 = 11(101 - 2 \cdot 37) - 8 \cdot 37 = 11 \cdot 101 - 30 \cdot 37$$

Czyli:

$$-30 \cdot 37 \equiv 1 \pmod{101} \Rightarrow 37^{-1} \equiv 71 \pmod{101}.$$

Stąd:

$$x \equiv 12 \cdot 71 = 852 \equiv 852 - 8 \cdot 101 = 852 - 808 = 44 \pmod{101}.$$

Zatem $x \equiv 44 \pmod{101}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Przykład 12.8

Rozwiąż układ:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Rozwiązanie.

Moduły parami są względnie pierwsze, więc rozwiązanie jest jedno modulo

$$3 \cdot 5 \cdot 7 = 105.$$

Niech $M = 105$, rozkładamy na czynniki

$$M_1 = 35$$

$$M_2 = 21$$

$$M_3 = 15$$

Szukamy odwrotności:

$$35y_1 \equiv 1 \pmod{3}. 35 \equiv 2, \text{ więc } 2y_1 \equiv 1 \Rightarrow y_1 \equiv 2.$$

$$21y_2 \equiv 1 \pmod{5}. 21 \equiv 1, \text{ więc } y_2 \equiv 1.$$

$$15y_3 \equiv 1 \pmod{7}. 15 \equiv 1, \text{ więc } y_3 \equiv 1.$$

Stąd

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}.$$

$$x \equiv 140 + 63 + 30 = 233 \equiv 233 - 2 \cdot 105 = 23 \pmod{105}.$$

Ostatecznie otrzymujemy rozwiązanie: $x \equiv 23 \pmod{105}$.

Ćwiczenia samodzielne

Zadanie 12.1

Oblicz $9^{157} \pmod{8}$.

Zadanie 12.2

Oblicz $4^{2025} \pmod{7}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 12.3

Wyznacz ostatnią cyfrę liczby 13^{1000} .

Zadanie 12.4

Oblicz:

- a) $11^{345} \pmod{12}$
- b) $7^{999} \pmod{15}$
- c) $2^{1001} \pmod{9}$

Zadanie 12.7

Wyznacz $5^{444} \pmod{11}$.

Zadanie 12.8

Oblicz $3^{256} \pmod{14}$.

Zadanie 12.9

Oblicz $7^{222} \pmod{40}$.

Zadanie 12.10

Oblicz $11^{1234} \pmod{21}$.

Zadanie 12.11

Oblicz $3^{1000} \pmod{26}$.

Zadanie 12.12

Oblicz $5^{999} \pmod{36}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 12.13

Oblicz $17^{2024} \pmod{45}$.

Zadanie 12.14

Oblicz $8^{777} \pmod{35}$.

Zadanie 12.15

Oblicz $19^{456} \pmod{22}$.

Zadanie 12.16

Oblicz $13^{100} \pmod{27}$.

Zadanie 12.17

Rozwiąż równanie $6x \equiv 10 \pmod{14}$.

Zadanie 12.18

Rozwiąż równanie $15x \equiv 9 \pmod{21}$.

Zadanie 12.19

Rozwiąż równanie $8x \equiv 12 \pmod{20}$.

Zadanie 12.20

Rozwiąż równanie $9x \equiv 7 \pmod{18}$.

Zadanie 12.21

Rozwiąż równanie $14x \equiv 6 \pmod{28}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 12.22

Rozwiąż równanie $10x \equiv 15 \pmod{25}$.

Zadanie 12.23

Rozwiąż równanie $21x \equiv 14 \pmod{35}$.

Zadanie 12.24

Rozwiąż równanie $16x \equiv 5 \pmod{24}$.

Zadanie 12.25

Wyznacz $7^{-1} \pmod{26}$.

Zadanie 12.26

Wyznacz $11^{-1} \pmod{30}$.

Zadanie 12.27

Wyznacz $17^{-1} \pmod{31}$.

Zadanie 12.28

Wyznacz $9^{-1} \pmod{28}$.

Zadanie 12.29

Wyznacz $23^{-1} \pmod{40}$.

Zadanie 12.30

Wyznacz $19^{-1} \pmod{43}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 12.31

Wyznacz $5^{-1}(\text{mod } 18)$.

Zadanie 12.32

Wyznacz $27^{-1}(\text{mod } 64)$.

Zadanie 12.33

Rozwiąż równanie $13x \equiv 7(\text{mod } 17)$.

