KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIWERSYTET GDAŃSKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Publikacja współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

SKRYPT Z MATEMATYKI DYSKRETNEJ

Matematyka dyskretna dla studentów kierunku Informatyka

Hanna Furmańczyk

Karol Horodecki

Paweł Żyliński

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIWERSYTET GDAŃSKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Publikacja współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

SKRYPT Z MATEMATYKI DYSKRETNEJ

Hanna Furmańczyk, Karol Horodecki

Paweł Żyliński

Matematyka dyskretna dla studentów kierunku Informatyka

Dziękujemy wszystkim Studentom, których cenne sugestie i spostrzeżenia pozwoliły nam na ulepszenie zawartości skryptu i wyeliminowanie błędów. Dziękujemy także Autorom, z których materiałów skorzystaliśmy, a na przestrzeni tych kilku lat zdążyliśmy już o tym zapomnieć.

Wydawnictwo Uniwersytetu Gdańskiego
Gdańsk 2010

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIWERSYTET GDAŃSKI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Publikacja współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Skład komputerowy (LaTeX): Paweł Żyliński

ISBN 978-83-7326-708-4

Recenzent:
Projekt okładki i strony tytułowej: Anna Białk – Bielińska

Wydawnictwo Uniwersytetu Gdańskiego, ul. Armii Krajowej 119/121.
81-824 Sopot, tel./fax (058) 523-11-37

Uniwersytet Gdański
Wydział Matematyki, Fizyki i Informatyki
Instytut Informatyki
80-952 Gdańsk, ul. Wita Stwosza 57

Zestaw zadań nr 1

Oznaczenia, pojęcia wstępne

Symbol sumy, $j, k \in \mathbb{Z}$, $j \leq k$:

$$\sum_{i=j}^{k} x_i = x_j + x_{j+1} + \cdots + x_k.$$

Przykład 1.1. Oblicz $\sum_{i=1}^{5} 2^i$.

Rozwiązanie. $\sum_{i=1}^{5} 2^i = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = 2 + 4 + 8 + 16 + 32 = 62.$ ♯

Symbol iloczynu, $j, k \in \mathbb{Z}$, $j \leq k$:

$$\prod_{i=j}^{k} x_i = x_j \cdot x_{j+1} \cdot \ldots \cdot x_k.$$

Przykład 1.2. Oblicz $\prod_{i=1}^{4} i$.

Rozwiązanie. $\prod_{i=1}^{4} i = 1 \cdot 2 \cdot 3 \cdot 4 = 4! = 24.$ ♯

Zadanie 1.3. Oblicz $\sum_{i=1}^{n}(i \cdot 2^i)$ dla $n = 0, 1, 2, 3, 4$.

Zadanie 1.4. Oblicz $\prod_{i=1}^{5}(i + 1)$.

Zadanie 1.5. Oblicz $\prod_{i=1}^{4}(2i + 1)$.

Zadanie 1.6. Sprawdzić prawdziwość poniższych równań dla podanych wartości zmiennych, obliczając wartość lewej i prawej strony.

a) $\sum_{i=1}^{n} i = \frac{(1+n)n}{2}$ dla $n = 3$ i $n = 6$,

b) $\sum_{k=0}^{2n}(3k - 2) = (2n + 1) \cdot (3n - 2)$ dla $n = 2$ i $n = 3$,

c) $\sum_{i=0, i\in\mathbb{P}}^{n} 3^i = \frac{3^{n+1}-1}{8}$ dla $n = 3$ i $n = 4$, gdzie $\mathbb{P}$ – zbiór liczb parzystych,

d) $\prod_{1\leq i\leq 5} i^2 = (5!)^2$

e) $\prod_{i\in T} 2i = 32$, gdzie $T = \{0, 1, 4\}$.

Działania na zbiorach A oraz B:

a) suma:
$$A \cup B = \{x : x \in A \text{ lub } x \in B\}$$
b) iloczyn (przekrój):
$$A \cap B = \{x : x \in A \text{ i } x \in B\}$$
c) różnica:
$$A \setminus B = \{x : x \in A \text{ i } x \notin B\}$$
d) różnica symetryczna:
$$A \oplus B = (A \setminus B) \cup (B \setminus A)$$
e) iloczyn kartezjański (produkt):
$$A \times B = \{(x, y) : x \in A \text{ i } y \in B\}$$

Dla ustalonego zbioru U (uniwersum, przestrzeń), *dopełnieniem* zbioru A, $A \subseteq U$ nazywamy zbiór $U - A$ i oznaczamy przez $\overline{A}$.

Przykład 1.7. Dla $A = \{1, 2, 3\}$ oraz $B = \{2, 4\}$ wyznacz: $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \oplus B$, $A \times B$ oraz $B \times A$.

Rozwiązanie.
$A \cup B = \{1, 2, 3, 4\}$, $A \cap B = \{2\}$, $A \setminus B = \{1, 3\}$,
$B \setminus A = \{4\}$, $A \oplus B = \{1, 3, 4\}$,
$A \times B = \{(1, 2), (1, 4), (2, 2), (2, 4), (3, 2), (3, 4)\}$,
$B \times A = \{(2, 1), (2, 2), (2, 3), (4, 1), (4, 2), (4, 3)\}$. ♯

Przykład 1.8. Dla $A = \{1, 2, 3\}$ oraz uniwersum $U = \{1, 2, 3, 4, 5, 6, 7\}$ wyznacz $\overline{A}$.

Rozwiązanie. $\overline{A} = \{4, 5, 6, 7\}$. ♯

Zadanie 1.9. Niech $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 3, 5, 7\}$, $C = \{4, 5, 6, 7, 8\}$ oraz $U = \mathbb{N}$. Wyznacz:

a) $A \cup B \cup C$,
b) $A \cap B \cap C$,
c) $A \setminus B$,
d) $A \cap (B \setminus C)$,
e) $A \oplus B$,
f) $A \oplus B \oplus C$,
g) $\overline{A} \cap \overline{B}$,
h) $\overline{A \cap B}$.

Niech dana będzie rodzina zbiorów $\mathcal{A} = \{A_1, A_2 \ldots, A_k\}$. Wówczas:

a) suma:
$$\bigcup_{1 \leq i \leq k} A_i = \{x : x \in A_i \text{ dla pewnego } 1 \leq i \leq k\}.$$

b) iloczyn (przekrój):
$$\bigcap_{1 \leq i \leq k} A_i = \{x : x \in A_i \text{ dla każdego } 1 \leq i \leq k\}.$$

c) różnica symetryczna:
$$\bigoplus_{1 \leq i \leq k} A_i = \begin{cases} A_1 \oplus A_2 & \text{jeśli } k = 2; \\ \bigoplus_{1 \leq i \leq k-1} A_i \oplus A_k & \text{w przeciwnym wypadku.} \end{cases}$$

Zadanie 1.10. Niech $I = \{1, 2, 3, 4, 5\}$ będzie zbiorem indeksów. Dla każdego $i \in I$ określmy zbiór $B_i = \{x \in \mathbb{N} : i \leq x \leq 2i\}$. Wyznacz:

a) $\bigcup_{i \in I} B_i$,

b) $\bigcap_{i \in I} B_i$,

c) $B_1 \oplus B_3 \oplus B_5$,

d) $B_1 \oplus B_2 \oplus B_3 \oplus B_4 \oplus B_5$.

Zadanie 1.11. Niech $T = \{1, 2, 3, 4, 5\}$ będzie zbiorem indeksów. Dla każdego $t \in T$ określmy zbiór $A_t = \{y \in \mathbb{N}^+ : y \leq t\}$ i $B_t = \{y \in \mathbb{N}^+ : y > t\}$, gdzie $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$. Wyznacz:

a) A_1, A_2, A_3, A_4, A_5 i B_1, B_2, B_3, B_4, B_5,

b) $\bigcup_{k=3}^{5} A_k$,

c) $\bigcap_{i=1, i \in \mathbb{NP}}^{5} A_i$, gdzie $\mathbb{NP}$ – zbiór liczb nieparzystych,

d) $\bigcup_{j=1}^{4} B_j$,

e) $\bigcap_{i \in T, i \leq 3} B_i$,

f) $\bigcap_{i=1}^{3} (A_i \cup A_{i+1})$,

g) $\bigcup_{k \in T, k \in \mathbb{P}} (A_k \cap B_k)$, gdzie $\mathbb{P}$ – zbiór liczb parzystych,

h) $\bigcap_{k \in T, k \in \mathbb{P}} (A_k \cup B_k)$, gdzie $\mathbb{P}$ – zbiór liczb parzystych.

Zadanie 1.12. Niech $I = \{1, 2, 3, 4, 5\}$ będzie zbiorem indeksów. Dla każdego $i \in I$ określmy zbiór $C_i = \{x \in \mathbb{N} : 1 \leq x \leq 30 \text{ oraz } i | x\}$. Wyznacz:

a) $\bigcup_{i \in I} C_i$,

b) $\bigcap_{i \in I} C_i$.

Zadanie 1.13. Niech $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3\}$. Wyznacz:

a) $A \times B$,
b) $B \times A$,
c) $\{(a, b) \in A \times B : a < b\}$.

Ile wynosi liczba elementów zbiorów $A \times B$ i $B \times A$.

Zadanie 1.14. Dane są zbiory: $A = \{k \in \mathbb{N} : k \text{ parzyste } \wedge k \leq 6\}$, $B = \{1, 4\}$, $C = \{n \in \mathbb{N} : 0 \leq n \leq 3\}$, $D = \{m \in \mathbb{N} : 3 < m < 6\}$.

a) Wyznaczyć zbiory A, C, D.

b) Znaleźć zbiory $A \oplus C$, $A \oplus D$, $D \times B$, $B \times D$, $(D \times B) \cap (B \times D)$.

Zadanie 1.15. Niech $S = \{0, 1, 2, 3, 4\}$ i niech $T = \{0, 2, 4\}$.

a) Ile par uporządkowanych należy do zbioru $S \times T$, a ile do zbioru $T \times S$?

b) Wypisz elementy zbioru $\{(m, n) \in S \times T : m + n = 5\}$.

c) Wypisz i narysuj elementy zbioru $\{(m, n) \in S \times T : m + n \geq 3\}$.

d) Wypisz elementy zbioru $\{(m, n) \in S \times S : m + n = 5\}$.

Zadanie 1.16. Wypisz wszystkie podzbiory podanych niżej zbiorów. Ile jest tych podzbiorów?

a) $A = \{a\}$,
b) $B = \{b, c\}$,
c) $C = \{c, d\}$,
d) $D = B \cup C$,
e) $E = B \times C$.

Zadanie 1.17. Niech $X = \{a, b, c\}$. Wypisz elementy $X^2 = X \times X$, X^3 oraz

$$\{(x, y) \in X^2 : x \neq y\}.$$

Zadanie 1.18. Udowodnij, że $A \subseteq B$ wtedy i tylko wtedy, gdy $A \cap B = A$.

Niech Σ będzie zbiorem skończonym, zwanym dalej *alfabetem*. Wówczas dowolny ciąg złożony z elementów tego zbioru nazywamy *słowem* nad alfabetem Σ. Np. dla alfabetu $\Sigma = \{a, b\}$ przykładowe słowa to: a, $abbb$, $aabb$, $aa \ldots a$. Zbiór wszystkich słów nad alfabetem Σ oznaczamy przez Σ^*. Długość słowa u oznaczamy przez $|u|$. Wśród słów wyróżniamy słowo *puste* λ, które nie zawiera żadnej litery ($|\lambda| = 0$).

Zadanie 1.19. Wypisz 10 dowolnych słów zbioru $\{a, b, c\}^*$.

Zadanie 1.20. Wypisz 5 pierwszych słów zbioru $\{a, b, c\}^*$ uporządkowanych według porządku leksykograficznego (słownikowego).

Mówimy, że słowo u poprzedza słowo v w porządku *kanonicznym*, jeżeli albo $|u| < |v|$, albo $|u| = |v|$ i u poprzedza v w porządku leksykograficznym.

Przykład 1.21. Początkowe słowa zbioru $\{0,1\}^*$ uporządkowane według porządku kanonicznego to:

$$\lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, 0000, \ldots$$

Zadanie 1.22. Wypisz 10 pierwszych słów zbioru $\{a,b,c\}^*$ uporządkowanych według porządku kanonicznego.

Zadanie 1.23. Wypisz wszystkie prefiksy i sufiksy słowa *aaba*.

Zadanie 1.24. Uporządkuj następujący zbiór słów według porządku leksykograficznego i kanonicznego: *słowik, wróbel, kos, jaskółka, kogut, dzięcioł, gil, kukułka, szczygieł, sowa, kruk, czubatka, drozd, sikora, dzierlatka, kaczka, gąska, jemiołuszka, dudek, trznadel, pośmie- ciuszka, wilga, zięba, bocian, szpak.*

Zaokrąglenia liczb rzeczywistych:

$\lceil x \rceil$ oznacza zaokrąglenie x w górę do najbliższej liczby całkowitej (sufit z x),

$\lfloor x \rfloor$ oznacza zaokrąglenie x w dół do najbliższej liczby całkowitej (podłoga z x).

Zadanie 1.25. Niech x, y będą dowolnymi liczbami rzeczywistymi, a k dowolną liczbą całkowitą. Udowodnij następujące zależności:

a) $\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$,

b) $\lfloor x+k \rfloor = \lfloor x \rfloor + k$,

c) $\lceil x+y \rceil \leq \lceil x \rceil + \lceil y \rceil$,

d) $\lceil x+k \rceil = \lceil x \rceil + k$.

Zadanie 1.26. Podaj przykład liczb rzeczywistych x i y, dla których zachodzi:

a) $\lfloor x+y \rfloor > \lfloor x \rfloor + \lfloor y \rfloor$,

b) $\lceil x+y \rceil < \lceil x \rceil + \lceil y \rceil$.

Zadanie 1.27. Podaj przykład liczby rzeczywistej x i liczby całkowitej k, dla których zachodzi $\lceil k \cdot x \rceil < k \cdot \lceil x \rceil$.

Zadanie 1.28. Dane są dwa wielomiany: $U(x) = 4x^3 + 3x + 2$ oraz $V(x) = 2x^4 + x^2 + 3x$. Oblicz ich sumę i iloczyn. Oblicz według schematu Hornera wartości $U(1)$ oraz $V(2)$.

Zadanie 1.29. Podziel wielomian $U(x) = 4x^4 + 3x^2 + x - 2$ przez $V(x) = x^2 + x$.

Odpowiedzi do zadań

1.3.

$n = 0$: błędnie określony zakres sumowania.

$n = 1$: 2.

$n = 2$: 10.

$n = 3$: 34.

$n = 4$: 98.

1.4. $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$.

1.5. $3 \cdot 5 \cdot 7 \cdot 9 = 945$.

1.6.

a) $6 = 6$, $21 = 21$,

b) $20 = 20$, $49 = 49$,

c) $10 = 10$, $91 \neq \frac{242}{8}$,

d) $14400 = 14400$,

e) $0 \neq 32$.

1.9.

a) $\{1, 2, 3, 4, 5, 6, 7, 8\}$,

b) $\{5\}$,

c) $\{2, 4\}$,

d) $\{1, 3\}$,

e) $\{2, 4, 7\}$,

f) $\{2, 5, 6, 8\}$,

g) $\{8, 9, 10, \ldots\}$,

h) $\{2, 4, 6, 7, 8, \ldots\}$.

1.10. Wyznaczone zbiory B_i: $B_1 = \{1, 2\}$, $B_2 = \{2, 3, 4\}$, $B_3 = \{3, 4, 5, 6\}$, $B_4 = \{4, 5, 6, 7, 8\}$, $B_5 = \{5, 6, 7, 8, 9, 10\}$.

a) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$,

b) zbiór pusty $\emptyset$,

c) $\{1, 2, 3, 4, 7, 8, 9, 10\}$,

d) $\{1, 4, 5, 6, 9, 10\}$.

1.11.

a) $A_1 = \{1\}$, $A_2 = \{1, 2\}$, $A_3 = \{1, 2, 3\}$, $A_4 = \{1, 2, 3, 4\}$, $A_5 = \{1, 2, 3, 4, 5\}$, $B_1 = \{2, 3, \ldots\}$, $B_2 = \{3, 4, \ldots\}$, $B_3 = \{4, 5, \ldots\}$, $B_4 = \{5, 6, \ldots\}$, $B_5 = \{6, 7, \ldots\}$,

b) $\{1, 2, 3, 4, 5\}$,

c) $\{1\}$,

d) $\{2, 3, \ldots\}$,

e) $\{4, 5, \ldots\}$,

f) $\{1, 2\}$,

g) $\emptyset$,

h) $\{1, 2, \ldots\}$,

1.12. Wyznaczone C_i: $C_1 = \{1, 2, 3, \ldots, 29, 30\}$, $C_2 = \{2, 4, 6, \ldots, 28, 30\}$, $C_3 = \{3, 6, 9, \ldots, 27, 30\}$, $C_4 = \{4, 8, 12, \ldots, 24, 28\}$, $C_5 = \{5, 10, 15, \ldots, 25, 30\}$.

a) $\{1, 2, 3, \ldots, 29, 30\} = C_1$,

b) $\emptyset$.

1.13.

a) $\{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), \ldots, (4,1), (4,2), (4,3)\}$, $4 * 3 = 12$

b) $\{(1,1), (1,2), (1,3), (1,4), \ldots, (3,1), (3,2), (3,3), (3,4)\}$, $3 * 4 = 12$,

c) $\{(1,2), (1,3), (2,3)\}$.

1.14.

a) $A = \{0, 2, 4, 6\},\ C = \{0, 1, 2, 3\},\ D = \{4, 5\}.$

b) $\{1, 3, 4, 6\}$,
$\{0, 2, 5, 6\}$,
$\{(4, 1), (4, 4), (5, 1), (5, 4)\}$,
$\{(1, 4), (4, 4), (1, 5), (4, 5)\}$,
$\{(4, 4)\}$.

1.15.

a) 15, 15

b) ...poprawić...

c) $\{(0, 4), (1, 2), (1, 4), (2, 2), (2, 4), (3, 0), (3, 2), (3, 4), (4, 0), (4, 2), (4, 4)\}$

d) ...poprawić...

1.16.

a) $\mathcal{P}(A) = \{\emptyset, \{a\}\}$,
$|\mathcal{P}(A)| = 2$,

b) $\mathcal{P}(B) = \{\emptyset, \{b\}, \{c\}, \{b, c\}\}$,
$|\mathcal{P}(B)| = 4$,

c) $\mathcal{P}(C) = \{\emptyset, \{c\}, \{d\}, \{c, d\}\}$,
$|\mathcal{P}(C)| = 4$,

d) $\mathcal{P}(D) = \{\emptyset, \{b\}, \{c\}, \{d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{b, c, d\}\}$,
$|\mathcal{P}(D)| = 8$,

e) $\mathcal{P}(D) = \{\emptyset, \{(b, c)\}, \{(b, d)\}, \{(c, c)\}, \{(c, d)\}, \{(b, c), (b, d)\}, \{(b, c), (c, c)\}, \{(b, c), (c, d)\},$
$\{(b, d), (c, c)\}, \{(b, d), (c, d)\}, \{(c, c), (c, d)\}, \{(b, c), (b, d), (c, c)\}, \ldots, \{(b, c), (b, d), (c, c), (c, d)\}\}$,
$|\mathcal{P}(E)| = 16$.