Zadanie 12.34

Rozwiąż równanie $19x \equiv 4(\text{mod } 29)$.

Zadanie 12.35

Rozwiąż równanie $8x \equiv 1(\text{mod } 15)$.

Zadanie 12.36

Rozwiąż równanie $21x \equiv 5(\text{mod } 26)$.

Zadanie 12.37

Rozwiąż równanie $25x \equiv 10(\text{mod } 37)$.

Zadanie 12.38

Rozwiąż równanie $14x \equiv 9(\text{mod } 41)$.

Zadanie 12.39

Rozwiąż równanie $16x \equiv 3(\text{mod } 25)$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 12.40

Rozwiąż $27x \equiv 11 \pmod{32}$.

Zadanie 12.41

Rozwiąż układ równań:

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases}$$

Zadanie 12.42

Rozwiąż układ równań:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{7} \end{cases}$$

Zadanie 12.43

Rozwiąż układ równań:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{9} \end{cases}$$

Zadanie 12.44

Rozwiąż układ równań:

$$\begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 5 \pmod{7} \end{cases}$$

Zadanie 12.45

Rozwiąż układ równań:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 1 \pmod{5} \end{cases}$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 12.46

Rozwiąż układ równań:

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 2 \pmod{9} \\ x \equiv 3 \pmod{10} \end{cases}$$

Pytania pomocnicze

1. Co oznacza zapis $a \equiv b \pmod{n}$?
2. Jak interpretować kongruencję w kategoriach reszty z dzielenia?
3. Czy relacja kongruencji jest relacją równoważności? Jakie ma własności?
4. Kiedy dwie liczby całkowite są kongruentne modulo n ?
5. Czy można swobodnie dodawać i mnożyć strony kongruencji? Dlaczego?
6. Dlaczego w obliczeniach modularnych można redukować liczby na każdym etapie rachunków?
7. Skąd bierze się okresowość potęg modulo n ?
8. Jak sprawdzić, czy opłaca się wypisać kilka pierwszych potęg, czy lepiej użyć twierdzenia Eulera?
9. Co oznacza „redukcja wykładnika modulo $\varphi(n)$ ”?
10. Dlaczego nie wolno stosować twierdzenia Eulera, gdy $\gcd(a, n) \neq 1$?
11. Co liczy funkcja Eulera $\varphi(n)$?
12. Jak obliczyć $\varphi(n)$, gdy n jest:
 - o liczbą pierwszą?
 - o iloczynem dwóch liczb pierwszych?
 - o potęgą liczby pierwszej?
13. Dlaczego rozkład n na czynniki pierwsze jest kluczowy przy stosowaniu twierdzenia Eulera?
14. Jaką rolę pełni warunek $\gcd(a, n) = 1$ w twierdzeniu Eulera?
15. Co to znaczy, że liczba ma odwrotność modulo n ?
16. Kiedy odwrotność modularna istnieje?
17. Dlaczego brak względnej pierwszości uniemożliwia istnienie odwrotności?



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



18. Jak interpretować odwrotność modularną w kontekście „dzielenia” w kongruencjach?
19. Jakie są dwie podstawowe metody obliczania odwrotności modularnej?
20. Dlaczego rozszerzony algorytm Euklidesa jest metodą uniwersalną?
21. Jaki jest ogólny warunek istnienia rozwiązań równania $ax \equiv b \pmod{n}$?
22. Co oznacza podzielenie kongruencji przez NWD (a, n) ?
23. Dlaczego nie zawsze wolno dzielić stronami kongruencji?
24. Ile rozwiązań może mieć równanie kongruencyjne liniowe modulo n ?
25. Jak przejść od jednego rozwiązania do wszystkich rozwiązań?

Podsumowanie

W trakcie ćwiczeń studenci pracują z pojęciem kongruencji jako relacji równoważności na zbiorze liczb całkowitych oraz wykorzystują jej własności do upraszczania obliczeń. Przeprowadzone zadania pokazują, że:

- arytmetyka modularna pozwala znacząco uprościć obliczenia z dużymi liczbami,
- twierdzenie Eulera umożliwia skuteczną redukcję wykładników potęg, pod warunkiem względnej pierwszości podstawy i modułu,
- równania kongruencyjne liniowe mogą mieć zero, jedno lub wiele rozwiązań, w zależności od największego wspólnego dzielnika współczynnika i modułu,
- istnienie odwrotności modularnej jest ściśle związane z pojęciem względnej pierwszości,
- rozszerzony algorytm Euklidesa stanowi uniwersalne i efektywne narzędzie do obliczania odwrotności modularnych,
- chińskie twierdzenie o resztach pozwala jednoznacznie wyznaczyć rozwiązania układów kongruencji o parami względnie pierwszych modułach.