1.17.

$X^2 = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$

$X^3 = \{(a, a, a), (a, a, b), (a, a, c), (a, b, a), (a, b, b), (a, b, c), (a, c, a), (a, c, b), (a, c, c),$
$(b, a, a), (b, a, b), (b, a, c), (b, b, a), (b, b, b), (b, b, c), (b, c, a), (b, c, b), (b, c, c),$
$(c, a, a), (c, a, b), (c, a, c), (c, b, a), (c, b, b), (c, b, c), (c, c, a), (c, c, b), (c, c, c)\}$

$\{(x, y) \in X^2 : x \neq y\} = \{(a, b), (a, c), (b, a), (b, c), (c, a), (c, b)\}.$

1.19. Np. $\{aaa, \lambda, a, bc, ca, caab, b, c, cccc, bbacc\}$.

1.20. $\{\lambda, a, aa, aaa, aaaa\}$.

1.22. $\{\lambda, a, b, c, aa, ab, ac, ba, bb, bc\}$.

1.23.

Prefiksy: $\lambda, a, aa, aab, aaba$.

Sufiksy: $\lambda, a, ba, aba, aaba$.

1.24.

Porządek leksykograficzny: *bocian, czubatka, drozd, dudek, dzierlatka, dzięcioł, gąska, gil, jaskółka, jemiołuszka, kaczka, kogut, kos, kruk, kukułka, pośmieciuszka, sikora, słowik, sowa, szczygieł, szpak, trznadel, wilga, wróbel, zięba.*

Porządek kanoniczny: *gil, kos, sowa, drozd, dudek, gąska, kogut, szpak, wilga, zięba, bocian, kaczka, sikora, słowik, wróbel, kukułka, dzięcioł, jaskółka, trznadel, czubatka, szczygieł, dzierlatka, jemiołuszka, pośmieciuszka.*

1.26.

a) Np. $x = 2.6$, $y = 2.7$.

b) Np. $x = 2.2$, $y = 2.1$.

1.27. Np. $k = 2$, $x = 2.3$.

1.28.

$U(x) + V(x) = 2x^4 + 3x^3 + x^2 + 6x + 2$.

$U(x) \cdot V(x) = 8x^{12} + 10x^5 + 16x^4 + 3x^3 + 11x^2 + 6x$.

$U(1) = 9$.

$V(2) = 42$.

1.29. $U(x) = (4x^2 - 4x + 7) \cdot V(x) - 6x - 2$.

Zestaw zadań nr 2

Arytmetyka

Niech $b = d_r d_{r-1} \dots d_1 d_0$ będzie zapisem liczby w systemie dwójkowym. Zamiana zapisu liczby b na system dziesiętny odbywa się poprzez wykonanie dodawania

$$d_r \cdot 2^r + d_{r-1} \cdot 2^{r-1} \dots d_1 \cdot 2^1 + d_0 \cdot 2^0,$$

przy czym dodawanie to jest wykonywane w systemie o podstawie 10.

Przykład 2.1. Liczbę 10010 zapisaną w systemie dwójkowym przedstaw w systemie dziesiętnym.

Rozwiązanie. $(10010)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = (18)_{10}$. ♯

Zadanie 2.2. Podane liczby zapisane w systemie dwójkowym przedstaw w systemie dziesiętnym:

a) 1010.
b) 111101.
c) 1011110.

Algorytm zwiększania liczby o „1”:

1. Wskaż ostatni bit rozważanej liczby.
2. Powtarzaj, co następuje:
   2.a. Jeżeli wskazywany bit to „0”, to zamień go na „1”; Koniec.
   2.b. W przeciwnym przypadku zamień go na „0” i wskaż kolejny bit na lewo; jeżeli nie ma następnego bitu w lewo, to wstaw „1”; Koniec.

Przykład 2.3. Prześledź działanie algorytmu dodawania „1” dla liczb (a) 10010 oraz (b) 101011.

Rozwiązanie.

a) $10010 + 1 = 10011$, bo $1001\underline{0} \to (= 0) \to 10011$ (Koniec).

b) $101011 + 1 = 101100$,
bo $10101\underline{1} \to (= 1) \to 1010\underline{1}0 \to (= 1) \to 101\underline{0}00 \to (= 0) \to 101100$ (Koniec). ♯

Zadanie 2.4. Prześledź działanie algorytmu dodawania „1” dla następujących liczb:

a) 111110.
b) 101111.
c) 10011.

Algorytm porównywania liczb:

1. Jeżeli liczby są różnej długości, to większą jest liczba o dłuższym zapisie.
2. Jeżeli liczby są tej samej długości, to porównujemy bit po bicie od lewej strony do prawej:
   2.a. Jeżeli bity są takie same, to przechodzimy do następnego bitu w prawo;
   2.b. Jeżeli bity są różne, to większą jest liczba o większym bicie na rozważanej pozycji; KONIEC.
3. Jeżeli wszystkie bity są takie same, to porównywane liczby są równe i KONIEC.

PRZYKŁAD 2.5. Prześledź działanie algorytmu porównywania liczb dla następujących par liczb:

a) 101101 i 11110.
b) 1011101 i 1011001.

Rozwiązanie.

a) Jako że długość (liczba bitów) pierwszej liczby jest większa od długości liczby drugiej, otrzymujemy $101101 > 11110$.

b) $(\underline{1}011101 \ ? \ \underline{1}011001) \to (=) \to (1\underline{0}11101 \ ? \ 1\underline{0}11001) \to (=) \to$
$(10\underline{1}1101 \ ? \ 10\underline{1}1001) \to (=) \to (101\underline{1}101 \ ? \ 101\underline{1}001) \to (=) \to$
$(1011\underline{1}01 \ ? \ 1011\underline{0}01) \to (>) \to$, a zatem $1011101 > 1011001$. ♯

ZADANIE 2.6. Prześledź działanie algorytmu porównywania liczb dla następujących par liczb:

a) 1111 i 10001.
b) 11010 i 10111.
c) 1111001 i 1111011.

Algorytm dodawania liczb:

Aby dodać do siebie dwie liczby zapisane w systemie dwójkowym, dodajemy bit po bicie od prawej do lewej, dodając jednocześnie w każdym z kroków bit przeniesienia z poprzedniej kolumny.

PRZYKŁAD 2.7. Wykonaj dodawanie (a) $10101 + 111$ oraz (b) $111 + 111 + 111 + 111 + 111$.

Rozwiązanie.

a) $10101 + 111 = 11100$, ponieważ

$$\begin{array}{r} \ 01010 \\ \hline \ 10101 \\ +\quad 111 \\ \hline 11100 \end{array} \quad . \qquad \begin{array}{r} \ 1 \\ \hline \ 1 \\ \hline \ 11 \\ \hline \ 10 \\ \hline \ 11 \\ \hline \end{array}$$

b) $111 + 101 + 111 + 111 + 111 + 101$, ponieważ

$$\begin{array}{r} \ 111 \\ \ 101 \\ \ 111 \\ \ 111 \\ \ 111 \\ +\quad 101 \\ \hline 100110 \end{array} \quad .$$

♯

Zadanie 2.8. Wykonaj dodawanie:

a) 1111 + 1110.
b) 10011 + 1100.
c) 110111 + 110011.
d) 101 + 111 + 111.
e) 1011 + 1011 + 111.

Algorytm odejmowania liczb:

Aby odjąć od siebie dwie liczby zapisane w systemie dwójkowym, odejmujemy bit po bicie od prawej do lewej, a w przypadku, gdy trzeba odjąć bit większy od mniejszego, „pożyczamy" dwójkę z następnej (w lewo) pozycji.

Przykład 2.9. Wykonaj odejmowanie:

a) 10101 - 111.
b) 111000 - 11111.

Rozwiązanie.

a) $10101 - 111 = 1110$, ponieważ
$$\begin{array}{rr} & 012 \\ \hline & 1002 \\ \hline & 10101 \\ - & 111 \\ \hline & 1110 \end{array}.$$

b) $111000 - 11111 = 11001$, ponieważ
$$\begin{array}{rr} & 02 \\ \hline & 102 \\ \hline & 110112 \\ \hline & 111000 \\ - & 11111 \\ \hline & 11001 \end{array}.$$

♯

Zadanie 2.10. Wykonaj odejmowanie:

a) 10011 - 1100.
b) 110111 - 110011.
c) 1010001 - 101110.
d) 1011100 - 1010111.

Algorytm mnożenia liczb:

Aby pomnożyć dwie liczby (zapisane dwójkowo), mnożymy pierwszą liczbę przez poszczególne bity drugiej, a otrzymane wyniki, każdy kolejno przesunięty o jedną kolumnę w lewo, na koniec sumujemy.

Przykład 2.11. Wykonaj mnożenie $10101 \cdot 101$.

Rozwiązanie. $10101 \cdot 101 = 1101001$, ponieważ

$$\begin{array}{r} 10101 \\ \cdot \quad 101 \\ \hline 10101 \\ 00000 \\ 10101 \\ \hline 1101001 \end{array}.$$

Zauważmy, że aby ułatwić sobie mnożenie liczb, mając na uwadze przemienność mnożenia, wygodniej jest mnożyć liczbę o większej liczbie jedynek przez liczbę o mniejszej liczbie jedynek, tzn. rozpatrywać iloczyn $10101 \cdot 101$ raczej niż iloczyn $101 \cdot 10101$. ♯

Zadanie 2.12. Wykonaj mnożenie:

a) $101 \cdot 111$.
b) $1111 \cdot 111$.
c) $10011 \cdot 1100$.
d) $111000 \cdot 111$.

Przykład 2.13. Wykonaj dzielenie $1101001 : 101$.

Rozwiązanie. $1101001 : 101 = 10101$, ponieważ

$$\begin{array}{rl} & 10101 \\ \hline 1101001 & : 101 \\ 101 & \\ \hline 00110 & \\ \quad 101 & \\ \hline \quad 00101 & \\ \quad 00101 & \\ \hline \qquad 0 & \end{array}.$$

♯

Zadanie 2.14. Wykonaj dzielenie:

a) $100011 : 101$.
b) $1101001 : 111$.
c) $110001 : 111$.
d) $11000 : 1000$.
e) $1010001 : 1001$.

Uwaga 1. Liczba jest podzielna przez 2 (lub 10), jeśli ostatni bit równy jest `0`.
Uwaga 2. Liczba jest podzielna przez 2^i ($1\underbrace{\texttt{0}\ldots\texttt{0}}_{i \text{ zer}}$), jeśli ma na końcu i bitów równych 0.

Niech b będzie liczbą zapisaną w systemie dziesiętnym. Zamiana zapisu liczby b na system dwójkowy odbywa się poprzez rozłożenie b na sumę kolejnych potęg dwójki:

$$b = d_r \cdot 2^r + d_{r-1} \cdot 2^{r-1} \ldots d_1 \cdot 2^1 + d_0 \cdot 2^0,$$

gdzie $d_i \in \{0, 1\}$. Wówczas $b = (d_r d_{r-1} \ldots d_1 d_0)_2$.

Przykład 2.15. Zamień zapis z dziesiętnego na dwójkowy liczby 81.

Rozwiązanie.
$(81)_{10} = (64 + 16 + 1) = 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^1 = (1010001)_2$. ♯

Zadanie 2.16. Zamień zapis z dziesiętnego na dwójkowy liczb:

a) 111.
b) 169.
c) 411.

Drugi sposób polega na kolejnym dzieleniu liczby w sposób całkowity przez 2 i zapamiętywaniu reszt z dzielenia. Reszty te, zapisane w odwrotnej kolejności, tworzą zapis binarny liczby.

Przykład 2.17. Korzystając z w/w opisanego sposobu zamień zapis z dziesiętnego na dwójkowy liczby 81.

Rozwiązanie. $(81)_{10} = (1010001)_2$, ponieważ

liczba	iloraz	reszta
81	40	1
40	20	0
20	10	0
10	5	0
5	2	1
2	1	0
1	0	1

. ♯

Zadanie 2.18. Korzystając z w/w opisanego sposobu zamień zapis z dziesiętnego na dwójkowy liczb z Zadania 2.16.

W systemie szesnastkowym używa się następujących „cyfr”: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}$. Przyjmijmy notację, że liczbę zapisaną w systemie szesnastkowym poprzedza znak dolara \$.

Przykład 2.19. Zamień zapis liczby \$A1 z szesnastkowego na dziesiętny.

Rozwiązanie. $\$\mathrm{A}1 = 10 \cdot 16^1 + 1 \cdot 16^0 = 160 + 1 = (161)_{10}$. ♯

Zadanie 2.20. Zamień zapis z szesnastkowego na dziesiętny liczb:

a) \$A91.
b) \$C2.
c) \$FCA.

Przykład 2.21. Zamień zapis liczby 320 z dziesiętnego na szesnastkowy.

Rozwiązanie. $320 = 1 \cdot 16^2 + 4 \cdot 16^1 + 0 \cdot 16^0 = \$140$. Możemy także skorzystać ze sposobu opisanego w Przykładzie 2.17, tym razem dzieląc przez 16:

liczba	iloraz	reszta
320	20	0
20	1	4
1	0	1

. ♯

Zadanie 2.22. Zamień zapis z dziesiętnego na szesnastkowy liczb:.

a) 199.
b) 541.
c) 855.

Przykład 2.23. Zamień zapis liczby $A1 z szesnastkowego na binarny.

Rozwiązanie. $A1 = (10100001)_2$, ponieważ $\begin{array}{r|r} \text{A} & 1 \\ \hline 1010 & 0001 \end{array}$. ♯

Zadanie 2.24. Zamień zapis z szesnastkowego na binarny liczb:

(a) $A91.
(b) $C2.
(c) $FCA.

Przykład 2.25. Zamień zapis liczby `10111100` z binarnego na szesnastkowy.

Rozwiązanie. $(10111100)_2 = \$BC$, ponieważ $\begin{array}{r|r} 1011 & 1100 \\ \hline \text{B} & \text{C} \end{array}$. ♯

Zadanie 2.26. Zamień zapis z binarnego na szesnastkowy liczb:

(a) 1011101.
(b) 100010.
(c) 111110110.

Zapis $0.d_1d_2\ldots d_r$ w systemie dziesiętnym oznacza liczbę $d_1 \cdot 10^{-1} + d_2 \cdot 10^{-2} \ldots d_r \cdot 10^{-r}$.
Analogicznie, zapis $0.d_1d_2\ldots d_r$ w systemie dwójkowym oznacza liczbę: $d_1 \cdot 2^{-1} + d_2 \cdot 2^{-2} \ldots d_r \cdot 2^{-r}$.

Przykład 2.27. $(0.11)_2 = 1 \cdot 2^{-1} + 1 \cdot 2^{-2} = \ldots \frac{3}{4} \ldots = 7 \cdot 10^{-1} + 5 \cdot 10^{-2} = (0.75)_{10}$

Aby zamienić zapis ułamka z systemu dziesiętnego na binarny należy rozważany ułamek kolejno mnożyć (w systemie dziesiętnym) przez 2, wypisując kolejno otrzymywane części całkowite, do momentu, aż część ułamkowa będzie równa 0.

Przykład 2.28. Zamień zapis liczby $(0.8125)_{10}$ z dziesiętnego na binarny.

Rozwiązanie.

część całkowita	część ułamkowa
0.	0.8125
1	0.625
1	0.25
0	0.5
1	0.0

Otrzymujemy ostatecznie, że $(0.8125)_{10} = (0.1101)_2$. ♯

Zadanie 2.29. Zamień zapis z dziesiętnego na binarny liczb:

a) 0.5625.
b) 0.15625.
c) 0.328125.
d) 0.78125.
e) 7.5625.
f) 11.15625.
g) 13.328125.

Przykład 2.30. Wykonaj następujące działania:

a) $(56)_7 + (43)_7$,
b) $(41)_5 - (24)_5$,
c) $(13)_6 \cdot (4)_6$.

Rozwiązanie.

a) $(56)_7 + (43)_7 = (132)_7$, ponieważ
$$\begin{array}{rr} & 110 \\ \hline & 56 \\ + & 43 \\ \hline & 132 \end{array}.$$

b) $(41)_5 - (24)_5 = (12)_5$, ponieważ
$$\begin{array}{rr} & 36 \\ \hline & 41 \\ - & 24 \\ \hline & 12 \end{array}.$$

c) $(13)_6 \cdot (4)_6 = (100)_6$, ponieważ
$$\begin{array}{rr} & 20 \\ \hline & 13 \\ \cdot & 4 \\ \hline & 100 \end{array}.$$

♯

Zadanie 2.31. Wykonaj następujące działania:

a) $(13)_4 + (33)_4$.
b) $(122)_3 + (122)_3 + (122)_3$.
c) $(456)_7 + (223)_7$.
d) $(302)_4 - (13)_4$.
e) $(4236)_7 - (2543)_7$.
f) $(13)_4 \cdot (3)_4$.
g) $(135)_7 \cdot (642)_7$.

Przykład 2.32. Pewna liczba x zapisana w zapisie ósemkowym ma 5 cyfr. Ile będzie miała cyfr w zapisie szesnastkowym?

Rozwiązanie. Liczba x, która w zapisie ósemkowym ma 5 cyfr, należy do zbioru

$$\{(10000)_8, (10001)_8, \ldots, (77776)_8, (77777)_8\}.$$

Jednym z poprawnych rozwiązań jest przekształcenie zapisu $(10000)_8$ i $(77777)_8$ w odpowiednie zapisy w systemie dziesiętnym, a następnie przekształcenie tak otrzymanych zapisów w system szesnastkowy. Otrzymamy wtedy:

$$(10000)_8 = 1\cdot 8^4 + 0\cdot 8^3 + 0\cdot 8^2 + 0\cdot 8^1 + 0\cdot 8^0 = 4096 = 1\cdot 16^3 + 0\cdot 16^2 + 0\cdot 16^1 + 0\cdot 16^0 = \$1000,$$

$$(77777)_8 = 7\cdot 8^4 + 7\cdot 8^3 + 7\cdot 8^2 + 7\cdot 8^1 + 7\cdot 8^0 = 32767 = 7\cdot 16^3 + 15\cdot 16^2 + 15\cdot 16^1 + 15\cdot 16^0 = \$7\text{FFF}.$$

A zatem liczba x w zapisie szesnastkowym będzie miała 4 cyfry.

Drugie rozwiązanie jest dużo prostsze. Opiera się ono na spostrzeżeniu, że 8 i 16 są potęgami dwójki. Zatem w łatwy sposób możemy zamienić zapisy $(10000)_8$ i $(77777)_8$ w zapis dwójkowy, z którego w równie łatwy sposób otrzymamy zapis szesnastkowy.

$$(10000)_8 = 1\ 000\ 000\ 000\ 000 = 1\ 0000\ 0000\ 0000 = \$1000,$$

$$(77777)_8 = 111\ 111\ 111\ 111\ 111 = 111\ 1111\ 1111\ 1111 = \$7\text{FFFF}. \qquad \sharp$$

Zadanie 2.33. Pewna liczba x zapisana w zapisie czwórkowym ma 7 cyfr.

a) Ile będzie miała cyfr w zapisie ósemkowym?
b) Ile będzie miała cyfr w zapisie dwójkowym?

Zadanie 2.34. Pewna liczba x zapisana w zapisie ósemkowym ma 5 cyfr. Ile będzie miała cyfr w zapisie czwórkowym?

2.1 Reprezentacja liczb w komputerze

Zmienne typu `integer` przechowywane są zwykle w dwóch bajtach, czyli 16 bitach. Pierwszy bit określa znak liczby – jeżeli wynosi on `0`, to liczba jest dodatnia, w przeciwnym razie liczba jest ujemna.

- Jeżeli liczba jest dodatnia, to pozostałe piętnaście bitów stanowi zapis binarny tej liczby.
- Liczby ujemne przechowywane są w tak zwanym systemie uzupełnieniowym, tzn. liczba ujemna o wartości bezwzględnej x przedstawiana jest jako liczba $2^{16} - x$ w postaci binarnej.

Przykład 2.35. Rozważmy liczbę $(82)_{10}$. Jest ona liczbą dodatnią. Jej zapis w postaci binarnej to 1010010. Zatem jest ona przechowywana w postaci:

znak	15 bitów
0	000 0000 0101 0010

, czyli ostatecznie $82 = (0000\ 0000\ 0101\ 0010)_{\texttt{int}}$.

Przykład 2.36. Rozważmy liczbę $(-82)_{10}$. Jest ona liczbą ujemną. Zapis jej wartości bezwzględnej, czyli 82, w postaci binarnej to 1010010. Zatem jest ona przechowywana w postaci:

$$\begin{array}{rr} & 1\ \underbrace{0000\ 0000\ 0000\ 0000}_{16\text{ zer}} \\ - & \qquad\qquad 1010010 \\ \hline & 1111\ 1111\ 1010\ 1110 \end{array}$$

, czyli ostatecznie $-82 = (1111\ 1111\ 1010\ 1110)_{\texttt{int}}$.

Przykład 2.37. Rozważmy liczbę $(-82)_{10}$. Jest ona liczbą ujemną. Jej zapis w postaci `int` można również uzyskać następująco:

- Zapis jej wartości bezwzględnej na 16 bitach „zaprzeczamy" i dodajemy „1";

$$\begin{array}{rr} & 0000\ 0000\ 0101\ 0010 \\ \hline & 1111\ 1111\ 1010\ 1101 \\ + & 1 \\ \hline & 1111\ 1111\ 1010\ 1110 \end{array}$$

- Bądź też odejmujemy „1" od jej wartości bezwzględnej na 16 bitach i „zaprzeczamy".

$$\begin{array}{rr} & 0000\ 0000\ 0101\ 0010 \\ - & 1 \\ \hline & 0000\ 0000\ 0101\ 0001 \\ \hline & 1111\ 1111\ 1010\ 1110 \end{array}$$

Analogicznie przebiega ‚rozkodowywanie".

Przykład 2.38. Rozważmy liczbę 1111 1111 1010 1110. Jako że pierwszy bit jest równy `1`, zatem jest to liczba ujemna. Wyznaczamy ją następująco:

- Sposób 1:

$$\begin{array}{rr} & 1\ 0000\ 0000\ 0000\ 0000 \\ - & 1111\ 1111\ 1010\ 1110 \\ \hline & 0000\ 0000\ 0101\ 0010 \end{array}$$

, co daje nam 82, ale że pierwszy bit był równy 1, zatem kodowaną liczbą jest -82.

- Sposób 2 (zapis „zaprzeczamy" i dodajemy „1"):

$$\begin{array}{rr} & 1111\ 1111\ 1010\ 1110 \\ \hline & 0000\ 0000\ 0101\ 0001 \\ + & 1 \\ \hline & 0000\ 0000\ 0101\ 0010 \end{array}$$

, co daje nam 82, ale że pierwszy bit był równy 1, zatem kodowaną liczbą jest -82.

- Sposób 3 (odejmujemy „1" od zapisu i „zaprzeczamy"):

$$\begin{array}{rr} & 1111\ 1111\ 1010\ 1110 \\ - & 1 \\ \hline & 1111\ 1111\ 1010\ 1101 \\ \hline & 0000\ 0000\ 0101\ 0010 \end{array}$$

, co daje nam 82, ale że pierwszy bit był równy 1, zatem kodowaną liczbą jest -82.

Przykład 2.39. Rozważmy liczbę 0000 0000 0101 0010. Jako że pierwszy bit jest równy `0`, zatem jest to liczba dodatnia. Jako że jej zapis binarny to 1010010, zakodowaną liczbą jest $(82)_{10}$.

Zadanie 2.40. Korzystając z opisanych wyżej trzech różnych sposobów, zapisz w `int` następujące liczby:

a) 131 i -131.
b) 79 i -79.
c) 211 i -211.

Zadanie 2.41. Korzystając z opisanych wyżej trzech różnych sposobów, zapisz w systemie dziesiętnym następujące liczby zapisane w `int`:

a) 0000 0000 1111 0011 i 1111 1111 0000 1100.
b) 0000 0000 0110 0110 i 1111 1111 1001 1001.
c) 0000 0001 0001 0001 i 1111 1110 1110 1110.

2.2 Przeszukiwania binarne

Niech $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$. Załóżmy, że w grze przeciwnik wybiera x ze zbioru A, a my musimy za pomocą jak najmniejszej ilości pytań odgadnąć tą liczbę. Wówczas sposób postępowania może być następujący:

> Dzielimy A na $A_1 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ i $A_2 = \{8, 9, 10, 11, 12, 13, 14, 15\}$ i pytamy, do którego zbioru należy x. Następnie znowu dzielimy ten zbiór A_i na połowy i powtarzamy pytanie, itd.

Przykład 2.42. Niech $x = 10$.

$\{0, 1, 2, 3, 4, 5, 6, 7\}$	$\{8, 9, 10, 11, 12, 13, 14, 15\}$
Nie	Tak
$\{8, 9, 10, 11\}$	$\{12, 13, 14, 15\}$
Tak	Nie
$\{8, 9\}$	$\{10, 11\}$
Nie	Tak
$\{10\}$	$\{11\}$
Tak	Nie

,

czyli ostatecznie $x = 10$. Zadaliśmy 4 pytania. ♯

Powyższy sposób rozumowania można rozszerzyć na dowolny n-elementowy zbiór X: odgadnięcie elementu utożsamiamy z odgadnięciem liczby ze zbioru $\{0, 1, \ldots, n-1\}$, przy czym w najgorszym przypadku minimalna liczba pytań, jaką należy zadać to $\lceil \log_2 n \rceil$. Zatem np. mając do dyspozycji k pytań można odgadnąć całkowitą liczbę z przedziału od 0 do $2^k - 1$ (czyli element ze zbioru o mocy 2^k).

Zadanie 2.43.

a) Ile pytań należy zadać, aby odgadnąć liczbę z przedziału od 0 do 100000?
b) Ile pytań należy zadać, aby odgadnąć element ze zbioru X, gdzie:

$$X = \{x \in \mathbb{N} \mid 1 \leq x \leq 33\}?$$

c) Ile pytań należy zadać, aby odgadnąć element ze zbioru X, gdzie:

$$X = \{x \in \mathbb{N} \mid 1 \leq x \leq 30 \text{ i } x \text{ parzyste}\}?$$

Metodę poszukiwań binarnych można zastosować do stwierdzenia, czy jakaś liczba naturalna n jest kwadratem innej liczby naturalnej, tzn. czy istnieje naturalna liczba k taka, że $k^2 = n$.

Algorytm(`int` n)

1. $k_d := 1$; $k_g := n$.
2. Powtarzaj aż do skutku:
   - 2.a. Jeżeli $k_g - k_d \leq 1$, to KONIEC, n nie ma pierwiastka.
   - 2.b. $j := \lfloor \frac{k_g + k_d}{2} \rfloor$;
   - 2.c. Jeżeli $j^2 = n$, to KONIEC, n jest potęgą j;
   - 2.d. Jeżeli $j^2 > n$, to $k_g := j$, w przeciwnym wypadku $k_d := j$.

PRZYKŁAD 2.44. Zastosuj algorytm wyznaczania pierwiastków do znalezienia pierwiastka stopnia 2 z liczb 49 i 59.

k_d	k_g	$?(k_g - k_d \leq 1)$	j	$?(j^2 = n)$	$?(>,<)$
1	49	$?(49 - 1 \leq 1)$	25	$?(25^2 = 49)$	$>$
1	25	$?(25 - 1 \leq 1)$	13	$?(13^2 = 49)$	$>$
1	13	$?(13 - 1 \leq 1)$	7	$?(7^2 = 49)$	KONIEC

,

czyli ostatecznie istnieje $k = 7$ takie, że $k^2 = 49$.

k_d	k_g	$?(k_g - k_d \leq 1)$	j	$?(j^2 = n)$	$?(>,<)$
1	59	$?(59 - 1 \leq 1)$	30	$?(30^2 = 59)$	$>$
1	30	$?(30 - 1 \leq 1)$	15	$?(15^2 = 59)$	$>$
1	15	$?(15 - 1 \leq 1)$	8	$?(8^2 = 59)$	$>$
1	8	$?(8 - 1 \leq 1)$	4	$?(4^2 = 59)$	$<$
4	8	$?(8 - 4 \leq 1)$	6	$?(6^2 = 59)$	$<$
6	8	$?(8 - 6 \leq 1)$	7	$?(7^2 = 59)$	$<$
7	8	$?(8 - 7 \leq 1)$	KONIEC		

,

czyli ostatecznie nie istnieje k takie, że $k^2 = 59$. Jednakże z warunków zatrzymania algorytmu wynika, że otrzymaliśmy przybliżenia z dołu: $= 7$ i z góry: $= 8$. ♯

ZADANIE 2.45. Zastosuj algorytm wyznaczania pierwiastków dla znalezienia pierwiastka stopnia 2 z następujących liczb:

a) 144.
b) 123.
c) 625.
d) 517.

2.3 Waga

Rozważmy wagę szalkową, dla której na lewej szalce kładziemy jakiś przedmiot do zważenia, a następnie na obu szalkach kładziemy odważniki. Jeżeli waga jest w równowadze, wówczas ważony przedmiot ma wagę równą sumie wag odważników położonych na prawej szalce minus suma wag odważników położonych na lewej szalce obok ważonego przedmiotu. Zakładamy, że zarówno odważniki jak i sam ważony przedmiot posiadają wagi będące liczbami naturalnymi.

Przykład 2.46. Jak ułożyć na szalkach odważniki o nominałach $1, 3, 9, 27$, aby zważyć odważyć ciężar 35?

Rozwiązanie. W ogólności, rozłożenie k odważników przy odważaniu ciężaru W odpowiada przedstawieniu W w postaci $W = \sum_{i=0}^{k-1} d_i \cdot 3^i$, gdzie $d_i \in \{-1, 0, 1\}$. Aby przedstawić ciężar W w tej postaci, należy najpierw przedstawić liczbę $W^* = W + \frac{3^k-1}{2}$ w systemie trójkowym: $W^* = (e_{k-1} \dots e_0)_3$, a następnie za d_i podstawić $e_i - 1$. Zatem w rozważanym przykładzie, $W^* = 35 + \frac{3^4-1}{2} = 35 + 40 = 75 = 2 \cdot 27 + 2 \cdot 9 + 1 \cdot 3 + 0 \cdot 1 = (2210)_3$, stąd $d_0 = -1, d_1 = 0, d_2 = 1, d_3 = 1$. Zatem rozłożenie jest następujące: odważnik o nominale 1 na lewej szalce, odważnik o nominale 3 pozostaje na stole, a odważniki o nominałach 9 i 27 na prawej szalce $(35 + 1 = 27 + 9)$. ♯

Zadanie 2.47. Jak ułożyć na szalkach odważniki o nominałach $1, 3, 9, 27, 81$, aby zważyć odważyć ciężar: (a) 92, (b) 111?

Zadanie 2.48. Mając do dyspozycji po dwa odważniki każdego rodzaju z $1, 3, 9, 27$ wyznaczyć ułożenie odważników na szalkach tak, aby odważyć ciężar 65. Opisz sposób postępowania.

Analogiczne rozumowanie jak w przykładzie 2.46 można zastosować np. dla odważników innego rodzaju będącego potęgą jakiejś liczby p. Wówczas potrzebujemy odważników nie po jednym z każdego rodzaju, lecz po większej ilości: wynika to z zapisu w systemie o żądanej podstawie. Jeśli np. rozważymy system odważników o nominałach czterech kolejnych potęg $p = 5$, tzn. $1, 5, 25, 125$, wówczas kolejne cyfry w zapisie liczby $W^* = W + \frac{5^k-1}{2}$ w systemie o podstawie 4 należą do zbioru $0, \dots, 4$. Aby otrzymać żądany rozkład odważników na szalce, podstawiamy $d_i = e_i - \lfloor \frac{p}{2} \rfloor = e_i - 2$. Jako że $d_i \in \{-2, -1, 0, 1, 2\}$, potrzebujemy po dwa odważniki z każdego rodzaju.

Zadanie 2.49. Mając do dyspozycji po dwa odważniki każdego rodzaju z $1, 5, 25, 125$ wyznaczyć ułożenie odważników na szalkach tak, aby odważyć ciężar 164.

Odpowiedzi do zadań

2.2.

a) 11.
b) 59.
c) 94.

2.4.

a) 111111.
b) 110000.
c) 10100.

2.6.

a) $1111 < 10001$.
b) $11010 > 10111$.
c) $1111001 < 1111011$.

2.8.

a) $1111 + 1110 = 11101$.
b) $10011 + 1100 = 11111$.
c) $110111 + 110011 = 1101010$.
d) $101 + 111 + 111 = 10011$.
e) $1011 + 1011 + 111 = 11101$.

2.10.

a) $10011 - 1100 = 111$.
b) $110111 - 110011 = 100$.
c) $1010001 - 101110 = 100011$.
d) $1011100 - 1010111 = 101$.

2.12.

a) $101 \cdot 111 = 100011$.
b) $1111 \cdot 111 = 1101001$.
c) $10011 \cdot 1100 = 11100100$.
d) $111000 \cdot 111 = 1100010000$.

2.14.

a) $100011 : 101 = 111$.
b) $1101001 : 111 = 1111$.
c) $110001 : 111 = 111$.
d) $11000 : 1000 = 11$.
e) $1010001 : 1001 = 1001$.

2.16.

a) $(111)_{10} = (1101111)_2$.
b) $(169)_{10} = (10101001)_2$.
c) $(411)_{10} = (110011011)_2$.

2.20.

a) \$A91 $= (2705)_{10}$.
b) \$C2 $= (194)_{10}$.
c) \$FCA $= (4042)_{10}$.

2.22.

a) 199 = \$127.
b) 541 = \$21D.
c) 855 = \$357.

2.24.

a) \$A91 $= (101010010001)_2$.
b) \$C2 $= (11000010)_2$.
c) \$8CA $= (11110101010)_2$.

2.26.

a) $(1011101)_2$ = \$5D.
b) $(100010)_2$ = \$22.
c) $(111110110)_2$ = \$1F6.

2.29.

a) $0.5625 = (0.1001)_2$.
b) $0.15625 = (0.00101)_2$.
c) $0.328125 = (0.010101)_2$.
d) $0.78125 = (0.11101)_2$.
e) $7.5625 = (111.1001)_2$.
f) $11.15625 = (1011.00101)_2$.
g) $13.328125 = (1101.010101)_2$.

2.31.

a) 112.
b) 1220.
c) 1012
d) 223.
e) 1363.
f) 111.
g) 130563.

2.33.

a) 5 cyfr.
b) Jeśli liczba $x \in \{(1000000)_4, (1000001)_4, \ldots, (1333333)_4\}$, to w zapisie dwójkowym ma ona 13 cyfr, w przeciwnym wypadku, jeśli liczba $x \in \{(2000000)_4, \ldots, (3333333)_4\}$, to w zapisie dwójkowym ma ona 14 cyfr.

2.34. Jeśli liczba $x \in \{(10000)_8, (10001)_8, \ldots, (37777)_8]$, to w zapisie czwórkowym ma ona 7 cyfr, w przeciwnym wypadku, jeśli liczba $x \in \{(40000)_8, \ldots, (77777)_8\}$, to w zapisie czwórkowym ma ona 8 cyfr.

2.40.

a) 0000 0000 1000 0011, 1111 1111 0111 1101.
b) 0000 0000 0100 1100, 1111 1111 1011 0100.
c) 0000 0000 1101 0011, 1111 1111 0010 1101.

2.41.

a) 243, -244,
b) 102, -103,
c) 273, -274.

2.43.

a) $\lceil \log_2 100001 \rceil = 17$.
b) Jako że X ma 33 elementy, należy zadać co najwyżej $\lceil \log_2 33 \rceil = 6$ pytań.
c) Jako że X ma 15 elementów, należy zadać co najwyżej $\lceil \log_2 15 \rceil = 4$ pytania.

2.45.

a) $k = 12$,
b) $k_d = 11$, $k_g = 13$,
c) $k = 25$,
d) $k_d = 22$, $k_g = 23$.

2.47.

a) Lewa szalka — 1, prawa szalka — 3+9+81.
b) Lewa szalka — 0, prawa szalka — 3+27+81.

2.48. Jako że $1 + 3 + 9 + 27 = 40$ i mamy do wyboru po dwa odważniki każdego rodzaju, należy wyznaczyć ułożenie odważników dla $65 - 40 = 25$, zakładając, że mamy tylko jeden komplet odważników. Otrzymane ułożenie dla 25: lewa szalka — 3, prawa szalka — 1+27. W konsekwencji dla 65 ułożenie jest następujące: lewa szalka — 3, prawa szalka — 2×1+3+9+2×27. Zauważmy, że ułożenie to jest równoważne: lewa szalka — 0, prawa szalka — 2×1+9+2×27, gdyż w pierwszym ułożeniu mamy odważniki o wadze 3 na obu szalkach.

2.49. Lewa szalka — 1×1+2×5, prawa szalka — 1×125+2×25.

Zestaw zadań nr 3

Kombinatoryka

3.1 Wariacje z powtórzeniami

Twierdzenie 3.1 (Wariacje z powtórzeniami)
– *Liczba ciągów długości k ze zbioru $\{a, b\}$ wynosi 2^k.*
– *Liczba ciągów długości k ze zbioru n-elementowego wynosi n^k.*
– *Liczba funkcji z k-elementowego zbioru A w n-elementowy zbiór wynosi n^k.*

Przykład 3.1. Wypisz wszystkie funkcje $f\colon X \to Y$, gdzie:

a) $X = \{1, 2, 3\}$, $Y = \{a, b\}$;
b) $X = \{a, b\}$, $Y = \{1, 2, 3\}$.

Czy można policzyć, ile jest tych funkcji bez ich wypisywania?

Rozwiązanie.

a)

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$
1	a	b	a	a	b	b	a	b
2	a	a	b	a	b	a	b	b
3	a	a	a	b	a	b	b	b

Zgodnie z twierdzeniem 3.1, tych funkcji jest $2^3 = 8$.

b)

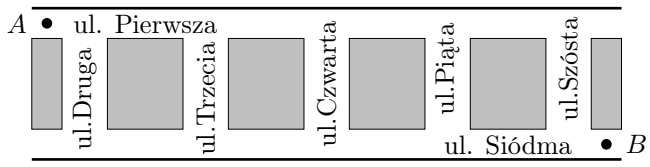
x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$	$f_9(x)$
a	1	2	3	1	2	3	1	2	3
b	1	1	1	2	2	2	3	3	3

Zgodnie z twierdzeniem 3.1, tych funkcji jest $3^2 = 9$. ♯

Przykład 3.2. Mamy 10 różnych piłek i 2 różne pudła. Każdą piłkę wrzucamy do jednego z pudeł. Na ile sposobów można to zrobić?