Zdobyte umiejętności stanowią podstawę do dalszych zagadnień teorii liczb oraz mają istotne znaczenie w zastosowaniach, m.in. w kryptografii, algorytmice i informatyce teoretycznej.



Fundusze Europejskie
dla Rozwoju Społecznego



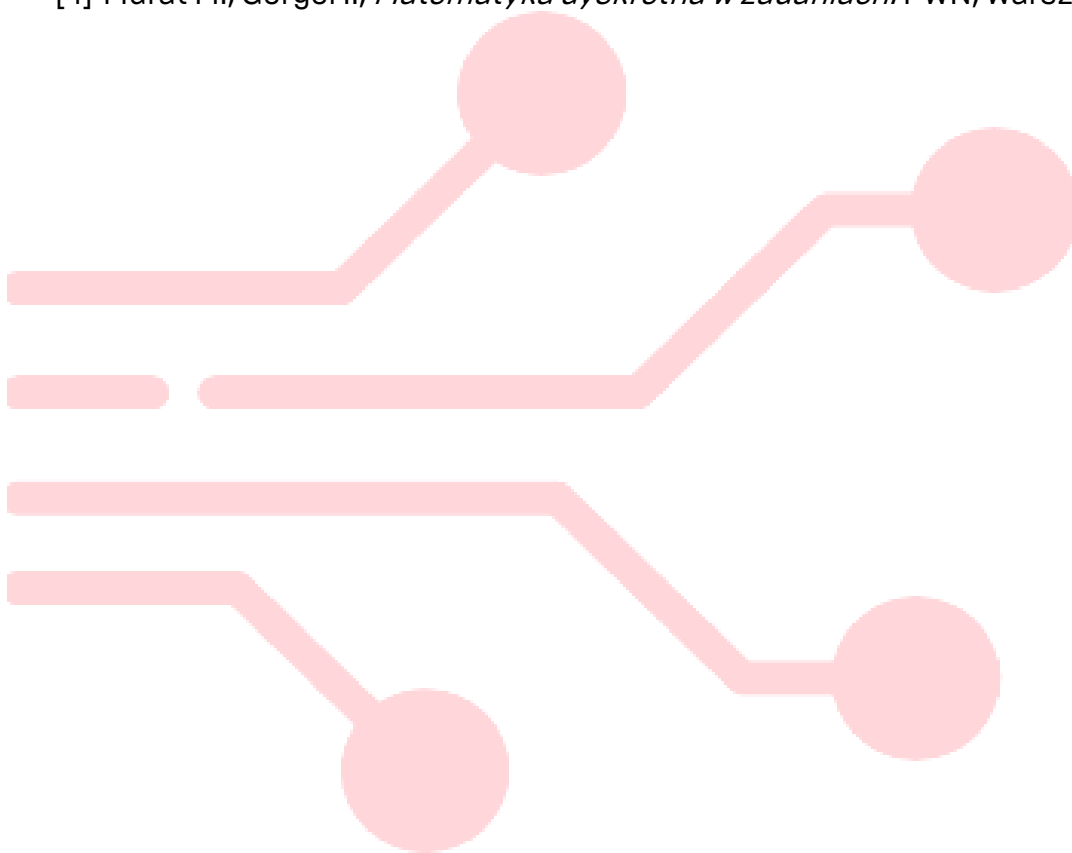
Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Materiały do przedmiotu:

Matematyka dyskretna z elementami teorii liczb

Ćwiczenia nr 13

Znajdowanie reszt kwadratowych i ich zastosowania. Implementacja krzywych eliptycznych w kryptografii

Autorzy:

dr hab. Adam Kiersztyn
mgr Krystyna Kiersztyn



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Spis treści

Wprowadzenie, tematyka zajęć	199
Cel ćwiczenia/laboratorium	201
Instrukcja laboratoryjna/ćwiczeniowa	202
Ćwiczenia samodzielne	206
Pytania pomocnicze	207
Podsumowanie	207
Literatura	208



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Wprowadzenie, tematyka zajęć

Arytmetyka modularna

Niech $a, b, m \in \mathbb{Z}, m \geq 2$.