Rozwiązanie. Jako że powyższą sytuację można utożsamić z funkcją $f\colon \{p_1, p_2, \ldots, p_{10}\} \to \{1, 2\}$, która każdej z dziesięciu piłek przyporządkowuje numer pudła, liczba rozmieszczeń równa jest liczbie różnych funkcji f. Na mocy twierdzenia 3.1 liczba ta wynosi 2^{10}. ♯

Przykład 3.3. Pewna osoba miała przedostać się **najkrótszą** drogą z punktu A do punktu B (patrz poniższy rysunek), a następnie wrócić z punktu B do punktu A. Szła tylko narysowanymi ulicami. Na ile sposobów mogła wybrać trasę?



Rozwiązanie. Wybór najkrótszej drogi, zarówno tej 'do' jak i 'z', równoważny jest wyborowi którejś z pięciu dróg *Druga, Trzecia, Czwarta, Piąta, Szósta*. Jako że takiego wyboru dokonujemy dwa razy, liczba możliwości wynosi 5^2.

Istnieje też rozwiązanie bardziej formalne. Zauważmy, że istnieje wzajemna odpowiedniość pomiędzy najkrótszymi drogami 'do' i 'z', a funkcjami

$$f\colon\{\text{do},\text{z}\} \to \{\mathit{Druga}, \mathit{Trzecia}, \mathit{Czwarta}, \mathit{Piąta}, \mathit{Szósta}\},$$

a tym samym, na mocy twierdzenia 3.1, liczba różnych dróg/funkcji wynosi 5^2. ♯

Zadanie 3.4.

a) Ile istnieje liczb naturalnych 5-cyfrowych, w których zapisie nie występuje cyfra '0'?
b) Ile istnieje liczb naturalnych 5-cyfrowych?
c) Ile istnieje liczb naturalnych 5-cyfrowych takich, w których cyfrą setek jest '5'?

Zadanie 3.5.

a) Ile jest funkcji f ze zbioru $\{1,\ldots,n\}$ w zbiór $\{a,b,c\}$?
b) Ile spośród nich spełnia warunek $f(1)=a$?
c) Ile spośród nich spełnia warunek $f(1)\neq f(2)$?

Zadanie 3.6. Ile jest liczb trzycyfrowych w systemie:

a) dziesiętnym,
b) dwójkowym,
c) trójkowym?

Ile jest liczb trzycyfrowych z różnymi cyframi?

Zadanie 3.7. Rzucamy 3 razy monetą, a następnie 4 razy kostką do gry. Ile różnych wyników tego doświadczenia możemy uzyskać? (Zakładamy, że istotna jest kolejność).

Zadanie 3.8. Grupa znajomych przyszła do ciastkarni, w której było 8 rodzajów ciastek. Każdy kupił jedno ciastko. Z ilu osób składała się grupa, jeżeli wiadomo, że mogło być 512 różnych możliwości wyboru?

3.2 Wariacje bez powtórzeń

Twierdzenie 3.2 (Wariacje bez powtórzeń)
– *Liczba ciągów bez powtórzeń długości k ze zbioru n-elementowego wynosi*

$$n \cdot (n-1) \cdot \ldots \cdot ((n-k)+1).$$

– *Liczba różnowartościowych funkcji z k-elementowego zbioru A w n-elementowy zbiór wynosi*

$$n \cdot (n-1) \cdot \ldots \cdot ((n-k)+1).$$

Przykład 3.9. Wypisz wszystkie różnowartościowe funkcje $f\colon X \to Y$, gdzie: (a) $X = \{1,2,3\}$, $Y = \{a,b\}$; (b) $X = \{a,b\}$, $Y = \{1,2,3\}$. Czy można policzyć, ile jest tych funkcji bez ich wypisywania?

Rozwiązanie.

a) Zauważmy, że nie istnieje różnowartościowa funkcja $f\colon X \to Y$, gdzie $X = \{1,2,3\}$, $Y = \{a,b\}$, gdyż musimy trzem elementom z X przypisać różne wartości, a zatem tych wartości do wyboru powinno być przynajmniej trzy, a mamy do wyboru tylko dwie.

Zgodnie z twierdzeniem 3.2, tych funkcji jest $2 \cdot 1 \cdot 0 = 0$.

b)

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
a	1	1	2	2	3	3
b	2	3	1	3	1	2

Zgodnie z twierdzeniem 3.2, tych funkcji jest $3 \cdot 2 = 6$. ♯

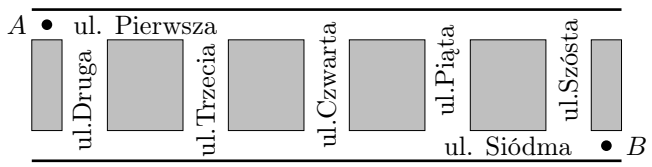
Przykład 3.10. W kawiarni, do której przyszło 7 osób, było 10 gatunków ciastek. Każdy kupił jedno ciastko, przy czym każdy kupił inne. Na ile sposobów można było kupić ciastka?

Rozwiązanie. Powyższą sytuację można utożsamić z różnowartościową funkcją

$$f\colon \{o_1, o_2, \ldots, o_7\} \to \{1, 2, \ldots, 10\},$$

która każdej z siedmiu osób przyporządkowuje inny rodzaj ciastka. Zatem liczba sposobów równa jest liczbie różnowartościowych funkcji f, która na mocy twierdzenia 3.2 wynosi $10 \cdot 9 \cdot \ldots \cdot 4$. ♯

Przykład 3.11. Pewna osoba miała przedostać sie **najkrótszą** drogą z punktu A do punktu B (patrz rysunek poniżej), a następnie wrócić z punktu B do punktu A. Szła tylko narysowanymi ulicami. Na ile sposobów mogła wybrać trasę, jeśli nie chciała wracać tą samą drogą?



Rozwiązanie. Zauważmy, że istnieje wzajemna odpowiedniość pomiędzy różnymi najkrótszymi drogami 'do' i 'z', a różnowartościowymi funkcjami

$$f\colon\{\text{do},\text{z}\} \to \{\textit{Druga}, \textit{Trzecia}, \textit{Czwarta}, \textit{Piąta}, \textit{Szósta}\},$$

stąd, na mocy twierdzenia 3.2, liczba różnowartościowych funkcji/tras wynosi $5 \cdot 4 = 20$. ♯

Zadanie 3.12.

a) Ile istnieje liczb naturalnych 5-cyfrowych o nie powtarzających się cyfrach takich, w których zapisie nie występuje cyfra '0'?
b) Ile istnieje liczb naturalnych 5-cyfrowych o nie powtarzających się cyfrach?
c) Ile istnieje liczb naturalnych 5-cyfrowych o nie powtarzających się cyfrach takich, w których cyfrą setek jest '5'?

Zadanie 3.13. W grupie składającej się z 3 dziewcząt i 5 chłopców, urodzonych w tym samym roku, żadna para dziewcząt i żadna para chłopców nie obchodzi urodzin tego samego dnia roku. Ile jest możliwości wystąpienia takiego zdarzenia ze względu na daty urodzin tych ośmiu osób?

Zadanie 3.14. Z ilu osób składa się grupa, jeżeli wiadomo, że na 5 miejscach osoby te mogą usiąść na 60 sposobów?

3.3 Permutacje

Twierdzenie 3.3 (Permutacje) *Liczba permutacji* (*czyli n-elementowych ciągów bez powtórzeń o elementach ze zbioru n-elementowego*) *wynosi*

$$n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!.$$

Przykład 3.15. Wypisz wszystkie różnowartościowe funkcje $f\colon X \to Y$, gdzie $X = \{1,2,3\}$, $Y = \{a,b,c\}$. Czy można policzyć, ile jest tych funkcji bez ich wypisywania?

Rozwiązanie.

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
1	a	a	b	b	c	c
2	b	c	a	c	a	b
3	c	b	c	a	b	a

Zgodnie z twierdzeniem 3.3, tych funkcji jest $3! = 6$. ♯

Przykład 3.16. Ile różnych 4-cyfrowych liczb można utworzyć z cyfr $1,2,3,4$ tak, aby żadna cyfra w liczbie nie powtarzała się?

Rozwiązanie. Jako że każda 4-cyfrowa liczba o niepowtarzających się cyfrach ze zbioru $\{1,2,3,4\}$ jednoznacznie odpowiada 4-elementowemu ciągowi bez powtórzeń, na mocy twierdzenia 3.3 liczb tych jest $4! = 24$. ♯

Zadanie 3.17.

a) Ile różnych 5-cyfrowych liczb można utworzyć z cyfr $1, 2, 3, 4, 5$ tak, aby żadna cyfra w liczbie nie powtarzała się?
b) Ile różnych 5-cyfrowych liczb można utworzyć z cyfr $1, 2, 3, 4, 5$ tak, aby żadna cyfra w liczbie nie powtarzała się i aby na miejscu dziesiątek stała '5' lub '4'?

Zadanie 3.18. Rodzina 6-osobowa (rodzice i czworo dzieci) ustawia się w szeregu do zdjęcia. Ile różnych fotografii można otrzymać, jeżeli:

a) każdy może stać obok każdego,
b) rodzice stoją na dwóch końcach szeregu?

Zadanie 3.19. 20-osobowa grupa wsiada do autobusu. Najpierw wsiada 12 pań, a za nimi 8 panów. Ile istnieje różnych możliwości tego zdarzenia?

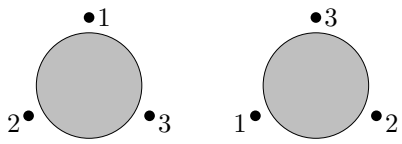
Zadanie 3.20. Ile jest różnych sposobów ustawienia na półce dzieła 5-tomowego tak, aby:

a) tomy I i II stały obok siebie,
b) tomy I i II nie stały obok siebie?

Zadanie 3.21. Na ile sposobów można rozsadzić:

a) 3 osoby na 3-osobowej karuzeli,
b) 4 osoby na 4-osobowej karuzeli,
c) n osób na n-osobowej karuzeli?

Uwaga. Jako że karuzela się kręci, dwa rozsadzenia uważamy za różne, jeżeli co najmniej jedna osoba ma co najmniej z jednej strony innego sąsiada — czyli rozsadzenia takie jak na poniższym rysunku są identyczne.



Zadanie 3.22. Na ile sposobów można rozsadzić przy okrągłym stole:

a) 3 osoby,
b) 4 osoby,
c) n osób?

Uwaga. Rozsadzenia przedstawione na powyższym rysunku traktujemy jako różne.

Zadanie 3.23. W ilu permutacjach zbioru $\{1, \ldots, 5\}$ jedynka stoi przed dwójką (niekoniecznie bezpośrednio)?

3.4 Permutacje z powtórzeniami

Twierdzenie 3.4 (Permutacje z powtórzeniami)
Niech dane będzie n elementów, gdzie elementów typu 1 (nierozróżnialnych) jest n_1, elementów typu 2 (nierozróżnialnych) jest n_2, ..., elementów typu k (nierozróżnialnych) jest n_k. Wówczas liczba sposobów, na które można uporządkować te elementy w rzędzie, wynosi

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! \cdot \ldots \cdot n_k!}.$$

Przykład 3.24. Ile różnych słów można utworzyć z liter słowa:

a) ULICA,
b) MARTA,
c) LALKA.

Rozwiązanie. Mając na uwadze z Twierdzenie 3.4 oraz:

a) że wszystkie litery w słowie ULICA są różne, otrzymujemy 5!.
b) że w słowie MARTA są dwie litery 'A', otrzymujemy $\frac{5!}{2!}$.
c) że w słowie LALKA mamy dwie litery 'L' i dwie litery 'A', otrzymujemy $\frac{5!}{2!2!}$. ♯

Zadanie 3.25. Ile różnych liczb 5-cyfrowych można utworzyć z cyfr $1, 1, 1, 2, 2$?

Zadanie 3.26. Ile różnych nieparzystych liczb 6-cyfrowych można utworzyć z cyfr $2, 2, 4, 4, 7, 9$?

Zadanie 3.27. Na ile różnych sposobów można nawlec na sznurek 10 korali: 4 czarne, 4 czerwone i 2 białe, jeśli ustalimy początek i koniec sznurka? A jeśli potraktujemy sznurek jako naszyjnik?

3.5 Kombinacje

Twierdzenie 3.5 (Kombinacje)
Liczba wyborów k-elementowego podzbioru ze zbioru n-elementowego wynosi

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

Przykład 3.28. Na ile sposobów można podzielić grupę 8-osobową na dwie grupy: 5-osobową i 3-osobową? Na ile sposobów można podzielić grupę 8-osobową na dwie równe grupy?

Rozwiązanie. Zauważmy, że wybór trzech osób z ośmiu automatycznie wyznacza wybór pięciu osób z tej samej grupy. Tym samym sposobów podziału grupy 8-osobowej na dwie grupy (5-osobową i 3-osobową) jest $\binom{8}{3} = 56$. Co więcej, powyższa obserwacja implikuje, że $\binom{8}{3} = \binom{8}{5}$, a w ogólności $\binom{n}{k} = \binom{n}{n-k}$. Jeśli natomiast rozważymy wybór czteroosobowej grupy, wówczas musimy pamiętać, że temu samemu podziałowi odpowiadają dwa różne wybory grupy, tzn. wybór osób $1, 2, 3, 4$ z ośmiu i otrzymany podział jest równoważny wyborowi osób $5, 6, 7, 8$, bo podział jest ten sam, zatem rozważanych podziałów jest $\frac{1}{2} \cdot \binom{8}{4} = 35$. ♯

Zadanie 3.29. Mamy do wyboru 3 rodzaje chlebów i 4 rodzaje bułek. Chcemy kupić 2 różne chleby i 2 różne bułki. Na ile sposobów możemy to zrobić?

Zadanie 3.30. Ustawiamy 30 różnych książek na 4 półkach tak, aby na pierwszej półce było 10 książek, na drugiej – 8, na trzeciej – 7, a na czwartej – 5). Ile jest takich ustawień, gdy nieistotne jest ustawienie/kolejność książek na półce, a ile w przypadku, gdy kolejność/ustawienie jest istotne?

Przypomnijmy, że w kartach do gry mamy cztery *kolory* — jest to kier ♡, karo ♢, trefl ♣ oraz pik ♠. *Parę* stanowią dwie te same figury ze zbioru {9,10,W,D,K,A} (w przypadku talii złożonej z 24 kart) lub ze zbioru {2,3,4,5,6,7,8,9,10,W,D,K,A} (w przypadku talii złożonej z 52 kart); analogicznie, *trójkę* stanowią trzy te same figury, np. trzy damy, a *kareta* to cztery figury, np. kareta asów.

Zadanie 3.31. Z talii 52 kart losujemy 10 kart. Ile istnieje możliwych wyników losowania, w których wylosujemy 2 damy?

Zadanie 3.32. Z talii 24 kart wybieramy 5 kart. Ile jest takich wyborów, w których dostaniemy:

a) 5 kart w jednym kolorze,
b) 1 parę i 1 trójkę,
c) 2 pary różnych figur,
d) 2 pary?

Zadanie 3.33. Na ile sposobów można utworzyć 5 par z 10 osób?

Zadanie 3.34. Na ile sposobów można rozdać 52 karty czterem osobom (po równo)?

Zadanie 3.35. Znajdź liczbę rozdań przy grze w brydża, w których każdy z grających otrzyma dokładnie jednego asa i jednego króla.

Zadanie 3.36. Z ilu osób składa się klasa, jeżeli wiadomo, że 2-osobową delegację można wybrać na 300 sposobów?

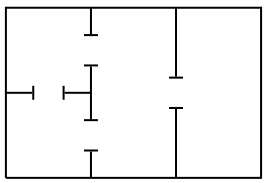
3.6 Zadania różne

Zadanie 3.37. Ile prostych można przeprowadzić przez 5 punktów, z których żadne 3 nie są współliniowe?

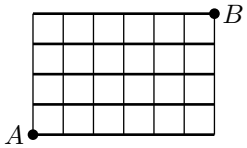
Zadanie 3.38. Ile przekątnych ma:

a) siedmiokąt wypukły,
b) n-kąt wypukły?

Zadanie 3.39. Pokoje w mieszkaniu, którego plan przedstawia poniższy rysunek, mają być pomalowane w taki sposób, aby pokoje mające wspólne drzwi były pomalowane różnymi kolorami. Na ile sposobów można pomalować mieszkanie mając do dyspozycji n kolorów?



Zadanie 3.40. Wyobraźmy sobie, że poniższy rysunek przedstawia prostokątną kratę ulic 6×4. Chcemy przejść ulicami od A do B idąc najkrótszą drogą. Ile jest takich dróg? Uogólnij wynik na kratę o dowolnych wymiarach $n \times k$.



Zadanie 3.41.

a) Ile rozwiązań ma równanie $x_1 + x_2 + x_3 + x_4 + x_5 = 6$, gdzie każde x_i jest nieujemną liczbą całkowitą?

Wskazówka. Rozważyć prostokątną kratę 6×4 i najkrótsze drogi z lewego dolnego rogu do prawego górnego rogu.

b) Ile rozwiązań ma równanie $x_1 + x_2 + \ldots + x_k = n$, gdzie każde x_i jest nieujemną liczbą całkowitą?

Zadanie 3.42. Załóżmy, że mamy przedmioty w k różnych typach, że liczba przedmiotów każdego typu jest nieograniczona oraz że przedmioty jednego typu są nierozróżnialne. Na ile sposobów można wybrać n przedmiotów spośród tych k typów przy założeniu, że dopuszczalne są powtórzenia typów i że kolejność wybranych przedmiotów jest nieistotna?

Wskazówka. Patrz poprzednie zadanie.

Zadanie 3.43. W kolejce do kina stoi n osób. Osoby te są wpuszczane do kina w k grupach, z których każda składa się z jednej lub więcej osób. Na ile sposobów można utworzyć tych k grup?

Wskazówka. Rozważyć wstawianie „bramek" pomiędzy osoby jako podział na grupy.

Zadanie 3.44. Ile rozwiązań ma równanie $x_1 + x_2 + \ldots + x_k = n$, gdzie każde x_i jest dodatnią liczbą całkowitą?

Wskazówka. Patrz poprzednie zadanie.

Zadanie 3.45. Zastosować odpowiedź do poprzedniego zadania w celu przedstawienia uzasadnienia, że liczba rozwiązań równania $x_1 + x_2 + \ldots + x_k = n$, gdzie każde x_i jest nieujemną liczbą całkowitą, wynosi $\binom{n+k-1}{k-1}$.

Wskazówka. Rozważyć podstawienie $y_i = x_i + 1$ oraz odpowiednio powstałe równanie.

Zadanie 3.46. Mamy 30 jednakowych piłek, które wrzucamy do różnych 5 pudeł. Ile jest takich rozmieszczeń, że żadne pudło nie jest puste?

Zadanie 3.47. Mamy r jednakowych kul i n różnych komórek. Ile jest takich rozmieszczeń kul w komórkach, że żadna komórka nie jest pusta?

Zadanie 3.48. Mamy r jednakowych kul i n różnych komórek. Ile jest wszystkich możliwych rozmieszczeń kul w komórkach?

Zadanie 3.49. W poczekalni u lekarza w rzędzie z n krzeseł siedzi k pacjentów w ten sposób, że żadni dwaj z nich nie znajdują się na sąsiednich krzesłach. Na ile sposobów może być wybrany odpowiedni zbiór krzeseł?

Zadanie 3.50. Jeżeli na obwodzie koła jest rozmieszczonych n punktów i każda para punktów jest połączona linią prostą, to koło dzieli się na pewną liczbę obszarów. Pokazać, że jeśli żadne trzy proste nie przetną się wewnątrz koła, to liczba obszarów będzie równa co najwyżej $1+n+\binom{n}{2}$.

3.7 Własności

Przykład 3.51. Wykaż, że $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Rozwiązanie. Lewą stronę równania stanowi ilość wyborów k liczb ze zbioru $\{1, 2, \ldots, n\}$. Zauważmy, że zbiory k-elementowe można podzielić na te, które zawierają liczbę n, oraz te, które jej nie zawierają. W pierwszym przypadku tych zbiorów jest $\binom{n-1}{k-1}$ (bo zakładając, że n należy do zbioru, pozostaje wybrać $k-1$ elementów ze zbioru $\{1, \ldots, n-1\}$), w drugim natomiast tych zbiorów jest $\binom{n-1}{k}$ (bo wybieramy k liczb ze zbioru $\{1, 2, \ldots, n-1\}$). I dokładnie suma ilości tych wyborów jest po prawej stronie równania.

Powyższą równość można wykazać też rozwijając lewą stronę równania. A dokładnie:

$$\begin{aligned}\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!\cdot((n-1)-(k-1))!} + \frac{(n-1)!}{k!\cdot(n-k-1)!} \\ &= \frac{k\cdot(n-1)!}{k\cdot(k-1)!\cdot(n-k)!} + \frac{(n-1)!\cdot(n-k)}{k!\cdot(n-k-1)!\cdot(n-k)} \\ &= \frac{(n-1)!\cdot(k+n-k)}{k!\cdot(n-k)!} = \frac{(n-1)!\cdot n}{k!\cdot(n-k)!} = \frac{n!}{k!\cdot(n-k)!} = \binom{n}{k}.\end{aligned}$$

Zauważmy na koniec, że z definicji zachodzi $\binom{n}{n_1} = \binom{n}{n_1, n_2}$ dla dowolnych n_1 i n_2 takich, że $n_1 + n_2 = n$, a zatem, ponieważ $\binom{n-1}{n_1-1, n_2} = \binom{n-1}{n_1-1}$ oraz $\binom{n-1}{n_1, n_2-1} = \binom{n-1}{n_1}$, powyższą równość możemy zapisać jako

$$\binom{n}{a, b} = \binom{n-1}{a-1, b} + \binom{n-1}{a, b-1}.$$

♯

Zadanie 3.52. Niech a, b i c będą liczbami naturalnymi takimi, że $a + b + c = n$. Wykaż, że

$$\binom{n}{a, b, c} = \binom{n-1}{a-1, b, c} + \binom{n-1}{a, b-1, c} + \binom{n-1}{a, b, c-1}.$$

Przykład 3.53. Udowodnij równość $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \ldots + \binom{k}{k-1} + \binom{k-1}{k-1}$.

Rozwiązanie. Zauważmy, że lewa strona jest z definicji ilością wyborów k liczb ze zbioru $\{1, 2, \ldots, n\}$. Z drugiej strony, zauważmy, że wśród wszystkich podzbiorów k-elementowych można wyróżnić te, które mają 1 jako najmniejszy element, następnie te, które mają 2 jako najmniejszy element, ..., i na koniec te, które mają $n-k$ jako najmniejszy element — i dokładnie suma ilości tych wyborów jest po prawej stronie równania. ♯

Zadanie 3.54. Udowodnij równość $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Wskazówka. Rozważyć ilość wszystkich podzbiorów zbioru n-elementowego.

Zadanie 3.55. Udowodnij równość $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^{n-1}\binom{n}{n-1} + (-1)^n\binom{n}{n} = 0$.

Wskazówka. Skorzystać z własności z Przykładu 51.

Zadanie 3.56. Udowodnij równość $\sum_{r=0}^{k} \binom{n}{r}\binom{m}{k-r} = \binom{m+n}{k}$.

Wskazówka. Rozważyć wybór k osób spośród grupy n kobiet i m mężczyzn.

Zadanie 3.57. Udowodnij równość $\sum_{i=0}^{n} \binom{n}{i}\binom{n-i}{k-i} = 2^k\binom{n}{k}$.

Wskazówka. Rozważyć kolorowanie k spośród n obiektów, mając do dyspozycji dwa kolory.

Zadanie 3.58. Udowodnij równość $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

Wskazówka. Rozważyć wybór n osób spośród grupy n kobiet i n mężczyzn.

Zadanie 3.59. Z powyższego zadania możemy wywnioskować, że chcąc wybrać z grupy $2n$ osób, składającej z n kobiet i n mężczyzn, podzbiór o takiej samej liczbie kobiet i mężczyzn, podzbiór ten może być wybrany na $\binom{2n}{n}$ sposobów. Zakładając, że po wybraniu takiego podzbioru chcemy ustalić ponadto przywódcę wśród mężczyzn i przywódczynię wśród kobiet, wywnioskować, że $\sum_{k=1}^{n} k^2\binom{n}{k}^2 = n^2\binom{2n-2}{n-1}$.

Wskazówka. Rozważyć wybór grupy z przywódcą.

Zadanie 3.60. Udowodnij równość $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$.

Wskazówka. Rozważyć sytuację, w ktorej mamy dokonać wyboru m osobowej delegacji spośród n osób, a następnie w tej delegacji wybrać k-osobowy zarząd.

Zadanie 3.61. Udowodnij równość: $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$.

Wskazówka. Rozważyć równanie $(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k$, pochodną oraz podstawienie $x = 1$.

3.8 Zasada włączania i wyłączania

Twierdzenie 3.6 (Zasada włączania i wyłączania)

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|,$$

$$|\bigcup_{i=1}^{n}| = \sum_{\substack{I \subset \{1,\ldots,n\} \\ I \neq \emptyset}} (-1)^{|I|+1}|A_I|, \ \textit{gdzie}\ A_I = \bigcap_{i \in I} A_i.$$

Przykład 3.62. Wyznacz liczbę elementów $|A \cap B \cap C|$ oraz $|C|$ wiedząc, że $|A| = 12$, $|B| = 10$, $|A \cap B| = 4$, $|B \cap C| = 2$, $|A \cap C| = 2$, $|A \cup B \cup C| = 20$.

Rozwiązanie. Na podstawie zasady włączania-wyłączania otrzymujemy, że $|C| + |A \cap B \cap C| = 6$. Zauważmy, że $|A \cap B \cap C| \leq |B \cap C| = 2$, a zatem $|A \cap B \cap C|$ może byc równe $0, 1$ lub 2. Otrzymujemy wtedy, że $|C| \in \{4, 5, 6\}$. ♯

Przykład 3.63. Oblicz, ile dodatnich liczb mniejszych od 100 jest podzielnych przez $2, 3$ lub 5.

Rozwiązanie. Niech D oznacza zbiór liczb podzielnych przez 2, T przez 3 i P przez pięć, $D \cap P$ zbiór liczb podzielnych przez 2 i 5, itp. Z zasady włączania-wyłączania otrzymujemy, że $|D \cup T \cup P| = 49 + 33 + 19 - 16 - 9 - 6 + 3 = 73$. ♯

Zadanie 3.64. Wyznacz liczbę elementów $|A \cap B \cap C|$ oraz $|C|$ wiedząc, że $|A| = 10$, $|B| = 9$, $|A \cap B| = 3$, $|A \cap C| = 1$, $|B \cap C| = 1$, $|A \cup B \cup C| = 18$.

Zadanie 3.65. Ile osób jest w grupie, jeśli wiemy, że 10 zna Francuski, 15 zna Szwedzki, 12 zna Duński? Ponadto spośród nich 5 zna Francuski i Szwedzki, 4 zna Francuski i Duński, a 3 Szwedzki i Duński. Tylko 2 zna wszystkie 3 języki.

Zadanie 3.66. Ile osób jest w grupie, jeśli wiemy, że 18 zna Francuski, 11 zna Niemiecki, 15 zna Duński, 13 zna Turecki, Duński i Turecki zna 8, Francuski i Niemiecki zna 9, Turecki i Francuski zna 7, Duński i Francuski zna 8, Niemiecki i Turecki zna 9, Niemiecki i Duński zna 5, Niemiecki i Francuski i Duński zna 3, Niemiecki i Francuski i Turecki zna 4, Francuski i Duński i Turecki zna 3, Niemiecki i Francuski i Turecki i Duński zna 2?

Zadanie 3.67. Oblicz, ile dodatnich liczb mniejszych od 100 nie jest podzielnych przez żadną z liczb $2, 3, 5$ lub 7.

3.9 Zasada szufladkowa Dirichleta

Przykład 3.68. Pewna grupa ludzi wita się podając sobie ręce. Nikt nie wita się z samym sobą, a żadna para nie wita się więcej niż raz. Pokazać, że będą istniały 2 osoby, które witały się tyle samo razy.

Rozwiązanie. Mamy n osób. Możliwe liczby powitań to od 0 do $n-1$, przy czym nie jest możliwe, by jednocześnie występowała osoba z 0 i osoba z $n-1$ powitaniami. Zatem liczba możliwych różnych ilości powitań jest równa co najwyżej $n-1$. Skoro osób jest n, z zasady szufladkowej Dirichleta otrzymujemy tezę. ♯

Zadanie 3.69. Paweł ma w szufladzie 200 białych skarpetek i 300 czarnych. Lewe skarpetki są nieodróżnialne od prawych. Niestety Paweł nie potrafi odróżnić koloru białego od czarnego. Ile skarpetek musi on zabrać, aby mieć pewność, że choć dwie będą tego samego koloru? Ile skarpetek musi on zabrać, aby mieć pewność, że choć 10 będzie tego samego koloru?

Zadanie 3.70. Pokazać, że wśród 25 studentów zdających egzamin zawsze znajdzie się pięciu, którzy otrzymali tę samą ocenę przy skali ocen: 2, 3, 3+, 4, 4+, 5.

Zadanie 3.71. Uzasadnij, że wśród dowolnych 14 liczb naturalnych znajdziemy dwie, które przy dzieleniu przez 13 dają tę samą resztę.

Zadanie 3.72. Mając danych 10 dowolnych różnych liczb dodatnich mniejszych od 107 pokazać, że będą istniały dwa rozłączne podzbiory tych liczb, których elementy dają taką samą sumę.

Zadanie 3.73. Udowodnij, że wśród dowolnych $n+1$ liczb całkowitych będzie istniała para liczb różniących się o wielokrotność n.

> *Wskazówka.* Mając dane liczby $l_0, \ldots, l_n$ rozważyć n szufladek ponumerowanych $0, 1, \ldots, n-1$. Następnie rozważyć każdą z liczb $l_i - l_0$ i włożyć ją do szufladki odpowiadającej reszcie z dzielenia tej liczby przez n.

Zadanie 3.74. Uzasadnij, że wśród dowolnych pięciu punktów należących do wnętrza kwadratu o boku 2 zawsze są dwa punkty odległe o nie więcej niż $\sqrt{2}$.

> *Wskazówka.* Podzielić kwadrat 2×2 na cztery jednakowe „szufladki”.

Zadanie 3.75. Udowodnij, że wśród dowolnych $n+1$ liczb całkowitych ze zbioru $\{1, 2, \ldots, 2n\}$ istnieje taka, która jest wielokrotnością innej.

Wskazówka. Rozważyć n szuflad ponumerowanych kolejnymi liczbami nieparzystymi $1, 3, \ldots, 2n-1$. Każdą z wylosowanych liczb wkładamy do szuflady z numerem m, jeżeli $k = 2^r m$ dla jakiegoś $r \geq 0$.

3.10 Algorytmy generowania podzbiorów i permutacji

Algorytm generowania podzbiorów zbioru $\{1, \ldots, n\}$.

- pierwszy podzbiór to $\emptyset$;
- kolejny podzbiór po podzbiorze A:
  - $\star$ znajdujemy największy element nie należący do A, czyli $a = \max\{i \notin A\}$;
  - $\star$ jeżeli nie ma takiego a, to rozważany podzbiór A jest ostatnim – Koniec;
  - $\star$ w przeciwnym przypadku, dodajemy a do zbioru A i usuwamy z A wszystkie elementy większe od a.

Przykład 3.76. Rozważmy zbór $\{1, 2, 3, 4, 5, 6\}$ i załóżmy, że wygenerowaliśmy podzbiór $A = \{1, 2, 3, 6\}$. Spośród elementów nienależących do A algorytm znajduje największy, czyli $a = 5$. Wstawiamy 5 do A i usuwamy wszystkie $x > 5$, czyli tutaj tylko 6, otrzymując $\{1, 2, 3, 5\}$. ♯

Zadanie 3.77. Wypisz 10 kolejnych podzbiorów zbioru $\{1, 2, 3, 4, 5, 6\}$.

Zadanie 3.78. Wypisz 10 kolejnych podzbiorów zbioru $\{1, 2, 3, 4, 5, 6, 7\}$ poczynając od podzbioru $\{1, 2, 3, 5\}$.

Algorytm generowania k-elementowych podzbiorów $\{1, \ldots, n\}$.

- pierwszy podzbiór to $\{1, \ldots, k\}$;
- kolejny podzbiór po podzbiorze $A = \{a_1, \ldots, a_k\}$, gdzie $a_1 < \ldots < a_k$:
  - $\star$ znajdujemy najmniejsze i takie, że $a_i + 1 \notin A$;
  - $\star$ jeżeli $a_i = a_n$, to rozważany podzbiór $A = \{n-k+1, \ldots, n\}$ jest ostatnim – Koniec;
  - $\star$ w przeciwnym przypadku, zwiększamy a_i o jeden, a elementy mniejsze od a_i zamieniamy na $i-1$ najmniejszych kolejnych liczb, tzn. $a_j := j$, dla $j < i$.

Przykład 3.79. Rozważmy zbiór $\{1, 2, 3, 4, 5, 6, 7\}$ i załóżmy, że wygenerowaliśmy już podzbiór $\{2, 3, 4, 6\}$. Algorytm znajduje $i = 3$, bo $a_i = 4$ i $a_i + 1 = 5 \notin \{2, 3, 4, 6\}$. Zatem $a_i := a_i + 1 = 5$, a elementy a_1, a_2 przyjmują odpowiednio wartości 1 i 2. Zatem kolejny podzbiór to $\{1, 2, 5, 6\}$. ♯

Zadanie 3.80. Wypisz 10 kolejnych 3-elementowych podzbiorów zbioru $\{1, 2, 3, 4, 5, 6\}$.

Zadanie 3.81. Wypisz 10 kolejnych 5-elementowych podzbiorów zbioru $\{1, 2, 3, 4, 5, 6, 7\}$.

Algorytm generowania permutacji zbioru $\{1, \ldots, n\}$.

- pierwsza permutacja to $a_i = i$, dla $1 \geq i \geq n$,
- kolejna permutacja po permutacji $(a_1 \ldots a_n)$:
  - $\star$ znajdujemy największe j spełniające warunek $a_j < a_{j+1}$
  - $\star$ jeżeli nie ma takiego j, to rozważana permutacja jest permutacją ostatnią – KONIEC
  - $\star$ w przeciwnym przypadku, zamieniamy a_j z najmniejszym a_k takim, że $a_k > a_j$ i $k > j$, a następnie odwracamy porządek elementów $a_{j+1}, \ldots, a_n$

PRZYKŁAD 3.82. Rozważmy permutację (436521). Algorytm znajduje $j = 2$ i $a_j = 3$. Mamy $3 < 6 = a_3$ oraz $3 < 5 = a_4$, zatem zamieniamy a_2 z a_4. Następnie odwracamy kolejność elementów a_3, a_4, a_5, a_6, otrzymując (451236).

ZADANIE 3.83. Wypisz 10 kolejnych permutacji zbioru $\{1, 2, 3, 4, 5, 6\}$ poczynając od permutacji (456321).

ZADANIE 3.84. Wypisz 10 kolejnych permutacji zbioru $\{1, 2, 3, 4, 5, 6, 7\}$ poczynając od permutacji (5463721).

3.11 Permutacje raz jeszcze

Na permutację n-elementową można patrzeć jak na dowolną różnowartościową funkcję ze zbioru $\{1, 2, \ldots, n\}$ na ten sam zbiór. Na oznaczenie permutacji π używa się zapisu

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}.$$

Przykładem permutacji jest

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix},$$

która jest funkcją przyjmującą następujące wartości: $\pi(1) = 2$, $\pi(2) = 5$, $\pi(3) = 4$, $\pi(4) = 3$ oraz $\pi(5) = 1$. Dwie permutacje można składać tak, jak się składa funkcje. Złożenie permutacji π_1 i π_2 określone jest wzorem

$$\pi_1 \circ \pi_2(x) = \pi_1(\pi_2(x)).$$

Na przykład dla permutacji

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \text{ oraz } \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

ich złożenie $\pi = \pi_1 \circ \pi_2$ wynosi

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix},$$

ponieważ $\pi(1) = \pi_1(\pi_2(1)) = \pi_1(3) = 4$, $\pi(2) = \pi_1(\pi_2(2)) = \pi_1(1) = 2$,
$\pi(3) = \pi_1(\pi_2(3)) = \pi_1(4) = 3$, oraz $\pi(4) = \pi_1(\pi_2(4)) = \pi_1(2) = 1$.

Zbiór S_n wszystkich permutacji na zbiorze $\{1, 2, \ldots, n\}$ z działaniem złożenia ma następujące własności:

a) Złożenie permutacji jest łączne, czyli, dla każdych trzech permutacji π_1, π_2 oraz π_3 zachodzi

$$\pi_1 \circ (\pi_2 \circ \pi_3) = (\pi_1 \circ \pi_2) \circ \pi_3.$$

b) Wśród permutacji istnieje identyczność id, czyli permutacja, która każdemu x z dziedziny przypisuje wartość $id(x) = x$. Identyczność jest elementem neutralnym operacji składania permutacji, ponieważ dla każdej permutacji π zachodzi

$$\pi \circ id = id \circ \pi = \pi.$$

c) Dla każdej permutacji π istnieje permutacja odwrotna (funkcja odwrotna) π^{-1} spełniająca warunek

$$\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = id.$$

Na przykład dla permutacji

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

permutacją odwrotną π^{-1} jest

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}.$$

Możemy sprawdzić np. dla $x = 3$:

$$\pi \circ \pi^{-1}(3) = \pi(\pi^{-1}(3)) = \pi(4) = 3.$$

Wyznaczenie permutacji odwrotnej odbywa się w następujący sposób: jeśli $\pi(x) = y$, to $\pi^{-1}(y) = x$, gdyż wówczas otrzymamy $\pi \circ \pi^{-1}(y) = \pi(\pi^{-1}(y)) = \pi(x) = y = id(y)$.

Zadanie 3.85. Mając dane poniżej permutacje π_1 i π_2, oblicz $\pi_1 \circ \pi_2$, $\pi_2 \circ \pi_1$, π_1^{-1}, π_2^{-1}.