Mówimy, że

$$a \equiv b \pmod{m},$$

jeżeli

$$m \mid (a - b).$$

Każda liczba całkowita jest **kongruentna** dokładnie jednej liczbie ze zbioru:

$$\{0, 1, 2, \dots, m - 1\}.$$

Niech p będzie nieparzystą liczbą pierwszą.

Liczbę $a \in \mathbb{Z}$ nazywamy **resztą kwadratową** modulo p , jeżeli:

$$\exists x \in \mathbb{Z}: x^2 \equiv a \pmod{p}.$$

Jeżeli taka liczba x nie istnieje, to a nazywamy **nieresztą kwadratową** modulo p .

Zbiór reszt kwadratowych $QR(p)$

$$QR(p) = \{a \in \mathbb{Z}_p: \exists x \in \mathbb{Z}_p x^2 \equiv a \pmod{p}\}.$$

Własności

1. Każda niezerowa reszta kwadratowa ma dokładnie dwa pierwiastki:

$$x^2 \equiv (-x)^2 \pmod{p}$$

2. Liczność zbioru reszt kwadratowych:

$$|QR(p)| = \frac{p+1}{2}$$

3. Dla każdej liczby p zachodzi:

$$0, 1 \in QR(p)$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Kongruencje kwadratowe

Rozważmy równanie:

$$x^2 \equiv a \pmod{p}$$

Twierdzenie

- Jeżeli $a \equiv 0 \pmod{p}$ i $a \in QR(p)$, to kongruencja ma dokładnie dwa rozwiązania modulo p .
- Jeżeli $a \notin QR(p)$, to brak rozwiązań.
- Jeżeli $a \equiv 0 \pmod{p}$, to jedynym rozwiązaniem jest $x \equiv 0$.

Symbol Legendre'a

Dla liczby pierwszej p oraz $a \in \mathbb{Z}$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{gdy } p \mid a \\ 1 & \text{gdy } a \in QR(p) \\ -1 & \text{gdy } a \notin QR(p) \end{cases}$$

Własności symbolu Legendre'a

Dla $a, b \in \mathbb{Z}$, p – nieparzysta liczba pierwsza:

1. Multiplikatywność: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
2. $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
3. $\left(\frac{a^2}{p}\right) = \begin{cases} 1 & \text{jeżeli } p \nmid a \\ 0 & \text{jeżeli } p \mid a \end{cases}$

Twierdzenie (kryterium Eulera)

Dla p – nieparzystej liczby pierwszej oraz $a \in \mathbb{Z}$:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

W szczególności:

- jeżeli $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, to a jest resztą kwadratową,
- jeżeli $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, to a jest nierestą kwadratową.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Krzywe eliptyczne nad ciałem $\mathbb{Z}_p$

Krzywą eliptyczną nad $\mathbb{Z}_p$ nazywamy zbiór punktów spełniających tożsamość:

$$E: y^2 \equiv x^3 + ax + b \pmod{p},$$

gdzie:

$$4a^3 + 27b^2 \not\equiv 0 \pmod{p}.$$

Warunek ten gwarantuje brak punktów osobliwych.

Punkty krzywej eliptycznej

Zbiór punktów:

$$E(\mathbb{Z}_p) = \{(x, y) \in \mathbb{Z}_p^2 : y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\},$$

gdzie $\mathcal{O}$ oznacza punkt w nieskończoności.

Cel ćwiczenia/laboratorium

Celem ćwiczeń jest wprowadzenie podstawowych pojęć związanych z resztami kwadratowymi w arytmetyce modularnej oraz rozwinięcie umiejętności ich zastosowania, w szczególności:

- pojęciem reszt kwadratowych modulo liczby pierwszej,
- definicją zbioru reszt kwadratowych $QR(p)$,
- badaniem rozwiązalności kongruencji postaci $x^2 \equiv a \pmod{p}$,
- własnościami kongruencji kwadratowych,
- pojęciem symbolu Legendre'a,
- stosowaniem kryterium Eulera.

Ponadto celem ćwiczeń jest zapoznanie studentów z zastosowaniem teorii liczb modularnych w konstrukcji krzywych eliptycznych nad ciałami skończonymi, w szczególności:

- definicją krzywej eliptycznej,
- opisem zbioru punktów krzywej eliptycznej,
- rolą reszt kwadratowych w istnieniu rozwiązań równań definiujących krzywą.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ćwiczenia mają na celu rozwinięcie umiejętności analitycznego myślenia oraz przygotowanie do dalszych zagadnień z zakresu teorii liczb i kryptografii.

Instrukcja laboratoryjna/ćwiczeniowa

Przykład 13.1

Wyznaczyć zbiór reszt kwadratowych (QR) modulo 11.

Rozwiązanie.

Obliczmy kwadraty kolejnych klas reszt modulo 11:

$$0^2 \equiv 0 \pmod{11}$$

$$1^2 \equiv 1 \pmod{11}$$

$$2^2 \equiv 4 \pmod{11}$$

$$3^2 \equiv 9 \pmod{11}$$

$$4^2 \equiv 5 \pmod{11}$$

$$5^2 \equiv 3 \pmod{11}$$

Dalsze wartości powtarzają się symetrycznie.

Zatem:

$$QR(11) = \{0, 1, 3, 4, 5, 9\}.$$

Przykład 13.2

Sprawdzić, czy kongruencja

$$x^2 \equiv 7 \pmod{11}$$

ma rozwiązanie.

Rozwiązanie.

Z poprzedniego przykładu:

$$QR(11) = \{0, 1, 3, 4, 5, 9\}.$$

Ponieważ $7 \notin QR(11)$, kongruencja nie ma rozwiązania.

Przykład 13.3

Wyznaczyć wszystkie rozwiązania kongruencji

$$x^2 \equiv 5 \pmod{11}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Rozwiązanie.

Obliczmy

$$4^2 \equiv 5(\text{mod } 11), 7^2 \equiv 49 \equiv 5(\text{mod } 11).$$

Zatem:

$$x \equiv 4 \text{ lub } x \equiv 7(\text{mod } 11).$$

Przykład 13.4

Sprawdzić, czy liczba 10 jest resztą kwadratową modulo 13.

Rozwiązanie.

Obliczamy:

$$1^2 = 1$$

$$2^2 = 4$$

$$3^2 = 9$$

$$4^2 = 16 \equiv 3(\text{mod } 13)$$

$$5^2 = 25 \equiv 12(\text{mod } 13)$$

$$6^2 = 36 \equiv 10(\text{mod } 13)$$

Zatem 10 jest resztą kwadratową modulo 13.

Przykład 13.5

Obliczyć symbol Legendre'a

$$\left(\frac{5}{11}\right).$$

Rozwiązanie.

Z Przykładu 13.1 wiemy, że $5 \in QR(11)$, więc:

$$\left(\frac{5}{11}\right) = 1.$$

Przykład 13.6

Obliczyć symbol Legendre'a

$$\left(\frac{7}{11}\right).$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Rozwiązanie.

[Z Przykładu 13.2] Ponieważ $7 \notin QR(11)$, otrzymujemy:

$$\left(\frac{7}{11}\right) = -1.$$

Przykład 13.7

Zastosować kryterium Eulera do sprawdzenia, czy 3 jest resztą kwadratową modulo 11.

Rozwiązanie.

Dla $a = 3$, $p = 11$ wyrażenie [kryterium Eulera] $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ przyjmuje postać:

$$3^{\frac{11-1}{2}} = 3^5 = 243 \equiv 1 \pmod{11}.$$

Zatem:

$$\left(\frac{3}{11}\right) = 1,$$

czyli 3 jest resztą kwadratową modulo 11.

Przykład 13.8

Rozwiązać kongruencję

$$x^2 \equiv 9 \pmod{13}.$$

Rozwiązanie.

Obliczmy kwadraty

$$3^2 \equiv 9,$$

$$4^2 = 16 \equiv 3 \pmod{13},$$

$$5^2 = 25 \equiv 12 \pmod{13},$$

$$6^2 = 36 \equiv 10 \pmod{13},$$

$$7^2 = 49 \equiv 10 \pmod{13},$$

$$8^2 = 64 \equiv 12 \pmod{13},$$

$$9^2 = 81 \equiv 3 \pmod{13},$$

$$10^2 \equiv 100 \equiv 9 \pmod{13}.$$



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ostatecznie:

$$x \equiv 3 \text{ lub } 10 \pmod{13}.$$

Przykład 13.9

Rozważmy krzywą eliptyczną

$$E: y^2 \equiv x^3 + x + 1 \pmod{5}.$$

Sprawdzić, czy punkt $P = (0,1)$ leży na krzywej.

Rozwiązanie.

Dla $y = 1$ lewa strona (L) przyjmuje postać:

$$1^2 = 1$$

Dla $x = 0$ prawa strona (P) wynosi:

$$0^3 + 0 + 1 = 1$$

Zachodzi równość $L = P$, więc $P \in E(\mathbb{Z}_5)$.

Przykład 13.10

Dla tej samej krzywej sprawdzić punkt $Q = (2, 2)$.

Rozwiązanie.

Podobnie jak w przykładzie 13.9, obliczamy lewą i prawą stronę wyrażenia.

$$L: y^2 = 2^2 = 4$$

$$P: x^3 + x + 1 = 8 + 2 + 1 = 11 \equiv 1 \pmod{5}.$$

Ponieważ $L \neq P$, punkt nie leży na krzywej.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Ćwiczenia samodzielne

Zadanie 13.1

Wyznaczyć $QR(7)$.

Zadanie 13.2

Wyznaczyć $QR(13)$.

Zadanie 13.3

Sprawdzić, czy 6 jest resztą kwadratową modulo 11.

Zadanie 13.4

Rozwiązać równanie $x^2 \equiv 4 \pmod{13}$.

Zadanie 13.5

Rozwiązać równanie $x^2 \equiv 10 \pmod{13}$.

Zadanie 13.6

Obliczyć symbol Legendre'a $\left(\frac{2}{7}\right)$.

Zadanie 13.7

Obliczyć symbol Legendre'a $\left(\frac{5}{13}\right)$.

Zadanie 13.8

Zastosować kryterium Eulera dla liczby 6 modulo 11.

Zadanie 13.9

Sprawdzić rozwiązalność $x^2 \equiv 3 \pmod{7}$.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Zadanie 13.10

Wyznaczyć wszystkie pierwiastki kwadratowe z 1 modulo 17.

Zadanie 13.11

Sprawdzić, czy 15 jest resztą kwadratową modulo 17.

Zadanie 13.12

Dla krzywej $y^2 \equiv x^3 + 2x + 1 \pmod{5}$ sprawdzić punkt (1,2).

Zadanie 13.13

Sprawdzić, czy (2,4) leży na krzywej $y^2 \equiv x^3 + x + 1 \pmod{7}$.

Zadanie 13.14

Wyznaczyć wszystkie punkty krzywej $y^2 \equiv x^3 + 1 \pmod{5}$.

Pytania pomocnicze

- 1) Ile jest reszt kwadratowych modulo liczby pierwszej?
- 2) Dlaczego rozwiązania $x^2 \equiv a \pmod{p}$ występują parami?
- 3) Na czym polega kryterium Eulera?
- 4) Dlaczego krzywa eliptyczna tworzy grupę?

Podsumowanie

W trakcie ćwiczeń omówiono pojęcie reszt kwadratowych modulo liczby pierwszej oraz metody badania rozwiązalności kongruencji kwadratowych. Wprowadzono zbiór $QR(p)$, jego własności oraz związki pomiędzy liczbą rozwiązań kongruencji a strukturą arytmetyki modularnej. Przedstawiono symbol Legendre'a jako formalne narzędzie klasyfikujące liczby na reszty i niereszty kwadratowe oraz zaprezentowano kryterium Eulera jako efektywną metodę obliczeniową.



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Następnie pokazano, że zagadnienia te są bezpośrednio związane z równaniami definiującymi krzywe eliptyczne nad ciałami skończonymi. Omówiono definicję krzywej eliptycznej, warunek nieosobliwości oraz zbiór jej punktów wraz z punktem w nieskończoności. Zwrócono uwagę na fakt, że istnienie punktów krzywej jest bezpośrednio związane z rozwiązalnością kongruencji kwadratowych.

Uzyskane pojęcia i narzędzia stanowią podstawę do dalszej analizy struktury grupowej krzywych eliptycznych oraz ich zastosowań w kryptografii klucza publicznego.

Literatura

- [1] Fałda B., Gruszecki L., *Wstęp do matematyki dyskretnej*. Wydawnictwo KUL, Lublin. 2010.
- [2] Kordecki W., Łyczkowska-Hanćkowiak A., *Matematyka dyskretna dla informatyków*. Helion, Gliwice. 2018.
- [3] Jabłoński S., *Wstęp do matematyki dyskretnej*. PWN, Warszawa, 1991.
- [4] Murat M., Gorgol I., *Matematyka dyskretna w zadaniach*. PWN, Warszawa, 2024



Fundusze Europejskie
dla Rozwoju Społecznego



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską