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

Przykład 3.86. Wypisz wszystkie 4-elementowe permutacje spełniające warunek $\pi(2) = 4$ (porównaj z Zadaniem 3.17).

Rozwiązanie.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$ ♯

Zadanie 3.87. Ile jest 6-elementowych permutacji π spełniających warunek:

a) $\pi(2) = 3$;
b) $\pi(2) = 3$ oraz $\pi(3) = 2$?

Zadanie 3.88. Wyznacz liczbę permutacji π ze zbioru S_6, które spełniają $\pi^2 = id$, $\pi \neq id$.

Często stosuje się *cykliczną* notację permutacji. Rozważmy dla przykładu permutację

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

Zauważmy, że $\pi(1) = 2, \pi(2) = 5$ oraz $\pi(5) = 1$ — mówimy tym samym, że elementy $1, 2$ oraz 5 tworzą *cykl* (1 2 5) długości 3. Analogicznie, mając na uwadze, że $\pi(3) = 4$ oraz $\pi(4) = 3$, otrzymujemy cykl (3 4) długości 2. Permutację π możemy teraz zapisać jako

$$\pi = (1\ 2\ 5) \circ (3\ 4),$$

albo równoważnie

$$\pi = (1\ 2\ 5)(3\ 4) \quad \text{(tzn. bez znaku operatora } \circ).$$

Dowolną permutację π zbioru $X = \{1, \ldots, n\}$ możemy rozłożyć na rozłączne cykle w sposób następujący:

1) Wybieramy dowolny element $x \in X$, który nie jest jeszcze w żadnym cyklu.

2) Iterujemy permutację π otrzymując kolejno:

$$x, \pi^1(x), \pi^2(x), \pi^3(x), \ldots$$

aż do uzyskania $\pi^j(x) = x$, gdzie $\pi^i(x) = \underbrace{\pi \circ \ldots \circ \pi}_{i \text{ razy}}(x)$, $i = 1, 2, \ldots, j$.

3) Dodajemy do rozkładu cykl $\Big(x\ \pi^1(x)\ \pi^2(x)\ \pi^3(x)\ \ldots\ \pi^{j-1}(x)\Big)$.

4) Jeśli w zbiorze X pozostały jeszcze elementy niepokryte przez żaden cykl, to wracamy do kroku (1) naszej procedury.

Jeśli permutacja π złożona jest z k rozłącznych cykli, to zapisujemy ją jako

$$\pi = (x_1\ \ldots)(x_2\ \ldots)\ldots(x_k\ \ldots),$$

gdzie w kolejnych nawiasach są elementy kolejnych cykli zaczynających się odpowiednio od $x_1, \ldots, x_k$. Należy podkreślić, że nie ma znaczenia kolejność cykli, ani to, od jakiego elementu zaczynamy cykl — np. (1 2 5)(3 4) i (3 4)(2 5 1) oznaczają tę samą permutację — ważne natomiast są długości cykli i kolejność elementów je tworzących. A dokładnie, zachodzi następujące twierdzenie.

Twierdzenie 3.7 (Rozkład permutacji na cykle) *Rozkład permutacji na cykle jest jednoznaczny z dokładnością do kolejności cykli i elementów początkowych.*

Przykład 3.89. Rozważmy permutację

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 1 & 5 & 2 & 6 & 9 & 8 \end{pmatrix}.$$

Rozkład π na cykle jest następujący:

- pierwszy cykl: $1, \pi(1) = 3, \pi(3) = 7, \pi(7) = 6, \pi(6) = 2, \pi(2) = 4, \pi(4) = 1$;
- drugi cykl: $5, \pi(5) = 5$;
- trzeci cykl: $8, \pi(8) = 9, \pi(9) = 8$.

Otrzymujemy ostatecznie $\pi = (1\ 3\ 7\ 6\ 2\ 4)(5)(8\ 9)$. ♯

Zadanie 3.90. Niech $\pi_1 = (1\ 2\ 3)(4\ 5\ 6)(7\ 8)$ oraz $\pi_2 = (1\ 3\ 5\ 7)(2\ 6)(4)(8)$. Wyznacz $\pi_1 \circ \pi_2$, $\pi_2 \circ \pi_1$, π_1^2, π_1^3, π_2^2, π_2^3 oraz π_1^{-1}, i przedstaw je w postaci cyklicznej.

Zadanie 3.91. Permutacja $\pi \in S_n$ jest nazywana *cykliczną*, jeśli jest postać w notacji cyklicznej składa się z jednego cyklu długości n. Wykaż, że istnieje dokładnie $(n-1)!$ permutacji cyklicznych w zbiorze S_n.

Przykład 3.92. Dwanaście kart ponumerowanych $1, \ldots, 12$ leży na stole w następujący sposób:

$$\begin{array}{ccc} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \\ 10 & 11 & 12 \end{array}$$

Zbieramy te karty od lewej do prawej, z kolejnych 4 wierszy, a następnie rozkładamy je, ale tym razem z góry na dół, w kolejnych 3 kolumnach.

$$\begin{array}{ccc} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{array}$$

Ile razy musimy powtórzyć powyższą operację, aby otrzymać pierwotne ułożenie kart?

Rozwiązanie. Niech π będzie permutacją, która określa zmianę ułożenia kart, a dokładnie, mamy $\pi(i) = j$, jeśli karta j pojawia się na pozycji zajmowanej uprzednio przez kartę i. Wówczas notacja cykliczna π jest postaci $(1)(2\ 5\ 6\ 10\ 4)(3\ 9\ 11\ 8\ 7)(12)$. Cykle (1) oraz (12) oznaczają, że karty 1 i 12 zawsze pozostają na swoim miejscu. Jako że pozostałe cykle mają długość 5, dokładnie ta liczba powtórnych przełożeń kart wystarczy, aby znalazły się one w swoim pierwotnym ułożeniu. (Zauważmy także, że $\pi^5 = id$.) ♯

Zadanie 3.93. Rozwiąż powyższy problem z kartami przy założeniu, że dostępnych jest 20 kart i rozważamy ułożenie postaci: 5 wierszy po 4 karty.

Typem permutacji π nazywamy wektor $(c_1, c_2, \ldots, c_n)$, gdzie c_i jest liczbą cykli długości i w rozkładzie π na cykle. Zazwyczaj typ permutacji zapisuje się jako $[1^{c_1} 2^{c_2} \ldots n^{c_n}]$, przy czym często pomija się te wartości, dla których $c_i = 0$.

Przykład 3.94. Permutacja $\pi = (1\ 3\ 7\ 6\ 2\ 4)(5)(8\ 9)$ ma jeden cykl długości 1, jeden cykl długości 2 oraz jeden cykl długości 6, a więc jest typu $[1^1 2^1 6^1]$. ♯

Transpozycja to permutacja typu $[1^{n-2}2^1]$. Innymi słowy, transpozycja dokonuje tylko jednego przestawienia dwóch elementów.

Przykład 3.95. Dla permutacji $\pi \in S_7$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 4 & 5 & 3 & 7 \end{pmatrix}$$

mamy $\pi = (1)(2)(3\ 6)(4)(5)(7) = (2\ 5)$, a więc π jest typu $[1^5 2^1]$, czyli π jest transpozycją. ♯

Twierdzenie 3.8 *Dowolny cykl z S_n jest złożeniem $n-1$ transpozycji.*

Ponieważ, na mocy twierdzenia 3.7, dowolna permutacja może być rozłożona na cykle, zatem z powyższego twierdzenia wynika, że każda permutacja jest złożeniem transpozycji. W szczególności, każda permutacja typu $[1^{c_1}2^{c_2}\dots n^{c_n}]$ ma rozkład na co najwyżej $c_2 + 2c_3 + \dots + (n-1)c_n$ transpozycji.

Przykład 3.96. Jak łatwo sprawdzić, permutacja cykliczna $\pi = (1\ 2\ 3) \in S_5$ jest złożeniem transpozycji $\tau_1 = (1\ 3)$ oraz $\tau_2 = (1\ 2)$.

x	1	2	3	4	5
τ_1	3	2	1	4	5
τ_2	2	1	3	4	5
x	1	2	3	4	5
$\tau_1 \circ \tau_2$	2	3	1	4	5

W ogólności zachodzi:

$$(x_1\ x_2\ x_3\ \dots\ x_{k-1}\ x_k) = (x_1\ x_k)(x_1\ x_{k-1})\dots(x_1\ x_3)(x_1\ x_2).$$

Permutacja jest *parzysta*, gdy jest złożeniem parzystej liczby transpozycji, w przeciwnym wypadku jest *nieparzysta*. *Znak* $\operatorname{sign}(\pi)$ permutacji π to

$$\operatorname{sign}(\pi) = (-1)^r,$$

gdzie r jest liczbą transpozycji, na które można rozłożyć π.

Przykład 3.97. Rozłóż podaną permutację $\pi \in S_9$ na cykle i transpozycje. Wyznacz typ tej permutacji. Czy permutacja π jest parzysta?

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 4 & 5 & 1 & 2 & 9 & 7 & 8 \end{pmatrix}.$$

Rozwiązanie. Rozłóżmy najpierw permutację π na cykle:

- cykl pierwszy: (1 3 4 5);
- cykl drugi: (2 6);

- cykl trzeci: (7 9 8).

A zatem $\pi = (1\ 3\ 4\ 5)(2\ 6)(7\ 9\ 8)$, a tym samym π jest typu $[2^1 3^1 4^1]$. Aby przedstawić teraz π jako złożenie transpozycji, najpierw rozkładamy każdy z cykli, zgodnie ze sposobem podanym wyżej:

- $(1\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)$.
- $(2\ 6)$ — bez zmian.
- $(7\ 9\ 8) = (7\ 8)(7\ 9)$.

A zatem otrzymujemy, że $\pi = (1\ 5)(1\ 4)(1\ 3)(2\ 6)(7\ 8)(7\ 9)$ i π jest permutacją parzystą. ♯

Zadanie 3.98. Permutacje $\pi_1, \pi_2 \in S_7$ zadane tabelami:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 6 & 5 & 7 & 1 & 2 \end{pmatrix} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 5 & 1 & 6 & 2 \end{pmatrix}$$

rozłóż na cykle i transpozycje. Wyznacz typy tych permutacji.

Zadanie 3.99. Rozłóż podaną permutację $\pi \in S_{14}$ na cykle i transpozycje. Wyznacz typ tej permutacji. Czy permutacja π jest nieparzysta?

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 14 & 2 & 7 & 3 & 4 & 1 & 10 & 8 & 13 & 9 & 11 & 12 & 5 & 6 \end{pmatrix}$$

Odpowiedzi do zadań

3.4.

a) 9^5.
b) $9 \cdot 10^4$.
c) $9 \cdot 10^3$.

3.5.

a) 3^n.
b) 3^{n-1}.
c) $3^{n-2} \cdot 3 \cdot 2 = 2 \cdot 3^{n-1}$.

3.6.

a) $9 \cdot 10^2$.
b) $1 \cdot 2^2$.
c) $2 \cdot 3^2$.

Z różnymi cyframi:

a) $9 \cdot 9 \cdot 8$.
b) brak.
c) $2 \cdot 2 \cdot 1$.

3.7. $2^3 \cdot 6^4$.

3.8. Grupa składała się z 3 osób.

3.12.

a) 15120.
b) 27216.
c) 2688.

3.13. $365^2 \cdot 364^2 \cdot 363^2 \cdot 362 \cdot 361$.

3.14. Grupa składa się z 3 osób.

3.17.

a) 120.
b) 48.

3.18.

a) 720.
b) 48.

3.19. $12! \cdot 8!$.

3.20.

a) 48.
b) 72.

3.21.

a) $2!$.
b) $3!$.
c) $(n-1)!$.

3.22.

a) $3!$.
b) $4!$.
c) $n!$.

3.23. 60.

3.25. 10.

3.26. 60.

3.27. Jeśli ustalimy koniec i początek, wówczas liczba sposobów wynosi $\frac{10!}{4!4!2!}$, jeśli natomiast rozważymy naszyjnik, wówczas otrzymamy $\frac{1}{10} \cdot \frac{1}{2} \cdot \frac{10!}{4!4!2!}$ sposobów.

3.29. 18.

3.30. $\frac{30!}{10!\cdot 8!\cdot 7!\cdot 5!}$ oraz $30!$.

3.31. $\binom{4}{2} \cdot \binom{48}{8}$.

3.32.

a) $4 \cdot \binom{6}{5}$.
b) $6 \cdot \binom{4}{2} \cdot 5 \cdot \binom{4}{3}$.
c) $\binom{6}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot \binom{16}{1}$.
d) $\binom{6}{2} \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot \binom{16}{1} + \binom{6}{1} \cdot \binom{20}{1}$.

3.33. $\frac{\binom{10}{2}\cdot\binom{8}{2}\cdot\binom{6}{2}\cdot\binom{4}{2}}{5!}$.

3.34. $\binom{52}{13}\cdot\binom{39}{13}\cdot\binom{26}{13}\cdot\binom{13}{13}$.

3.35. $[\binom{4}{1}\cdot\binom{4}{1}\cdot\binom{44}{11}]\cdot[\binom{3}{1}\cdot\binom{3}{1}\cdot\binom{33}{11}]\cdot[\binom{2}{1}\cdot\binom{2}{1}\cdot\binom{22}{11}]\cdot[\binom{1}{1}\cdot\binom{1}{1}\cdot\binom{11}{11}]$.

3.36. Klasa składa się z 25 osób.

3.37. 10.

3.38.

a) 14.
b) $\binom{n}{2}-n$.

3.39. $n(n-1)^2(n-2)$.

3.40.

a) $\binom{10}{4}$.
b) $\binom{n+k}{k}$.

3.41.

a) $\binom{10}{4}$.
b) $\binom{n+k-1}{k-1}$.

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

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

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

3.46. $\binom{29}{4}$.

3.47. $\binom{r-1}{n-1}$.

3.48. $\binom{r+n-1}{n-1}$.

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

3.52.

$$\begin{aligned}\binom{n-1}{a-1,b,c}+\binom{n-1}{a,b-1,c}+\binom{n-1}{a,b,c-1} &= \frac{(n-1)!}{(a-1)!\cdot b!\cdot c!}+\frac{(n-1)!}{a!\cdot(b-1)!\cdot c!}+\frac{(n-1)!}{a!\cdot b!\cdot(c-1)!}\\ &= \frac{a\cdot(n-1)!}{a\cdot(a-1)!\cdot b!\cdot c!}+\frac{b\cdot(n-1)!}{a!\cdot b\cdot(b-1)!\cdot c!}+\frac{c\cdot(n-1)!}{a!\cdot b!\cdot c(c-1)!}\\ &= \frac{(a+b+c)\cdot(n-1)!}{a!\cdot b!\cdot c!}=\frac{n\cdot(n-1)!}{a!\cdot b!\cdot c!}=\frac{n!}{a!\cdot b!\cdot c!}=\binom{n}{a,b,c}.\end{aligned}$$

3.64. $|A \cap B \cap C| \in \{0, 1\}$. $|C| = 4 - |A \cap B \cap C|$, stąd $|C| \in \{3, 4\}$.

3.65. W grupie jest 27 osób.

3.66. W grupie jest przynajmniej 21 osób, ale nie więcej niż 24.

3.67. Liczb mniejszych od 100 i niepodzielnych przez $2, 3, 5,$ ani 7 jest 22.

3.77.

$\emptyset$
$\{6\}$
$\{5\}$
$\{5, 6\}$
$\{4\}$
$\{4, 6\}$
$\{4, 5\}$
$\{4, 5, 6\}$
$\{3\}$
$\{3, 6\}$

3.78.

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

3.80.

$\{1, 2, 3\}$
$\{1, 2, 4\}$
$\{1, 3, 4\}$
$\{2, 3, 4\}$
$\{1, 2, 5\}$
$\{1, 3, 5\}$
$\{2, 3, 5\}$
$\{1, 4, 5\}$
$\{2, 4, 5\}$
$\{3, 4, 5\}$

3.81.

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

3.83.

$\{4,6,5,1,2,3\}$
$\{4,6,5,1,3,2\}$
$\{4,6,5,2,1,3\}$
$\{4,6,5,2,3,1\}$
$\{4,6,5,3,1,2\}$
$\{4,6,5,3,2,1\}$
$\{5,1,2,3,4,6\}$
$\{5,1,2,3,6,4\}$
$\{5,1,2,4,3,6\}$
$\{5,1,2,4,6,3\}$

3.84.

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

3.85.

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$$
$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\pi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$$
$$\pi_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

3.87.

a) $5!$.
b) $2 \cdot 5!$.

3.88. 190.

3.90.

$\pi_1 \circ \pi_2 = (1)(2\ 4\ 5\ 8\ 7)(3\ 6)$
$\pi_2 \circ \pi_1 = (1\ 6\ 4\ 7\ 8)(2\ 5)(3)$
$\pi_1^2 = (1\ 3\ 2)(6\ 5\ 4)(7)(8)$
$\pi_1^3 = (1)(2)(3)(4)(5)(6)(7\ 8)$
$\pi_2^2 = (1\ 5)(2)(3\ 7)(4)(6)(8)$
$\pi_2^3 = (1\ 7\ 5\ 3)(2\ 6)(4)(8)$
$\pi_1^{-1} = (1\ 3\ 2)(4\ 6\ 5)(8\ 7)$

3.93. 9.

3.98.

$\pi_1 = (1\ 3\ 6)(4\ 5\ 7\ 2)$, a tym samym π_1 jest typu $[3^1 4^1]$.
Rozkład na transpozycje: $\pi_1 = (1\ 6)(1\ 6)(4\ 2)(4\ 7)(4\ 5)$.

$\pi_2 = (1\ 4\ 5)(2\ 7)(3)(6)$, a tym samym π_1 jest typu $[1^2 2^1 3^1]$.
Rozkład na transpozycje: $\pi_1 = (1\ 5)(1\ 4)(2\ 7)$.

3.99.

$\pi = (1\ 14\ 6)(2)(3\ 7\ 10\ 9\ 13\ 5\ 4)(8)(11)(12)$, a tym samym π jest typu $[1^4 3^1 7^1]$.
$\pi = (1\ 6)(1\ 14)(3\ 4)(3\ 5)(3\ 13)(3\ 9)(3\ 10)(3\ 7)$, a zatem π jest parzysta.

Wskazówki dla Prowadzących

3.8. $8^x = 512$, zatem $x = 3$.

3.12.

a) $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = 15120$.
b) $9 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 27216$.
c) $8 \cdot 8 \cdot 7 \cdot 6 = 2688$.

3.13. $(365 \cdot 364 \cdot 363) \cdot (365 \cdot 364 \cdot 363 \cdot 362 \cdot 361) = 365^2 \cdot 364^2 \cdot 363^2 \cdot 362 \cdot 361$.

3.14. $5 \cdot 4 \cdot \ldots \cdot ((5 - x) + 1) = 60$, stąd $x = 3$.

3.17.

a) $5! = 120$.
b) $2 \cdot 4! = 48$.

3.18.

a) $6! = 720$.
b) $2 \cdot 4! = 48$.

3.20.

a) Traktując tomy I i II jako jeden (wtedy możliwe ustawienie I-II lub II-I) otrzymujemy $2 \cdot 4! = 48$.

b) Korzystając z (a): $5! - 2 \cdot 4! = 3 \cdot 4! = 72$.

   Nie korzystając: $2 \cdot 3 \cdot 3!$ (gdy jeden z tomów na pierwszej pozycji, drugi gdzieś na lewo) plus $2 \cdot 2 \cdot 3!$ (gdy jeden z tomów na drugiej pozycji, drugi gdzieś na lewo) plus $2 \cdot 3!$ (gdy jeden z tomów na trzeciej pozycji, a drugi dokładnie i tylko na piątej), co daje w sumie $3 \cdot 4! = 72$.

3.21. (a) Gdyby osoby stały w miejscu, mielibyśmy 3!. Jednakże karuzela kręci się, więc ich położenie względem otaczających je przedmiotów jest bez znaczenia, ważne jest jedynie ich położenie. Dlatego permutacje, które w trakcie krążenia przechodzą jedna w drugą, należy uznać za jednakowe. Jako że z każdej permutacji można za pomocą obrotu otrzymać jeszcze dwie nowe, pierwotną liczbę permutacji należy podzielić przez 3, stąd 2!. Analogicznie: (b) 3! i (c) $(n - 1)!$.

3.22. Mając na uwadze rozważania powyżej:

a) 3!.
b) 4!.
c) $n!$.

3.23. 4! (gdy 1 na pierwszej pozycji) plus $3 \cdot 3!$ (gdy 1 na drugiej pozycji) plus $2 \cdot 3!$ (gdy 1 na trzeciej pozycji) plus 3! (gdy 1 na czwartej pozycji), co daje w sumie $(4+3+2+1) \cdot 3! = 10 \cdot 3! = 60$.

3.25. $\frac{5!}{3!2!} = 10$.

3.26. $2 \cdot \frac{5!}{2!2!} = 60$.

3.27. Jeśli ustalimy koniec i początek, wówczas liczba sposobów wynosi $\frac{10!}{4!4!2!}$, jeśli natomiast rozważymy naszyjnik, wówczas należy uwzględnić równoważność tych permutacji, które w trakcie krążenia przechodzą jedna w drugą, oraz tych, które powstają przez lustrzane odbicie naszyjnika, tym samym otrzymujemy: $\frac{1}{10} \cdot \frac{1}{2} \cdot \frac{10!}{4!4!2!}$.

3.29. $\binom{3}{2} \cdot \binom{4}{2} = 18$.

3.30. W przypadku nieistotności kolejności:

$$\binom{30}{10} \cdot \binom{20}{8} \cdot \binom{12}{7} \cdot \binom{5}{5} = \frac{30!}{10! \cdot 20!} \cdot \frac{20!}{8! \cdot 12!} \cdot \frac{12!}{7! \cdot 5!} \cdot \frac{5!}{5! \cdot 0!} = \frac{30!}{10! \cdot 8! \cdot 7! \cdot 5!}.$$

Biorąc pod uwagę kolejność ustawienia:

$$\binom{30}{10} \cdot 10! \cdot \binom{20}{8} \cdot 8! \cdot \binom{12}{7} \cdot 7! \cdot \binom{5}{5} \cdot 5! = 30!.$$

3.36. $\binom{x}{2} = 300$, stąd $x(x-1) = 600$, zatem $x = 25$.

3.37. $\binom{5}{2} = 10$.

3.38.

a) $\binom{7}{2} - 7 = 14$.

b) $\binom{n}{2} - n$.

3.40.

a) Każda najkrótsza droga z A do B musi zawierać 10 odcinków, z których dowolne cztery muszą być „do góry", a pozostałe muszą być „w prawo". Stąd liczba najkrótszych dróg jest równa liczbie sposobów wskazania, które cztery spośród dziesięciu odcinków muszą być „do góry". Mamy $\binom{10}{4}$ takich wyborów.

b) Uogólnienie: $\binom{n+k}{k}$.

3.41.

a) Rozważmy kratę 6×4. Jeśli potraktujemy liczbę przebytych odcinków w rzędzie $i-1$ jako x_i, wówczas każda z najkrótszych dróg stanowi pewne rozwiązanie równania $x_1 + x_2 + x_3 + x_4 + x_5 = 6$. Istnieje więc wzajemnie jednoznaczna zależność między drogami i rozwiązaniami i stąd wynika, że liczba tych rozwiązań wynosi $\binom{10}{4}$.

b) Uogólnienie: $\binom{n+k-1}{k-1}$.

3.42. Każdy taki wybór można utożsamić z pewnym rozwiązaniem równania $x_1 + \cdots + x_k = n$, gdzie x_i jest nieujemne i określa liczbę przedmiotów typu i. Zatem liczba rozwiązań równania wynosi $\binom{n+k-1}{k-1}$.

3.43. Każdy taki wybór równoważny jest wstawieniu $k-1$ barierek w $n-1$ możliwe miejsca pomiędzy osobami w kolejce, zatem rozwiązanie: $\binom{n-1}{k-1}$.

3.44. Zauważmy, że rozbicie n na dodatnie x_i równoważne jest rozdzieleniu kolejki na grupy w zadaniu powyżej, zatem rozwiązanie: $\binom{n-1}{k-1}$.

3.45. Zauważmy, że równanie $x_1+\cdots+x_k = n$, gdzie x_i jest nieujemne, równoważne jest równaniu $(x_1+1)+\cdots+(x_k+1) = n+k$, gdzie x_i+1 jest nieujemne, czyli równaniu $y_1+\cdots+y_k = n+k$, gdzie y_i jest dodatnie. Z poprzedniego zadania: $\binom{n+k-1}{k-1}$.

3.46. Niech $x_i > 0$, $i = 1, \ldots, 5$, będzie liczbą piłek w pudle i. Wówczas zachodzi $x_1 + x_2 + x_3 + x_4 + x_5 = 30$. Z porzedniego zadania otrzymujemy zatem, że liczba rozmieszczeń takich, że żadne pudło nie jest puste, wynosi $\binom{29}{4}$.

3.47. Rozumowanie analogiczne do powyższego prowadzi do: $\binom{r-1}{n-1}$.

3.48. Niech $x_i \geq 0$, $i = 1, \ldots, r$, będzie liczbą piłek w pudle i. Wówczas zachodzi $x_1 + \ldots x_n = r$. Z zadania 42(b) otrzymujemy zatem, że liczba wszystkich rozmieszczeń wynosi $\binom{r+n-1}{n-1}$.

3.49. Problem równoważny jest wybraniu spośród $n-k+1$ miejsc pomiędzy wolnymi $n-k$ krzesłami (rozłącznych) miejsc do wstawienia k krzeseł. Tym samym szukana liczba to $\binom{n-k+1}{k}$.

3.50. Dowód oprzemy na indukcji względem n.

(0) Koło bez żadnej linii ma jeden obszar.

(n) Załóżmy, że liczba obszarów utworzonych przez n prostych wynosi co najwyżej

$$1 + n + \binom{n}{2}.$$

($n+1$) Załóżmy, że mamy $n+1$ prostych i rozważmy $(n+1)$-szą prostą l. Usuńmy ją. Z założenia indukcyjnego liczba obszarów utworzonych przez n prostych wynosi co najwyżej $1 + n + \binom{n}{2}$. Dodajmy z powrotem prostą l (w ten sam sposób).

Jeśli l nie przecina żadnej z istniejących linii, to liczba obszarów zwiększa się o jeden. Dodatkowo, za każdym razem, kiedy linia l przecina jedną z n linii wewnątrz koła, liczba obszarów ponownie powiększa się o 1. Tym samym otrzymujemy, że liczba obszarów wynosi co najwyżej

$$\begin{aligned} 1 + n + \tbinom{n}{2} + 1 + n &= 1 + (n+1) + \tfrac{n(n-1)}{2} + n = 1 + (n+1) + \tfrac{n(n-1)+2n}{2} \\ &= 1 + (n+1) + \tfrac{n(n+1)}{2} + n = 1 + (n+1) + \tbinom{n+1}{2}, \end{aligned}$$

co należało wykazać.

3.52.

$$\begin{aligned}\binom{n-1}{a-1,b,c}+\binom{n-1}{a,b-1,c}+\binom{n-1}{a,b,c-1} &= \frac{(n-1)!}{(a-1)!\cdot b!\cdot c!}+\frac{(n-1)!}{a!\cdot(b-1)!\cdot c!}+\frac{(n-1)!}{a!\cdot b!\cdot(c-1)!}\\ &= \frac{a\cdot(n-1)!}{a\cdot(a-1)!\cdot b!\cdot c!}+\frac{b\cdot(n-1)!}{a!\cdot b\cdot(b-1)!\cdot c!}+\frac{c\cdot(n-1)!}{a!\cdot b!\cdot c(c-1)!}\\ &= \frac{(a+b+c)\cdot(n-1)!}{a!\cdot b!\cdot c!}=\frac{n\cdot(n-1)!}{a!\cdot b!\cdot c!}=\frac{n!}{a!\cdot b!\cdot c!}=\binom{n}{a,b,c}.\end{aligned}$$

3.54. Mając na uwadze, że $\binom{n}{0}\binom{n}{n}=1$ oraz równość $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$, lewa strona rozważanego równania przyjmuje postać

$$1-\left[\binom{n-1}{0}+\binom{n-1}{1}\right]+\left[\binom{n-1}{2}+\binom{n-1}{2}\right]-\ldots+(-1)^{n-1}\left[\binom{n-1}{n-2}+\binom{n-1}{n-1}\right]+(-1)^n=0.$$

Zauważmy, że każdy z czynników $\binom{n-1}{k}$, $1\le k\le n-2$, występuje zarówno ze znakiem '+', jak i '−', a zatem współczynniki te sumują się nawzajem do 0. Pozostaje $1-\binom{n-1}{0}+(-1)^{n-1}\binom{n-1}{n-1}+(-1)^n=1-1+(-1)^{n-1}+(-1)^n$, co oczywiście sumuje się do 0.

3.60. Na podstawie zasady włączania-wyłączania otrzymujemy, że $|C|+|A\cap B\cap C|=4$. Zauważmy, że $|A\cap B\cap C|$ może byc równe 0 lub 1. Mamy wtedy, że $|C|$ jest równe 3 lub 4.

3.62. Niech F oznacza zbiór osób znających francuski, $N\cap D$ zbiór osób znających niemiecki i duński, *etc.* Mamy wtedy, że $|D\cup F\cup N\cup T|=19+|D\cap N\cap T|$. Ale $2\le|D\cap N\cap T|\le 5$ (co wynika z liczności $|D\cap N|$ i $|D\cap F\cap N\cap T|$. Stąd $|D\cup F\cup N\cup T|\in\{21,...,24\}$.

3.63. Niech D oznacza zbiór liczb podzielnych przez 2, T przez 3 i P przez pięć, $D\cap P$ zbiór liczb podzielnych przez 2 i 5, itd. Z zasady włączania-wyłączania otrzymujemy, że liczb mniejszych od 100 i niepodzielnych przez $2,3,5$, ani 7 jest $99-|D\cup T\cup P\cup S|=99-(49+33+19+14-16-9-7-6-4-2+3+2+1-0)=22$.

3.72. Wszystkich podzbiorów zbioru 10-elementowego jest $2^{10}=1024$. Maksymalna możliwa suma liczb z zadanego podzbioru to $98+99+...+107=1015$. Na podstawie zasady szufladkowej łatwo jest wykazać żądaną własność — należy pamiętać, aby zbiory były rozłączne, a zatem jeśli nie są — usuwamy część wspólną.

3.88. $\binom{6}{2}\cdot\binom{4}{2}\cdot\binom{2}{2}+\binom{6}{2}\cdot\binom{4}{2}+\binom{6}{2}=190$.

3.93. Wyznaczona permutacja kolejnych zmian pozycji kart ma postać

$$(1)(2\ 6\ 7\ 12\ 18\ 10\ 8\ 17\ 5)(3\ 11\ 13\ 4\ 16\ 19\ 15\ 14\ 9)(20),$$

a zatem, jako że mamy dwa cykle długości 9, potrzebujemy 9 przełożeń.

Zestaw zadań nr 4

Prawdopodobieństwo

Przykład 4.1. Czterem graczom rozdano 52 karty. Niech I_k, $k = 1, 2, 3, 4$, będzie zdarzeniem polegającym na tym, że pierwszy gracz otrzymał co najmniej k asów. Przez II_k, III_k, IV_k oznaczono analogicznie zdarzenia dla drugiego, trzeciego i czwartego gracza. Co można powiedzieć o liczbie asów u czwartego gracza, wiedząc, że zaszło zdarzenie:

a) $\overline{IV_1}$,
b) $I_2 \cap II_2$,
c) $\overline{I_1} \cap \overline{II_1} \cap \overline{III_1}$,
d) $IV_2 - IV_3$,
e) $I_1 \cap II_1 \cap III_1 \cap IV_1$,
f) $I_3 \cap IV_1$,
g) $(I_2 \cup II_2) \cap III_2$?

Rozwiązanie.

a) Zdarzenie IV_1 polega na otrzymaniu co najmniej jednego asa przez czwartego gracza. Zdarzenie $\overline{IV_1}$ jest zdarzeniem przeciwnym temu zdarzeniu, a zatem polega na nieotrzymaniu przez niego żadnego asa.

b) Zdarzenie $I_2 \cap II_2$ polega na otrzymaniu co najmniej dwóch asów przez pierwszego gracza i na otrzymaniu co najmniej dwóch asów przez drugiego gracza. Ponieważ są tylko cztery asy, więc powyższe zdarzenie polega na otrzymaniu dokładnie dwóch asów przez pierwszego gracza i dokładnie dwóch asów przez drugiego gracza. Oczywiście w takim przypadku pozostali gracze nie mogli dostać żadnego asa.

c) W zdarzeniu $\overline{I_1} \cap \overline{II_1} \cap \overline{III_1}$ zarówno pierwszy, drugi i trzeci gracz nie otrzymali żadnego z asów, stąd wynika, że gracz czwarty otrzymał dokładnie cztery asy.

d) Zdarzenie IV_2 oznacza, że czwarty gracz posiada dwa, trzy lub cztery asy. Analogicznie, zdarzenie IV_3 oznacza, że czwarty gracz posiada trzy lub cztery asy. Stąd wynika, że zdarzenie $IV_2 - III_3$ polega na otrzymaniu przez czwartego gracza dokładnie dwóch asów.

e) Zdarzenie $I_1 \cap II_1 \cap III_1 \cap IV_1$ polega na otrzymaniu przez każdego z graczy dokładnie po jednym asie.

f) Zdarzenie $I_3 \cap IV_1$ polega na otrzymaniu przez pierwszego gracza trzech asów i przez czwartego gracza jednego asa.

g) Zdarzenie $(I_2 \cup II_2) \cap III_2$ polega na otrzymaniu przez pierwszego albo drugiego gracza co najmniej dwóch asów i na otrzymaniu przez trzeciego gracza co najmniej dwóch asów. Stąd wynika, że albo pierwszy albo drugi gracz ma otrzymać dokładnie dwa asy i także trzeci gracz ma otrzymać dwa asy, a zatem czwarty gracz będzie pozbawiony asa. ♯

Zadanie 4.2. Weźmy pod uwagę dwie wielkości: X – wzrost męża, Y – żony. Każdej parze małżeńskiej można przypisać punkt na płaszczyźnie o współrzędnych (x, y), gdzie $x > 0$ i $y > 0$ (I. ćwiartka układu współrzędnych). Niech zdarzenie A polega na tym, że mąż ma wzrost większy niż $1,8$m; zdarzenie B – mąż wyższy od żony; zdarzenie C – żona ma wzrost większy niż $1,8$m.

a) Zilustrować to zdarzenie geometrycznie.
b) Wyjaśnić, na czym polegają zdarzenia $A \cap B \cap C$, $A \setminus (A \cap B)$, $A \cap \overline{B} \cap C$.
c) Wyjaśnić, dlaczego $A \cap \overline{C} \subset B$.

Zadanie 4.3. Rzucamy dwiema kostkami do gry. Niech zdarzenie A polega na tym, że suma oczek jest liczbą nieparzystą, zdarzenie B – na otrzymaniu jedynki co najmniej na jednej kostce. Opisać zdarzenia $A \cap B$, $A \cup B$, $A \cap \overline{B}$ oraz obliczyć ich prawdopodobieństwa zakładając, że zdarzenia elementarne w liczbie 36 są jednakowo możliwe.

Przykład 4.4. Dokonujemy trzech rzutów monetą. Jakie jest prawdopodobieństwo zajścia zdarzenia A polegającego na tym, że orzeł pojawi się dwa razy? Jakie jest prawdopodobieństwo zajścia zdarzenia B polegającego na tym, że orzeł pojawi się co najmniej dwa razy? Jakie jest prawdopodobieństwo zajścia zdarzenia C polegającego na tym, że orzeł pojawi się co najwyżej dwa razy?

Rozwiązanie. Zbiór zdarzeń elementarnych jest następujący:

$$\{\mathrm{OOO}, \mathrm{OOR}, \mathrm{ORO}, \mathrm{ROO}, \mathrm{RRR}, \mathrm{ORR}, \mathrm{ROR}, \mathrm{RRO}\}.$$

Mając na uwadze liczbę zdarzeń elementarnych sprzyjającą każdemu ze zdarzeń, otrzymujemy $P(A) = \frac{3}{8}$, $P(B) = \frac{1}{2}$ i $P(C) = \frac{7}{8}$. ♯

Zadanie 4.5. Wybieramy jedną z cyfr $1, 2, 3, 4, 5$, a następnie z pozostałych – drugą. Obliczyć prawdopodobieństwo tego, że za pierwszym (drugim, obydwa razy) będzie wybrana nieparzysta liczba.

Zadanie 4.6. Fabryka produkuje towar sztukowy: 3 razy tyle białego co czarnego, a 5 razy tyle białego co niebieskiego. Jakie jest prawdopodobieństwo p tego, że biorąc sztukę losowo, otrzyma się sztukę czarną?

Zadanie 4.7. W urnie są kule o numerach $1, 2, 3, 4, 5$. Wybieramy losowo dwie kule bez zwracania. Obliczyć prawdopodobieństwo p tego, że otrzymamy kule o kolejnych rosnących numerach.

Zadanie 4.8. Cyfry $1, 2, 3, 4, 5$ są napisane na pięciu kartkach tak, że każdej cyfrze odpowiada jedna kartka. Pobieramy losowo jednocześnie trzy kartki. Jakie jest prawdopodobieństwo p tego, że suma otrzymanych liczb jest liczbą parzystą?

Zadanie 4.9. Z elementów a_1, a_2, a_3 utworzono wszystkie możliwe permutacje. Obliczyć prawdopodobieństwo tego, że w wybranej losowo permutacji:

a) są nie mniej niż dwie inwersje;
b) element a_2 tworzy jedną inwersję.

Twierdzenie 4.9 *Prawdopodobieństwo zdarzenia A polegającego na zajściu przynajmniej jednego ze zdarzeń A_1 lub A_2 równa się sumie prawdopodobieństw tych zdarzeń zmniejszonej o prawdopodobieństwo łącznego ich zajścia, tzn.*

$$P(A) = P(A_1) + P(A_2) - P(A_1 \cap A_2).$$

Przykład 4.10. Obliczyć prawdopodobieństwo tego, że losując z talii 52 kart jedną kartę, otrzymamy pika lub asa.

Rozwiązanie. Oznaczmy przez A_1 zdarzenie polegające na otrzymaniu pika, A_2 zdarzenie polegające na otrzymaniu asa, A zdarzenie polegające na zajściu przynajmniej jednego z wyżej wymienionych zdarzeń. Zauważmy, że zdarzenie $A_1 \cap A_2$ polega na otrzymaniu asa pik. Tym samym ze wzoru otrzymujemy

$$P(A) = P(A_1) + P(A_2) - P(A_1 \cap A_2) = \frac{13}{52} + \frac{4}{52} - \frac{1}{52} = \frac{4}{13}. \qquad \sharp$$

Zadanie 4.11. Dwaj myśliwi jednocześnie ujrzeli zająca i jednocześnie strzelili do niego. Zakładamy, że dla każdego z myśliwych prawdopodobieństwo zabicia jednym strzałem zająca wynosi $\frac{1}{3}$. Jakie jest prawdopodobieństwo tego, że zając zostanie zastrzelony?

Zadanie 4.12. Z urny, w której znajduje się 20 kul białych i 2 kule czarne, wyjmuje się kolejno n kul, przy czym każdą wyciągniętą kulę kładzie się z powrotem do urny. Znaleźć najmniejszą wartość n taką, przy której prawdopodobieństwo wylosowania chociaż raz czarnej kuli jest większe od $\frac{1}{2}$.

Zadanie 4.13. Dane są $P(\overline{A}) = \frac{1}{3}$, $P(A \cap B) = \frac{1}{4}$ i $P(A \cup B) = \frac{2}{3}$. Oblicz $P(\overline{B})$, $P(A \cap \overline{B})$, $P(B \setminus A)$.

Zadanie 4.14. Dane są $P(A \cap B) = \frac{1}{4}$, $P(A \cup B) = \frac{1}{2}$ i wiadomo, że $P(A \setminus B) = P(B \setminus A)$. Oblicz $P(B)$ i $P(B \setminus A)$.

4.1 Prawdopodobieństwo warunkowe

Definicja 4.1 Prawdopodobieństwem warunkowym $P(A|B)$ *zdarzenia A przy założeniu, że zaszło zdarzenie B nazywamy iloraz prawdopodobieństwa łącznego zajścia zdarzeń A i B do prawdopodobieństwa zajścia zdarzenia B:*

$$P(A|B) = \frac{P(A \cap B)}{P(B)}, \ \textit{gdzie}\, P(B) > 0.$$

Definicja 4.2 *Mówimy, że zdarzenie A jest* niezależne *od zdarzenia B, jeśli zachodzi jeden z dwóch przypadków: $P(A|B) = P(A)$ i $P(B) > 0$ albo $P(B) = 0$.*

Twierdzenie 4.10
Na to, aby zdarzenia A i B były niezależne, potrzeba i wystarcza, aby $P(A \cap B) = P(A) \cdot P(B)$.

Przykład 4.15. Rzucamy trzema kostkami. Jakie jest prawdopodobieństwo, że na żadnej kostce nie wypadnie 6, jeżeli na każdej kostce wypada inna liczba oczek?

Rozwiązanie. Oznaczmy przez A zdarzenie polegające na niewypadnięciu szóstki na żadnej z kostek, a przez B zdarzenie polegające na wypadnięciu na każdej z kostek innej liczby oczek. Wówczas, z klasycznej definicji prawdopodobieństwa oraz mając na uwadze wzór $P(A|B) = \frac{P(A \cap B)}{P(B)}$, otrzymujemy, że

$$P(A|B) = \frac{\frac{5 \cdot 4 \cdot 3}{6^3}}{\frac{6 \cdot 5 \cdot 4}{6^3}} = \frac{\binom{5}{3}}{\binom{6}{3}} = \frac{1}{2}.$$

♯

Zadanie 4.16. Rzucamy dwiema kostkami do gry. Obliczyć prawdopodobieństwo:

a) zdarzenia A polegającego na otrzymaniu sumy oczek nie większej od czterech;

b) zdarzenia B polegającego na otrzymaniu dwóch oczek co najmniej na jednej kostce;

c) zdarzenia $A \cap B$ polegającego na tym, że co najmniej na jednej z kostek otrzymamy dwa oczka i że suma oczek nie będzie większa od czterech;

d) zdarzenia polegającego na tym, że suma oczek nie będzie większa od czterech, jeśli wiadomo, że co najmniej na jednej kostce otrzymano dwa oczka.

Zadanie 4.17. W pudełku są długopisy: 10 czerwono-niebieskich, 2 niebieskie, 7 zielonych, i zielono-czerwony. Losujemy jeden długopis.

a) Jakie jest prawdopodobieństwo zdarzenia A_c polegającego na tym, że otrzymanym długopisem można pisać w kolorze czerwonym?

b) Jakie jest prawdopodobieństwo zdarzenia A_c polegającego na tym, że otrzymanym długopisem można pisać w kolorze czerwonym, jeśli wiadomo, że długopis ten pisze:

   1) na niebiesko (zdarzenie A_n),
   2) na zielono (zdarzenie A_z)?

Zadanie 4.18. W urnie znajdują się 3 kule białe i 4 kule czarne. Jakie jest prawdopodobieństwo zajścia zdarzenia B polegającego na otrzymaniu dwóch kul białych przy założeniu, że losujemy z urny dwa razy i po pierwszym losowaniu kula nie zostaje zwrócona do urny?

Zadanie 4.19. Udowodnij, że jeśli zdarzenia A i B są niezależne, to niezależne są także zdarzenia A i $\overline{B}$ oraz $\overline{A}$ i $\overline{B}$.

Przykład 4.20. Rzucamy dwiema kostkami do gry. Niech A_1 oznacza zdarzenie polegające na wyrzuceniu nieparzystej liczby oczek na pierwszej kostce, A_2 – parzystej liczby oczek na drugiej kostce, A_3 – nieparzystej bądź parzystej liczby oczek na obu kostkach. Zbadać niezależność zdarzeń A_1, A_2 i A_3.

Rozwiązanie. Analizując możliwe zdarzenia elementarne otrzymamy, że

$$P(A_1) = P(A_2) = P(A_3) = \frac{1}{2}.$$

Ponadto $P(A_1 \cap A_2) = P(A_1 \cap A_3) = P(A_2 \cap A_3) = \frac{1}{4}$, a zatem zdarzenia A_1, A_2, A_3 są niezależne parami. W szczególności $P(A_2 \cap A_3) = P(A_2)P(A_3)$. Zauważmy, że $P(A_1|(A_2 \cap A_3)) = 0$, gdyż jeśli zaszło zdarzenie $A_2 \cap A_3$, tzn. wyrzuciliśmy na obu kostkach parzystą liczbę oczek, to niemożliwe jest otrzymanie zdarzenia A_1, tj. wyrzucenia nieparzystej liczby oczek na jednej z kości. Zatem $P(A_1) \cdot P(A_2) \cdot P(A_3) \neq P(A_1 \cap A_2 \cap A_3)$ i zdarzenia nie są niezależne zespołowo. ♯

Zadanie 4.21. Niech przestrzeń zdarzeń elementarnych będzie zbiorem 3-elementowych ciągów zero-jedynkowych. Rozważmy zdarzenia:

a) na 1. współrzędnej stoi 0;
b) na 1. i 3. współrzędnej stoi 0;
c) na 1. i 3. współrzędnej mamy różne wartości;
d) na wszystkich współrzędnych to samo.

Jakie jest klasyczne prawdopodobieństwo tych zdarzeń? Czy zdarzenia te są parami niezależne? Rozważyć przestrzeń dla ciągów n-elementowych.

Twierdzenie 4.11 *Jeśli zdarzenia $A_1, \cdots, A_n$ tworzą układ zupełny zdarzeń, to prawdopodobieństwo dowolnego zdarzenia B wyliczamy ze wzoru*

$$P(B) = P(A_1) \cdot P(B|A_1) + \ldots + P(A_n) \cdot P(B|A_n).$$

Przykład 4.22. W urnie są 4 kule białe i 3 czarne. Losujemy dwie kule. Jakie jest prawdopodobieństwo wylosowania kul w różnych kolorach?

Rozwiązanie. Niech B oznacza zdarzenie polegające na wylosowaniu za pierwszym razem kuli białej, a C – wylosowaniu kuli czarnej. Niech R oznacza wylosowanie za drugim razem kuli różnej od tej za pierwszym razem. Wówczas z twierdzenia o prawdopodobieństwie zupełnym (całkowitym) otrzymujemy

$$P(R) = P(B) \cdot P(R|B) + P(C) \cdot P(R|C) = \frac{4}{7} \cdot \frac{1}{2} + \frac{3}{7} \cdot \frac{2}{3} = \frac{4}{7}.$$ ♯

Zadanie 4.23. W każdej z 5 urn pierwszej serii znajdują się 4 kule białe i 6 kule czarnych, w każdej z 8 urn drugiej serii znajduje się 9 kul białych i 6 kul czarnych. Sięgamy losowo do jednej z urn i i wyciągamy jedną kulę. Jakie jest prawdopodobieństwo, że wylosowana kula będzie biała?

Zadanie 4.24. Losujemy jedną kulę z jednej z 4 urn typu A i 16 urn typu B. W każdej z urn typu A znajduje się 7 kul białych i 3 kule czarne, natomiast w każdej z urn typu B znajdują się 4 kule białe i 6 kul czarnych. Jakie jest prawdopodobieństwo zajścia zdarzenia C polegającego na wylosowaniu kuli białej?

Zadanie 4.25. Mamy dwie urny z kulami: w I. urnie są 2 kule białe i 4 czarne, w II. urnie są 3 kule białe i 3 czarne. Rzucamy kostką do gry. Jeśli wypadnie 1 lub 2, to losujemy kulę z I.

urny, jeśli wypadnie 3, 4, 5, 6, to losujemy kulę z II. urny. Jakie jest prawdopodobieństwo, że wylosujemy kulę białą?

Zadanie 4.26. Z urny, w której jest b kul białych i c kul czarnych, wyjęto losowo jedną kulę. Jakie jest teraz prawdopodobieństwo wylosowania kuli białej, jeśli nie znamy koloru kuli poprzednio wylosowanej?

Zadanie 4.27. Z urny, w której jest b kul białych i c kul czarnych, wyjęto losowo jedną kulę i nie oglądając jej, wrzucono do drugiej urny, w której było b_1 kul białych i c_1 kul czarnych. Jakie jest teraz prawdopodobieństwo wylosowania kuli białej z drugiej urny?

Zadanie 4.28. W urnie jest n kul, w tym $k \leq n$ białych. n osób losuje kulę po kolei bez zwracania. Jakie jest prawdopodobieństwo wylosowania kuli białej dla: (a) 2-giej osoby, (b) 3-ciej osoby?

Zadanie 4.29.* Przeprowadzamy serię kolejnych doświadczeń tak, że w wyniku każdego z nich może zajść zdarzenie A albo zdarzenie przeciwne $\overline{A}$. Oznaczmy zajście zdarzenia A w n-tym doświadczeniu przez A_n i zdarzenia doń przeciwnego przez $\overline{A_n}$, oraz odpowiednio przez p_n prawdopodobieństwo zajścia zdarzenia A_n i q_n – odpowiednie prawdopodobieństwo zajścia zdarzenia przeciwnego, tzn. $p_n = P(A_n)$, $q_n = P(\overline{A_n}) = 1 - p_n$. Niech teraz w przypadku zajścia zdarzenia A w n-tym doświadczeniu prawdopodobieństwo zajścia zdarzenia A w $(n+1)$-doświadczeniu równa się a. W przypadku zaś, gdy nie zajdzie zdarzenie A w n-tym doświadczeniu, prawdopodobieństwo jego zajścia w $(n+1)$-szym doświadczeniu niech równa się b, tzn. $P(A_{n+1}|A_n) = a$, $P(A_{n+1}|\overline{A_n})$=b. W tak postawionym zagadnieniu należy obliczyć prawdopodobieństwo zajścia zdarzenia A w $(n+1)$-szym doświadczeniu znając prawdopodobieństwa p_1, a, b.

Zadanie 4.30.* Niech prawdopodobieństwo, że po wyjeździe z domu napotkamy na pierwszym skrzyżowaniu zielony sygnał świetlny, będzie równe $\frac{1}{2}$. Sygnalizacja jest tak ustawiona, że w przypadku zatrzymania się na dowolnym skrzyżowaniu przy świetle czerwonym prawdopodobieństwo tego, że na następnym skrzyżowaniu zastaniemy światło zielone jest równe $\frac{95}{100}$, natomiast prawdopodobieństwo tego, że jeśli na dowolnym skrzyżowaniu będziemy mieli światło zielone, to i na następnym będziemy mieli światło zielone, jest równe $\frac{1}{10}$.

a) Obliczyć prawdopodobieństwo, że po wyjeździe z garażu na trzecim skrzyżowaniu będziemy mieli światło zielone.

b) Obliczyć prawdopodobieństwo graniczne, tj. $\lim_{n\to\infty} p_{n+1}$, gdzie p_k oznacza prawdopodobieństwo, że po wyjeździe z garażu na k-tym skrzyżowaniu będziemy mieli światło zielone.

4.2 Schemat Bernoulliego

Twierdzenie 4.12 *Prawdopodobieństwo tego, że na n przeprowadzonych doświadczeń według schematu Bernoulliego uzyska się k sukcesów w dowolnej kolejności, wyraża się wzorem*

$$P_{n,k} = \binom{n}{k} \cdot p^k \cdot q^{n-k},$$

gdzie $0 < p \leq 1$ i $q = 1 - p$.

Przykład 4.31. W urnie mamy N kul, wśród których M jest białych, pozostałe są czarne. Losujemy n razy po jednej kuli, zwracając ją za każdym razem. Obliczyć prawdopodobieństwo wylosowania k kul białych.

Rozwiązanie. Zwrot kuli za każdym razem zapewnia stały skład urny przy każdym losowaniu, a co za tym idzie, spełnienie warunku niezależności doświadczeń i jednakowego prawdopodobieństwa wylosowania kuli białej w każdym doświadczeniu równego $\frac{M}{N}$. Szukane prawdopodobieństwo w myśl twierdzenia Bernoulliego jest więc następujące

$$P_{n,k} = \binom{n}{k} \cdot (\frac{M}{N})^k \cdot (1 - \frac{M}{N})^{n-k} = \binom{n}{k} \cdot \frac{M^k \cdot (N-M)^{n-k}}{N^n}.$$

♯

Zadanie 4.32. Pewna gra polega na rzucie kostką i monetą. Wygrana następuje przy łącznym otrzymaniu piątki i orła. Jakie jest prawdopodobieństwo tego, że w trzech grach wygrana nastąpi dokładnie raz?

Zadanie 4.33. Co jest bardziej prawdopodobne u równego siłą gry przeciwnika: (1) wygranie 3 partii z 4 czy 5 z 8? (2) wygranie nie mniej niż 3 partii z 4, czy nie mniej niż 5 partii z 8?

Zadanie 4.34. Obliczyć prawdopodobieństwo tego, że na 7 rzutów kostką co najwyżej 3 razy wypadnie liczba oczek nie mniejsza niż 4.

Zadanie 4.35. Dana jest urna, w której są kule: 6 czarnych i 9 białych. Losujemy 5 razy po jednej kuli, kładąc za każdym razem wyciągniętą kulę z powrotem do urny. Jakie jest prawdopodobieństwo tego, że otrzymamy co najwyżej 3 razy kulę białą?

Odpowiedzi do zadań

4.3. $P(A \cap B) = \frac{1}{6}$, $P(A \cup B) = \frac{23}{36}$, $P(A \cap \overline{B}) = \frac{1}{3}$.

4.5. Wprowadźmy następujące oznaczenia:

A – zdarzenie polegające na wyrzuceniu nieparzystej liczba oczek za pierwszym razem;
B – zdarzenie polegające na wyrzuceniu nieparzystej liczba oczek za drugim razem;
C – przekrój zdarzeń A i B.

Wówczas zachodzi $P(A) = \frac{3}{5}$, $P(B) = \frac{3}{5}$ i $P(C) = P(A \cap B) = \frac{3}{10}$.

4.6. $\frac{5}{23}$.

4.7. $\frac{1}{5}$.

4.8. $\frac{3}{5}$.

4.9.
a) $\frac{1}{2}$.
b) $\frac{1}{3}$.

4.11. $\frac{5}{9}$.

4.12. 8.

4.13. $P(\overline{B}) = \frac{3}{4}$, $P(A \cap \overline{B}) = \frac{5}{12}$, $P(B \setminus A) = 0$.

4.14. $P(B) = \frac{3}{8}$, $P(B \setminus A) = \frac{1}{8}$.

4.16.

a) $P(A) = \frac{1}{6}$.
b) $P(B) = \frac{11}{36}$.
c) $P(A \cap B) = \frac{1}{12}$.
d) $P(A|B) = \frac{3}{11}$.

4.17. $P(A_c) = \frac{11}{20}$, $P(A_c|A_n) = \frac{10}{12}$, $P(A_c|A_z) = \frac{1}{8}$.

4.18. $\frac{1}{7}$.

4.21.

a) $P(A) = \frac{1}{2}$.
b) $P(B) = \frac{1}{4}$.
c) $P(C) = \frac{1}{2}$.
d) $P(D) = \frac{1}{8}$.
Ogólnie: $P(D) = \frac{1}{2^{n-1}}$.
Zdarzenia te nie są parami niezależne.

4.23. $\frac{34}{65}$.

4.24. $\frac{23}{50}$.

4.25. $\frac{4}{9}$.

4.26. $\frac{b}{b+c}$.

4.27. $\frac{b}{b+c} \cdot \frac{b_1+1}{b_1+c_1+1} + \frac{c}{b+c} \cdot \frac{b_1}{b_1+c_1+1}$.

4.28. $\frac{k}{n}$. (Patrz Zadanie 26.)

4.29. $\frac{b}{1-a+b}$.

4.30. Korzystając ze wzoru otrzymanego w Zadaniu 4.29 otrzymujemy:

a) $p_3 = \frac{0{,}95(1-(1-0{,}1+0{,}95)^3)}{1-0{,}1+0{,}95} + (0,5 - \frac{0{,}95}{1-0{,}1+0{,}95}) \cdot (0,1-0,95)^3 \approx 0,837174$;

b) w granicy liczby skrzyżowań zbiegającej do nieskończoności: $p = \lim_{n\to\infty} p_{n+1} \approx 0,513514$.

4.32. $\frac{121}{576}$.

4.33.

a) Bardziej prawdopodobne jest wygranie 3 z 4 partii niż 5 z 8.

b) Bardziej prawdopodobne jest wygranie nie mniej niż 5 z 8 partii od wygrania nie mniej niż 3 z 4 partii.

4.34. $\frac{1}{2}$

4.35. $\frac{2072}{3125}$.

Wskazówki dla Prowadzących

4.2.

a) Zdarzenia A, B i C możemy zakodować następująco: $A := \{(m,z) \in R \times R : m > 1.8\}$, $B := \{(m,z) \in R \times R : m > z\}$ oraz $C := \{(m,z) \in R \times R : z > 1.8\}$.

b) Zgodnie z opisem z podpunktu (a), zdarzenie $A \cap B \cap C$ zapisujemy jako

$$\{(m,z) \in R \times R : m > 1.8 \wedge m > z \wedge z > 1.8\},$$

czyli polega ono na tym że mąż jest wyższy od żony i oboje mierzą więcej niż 1.8 metra. Zdarzenie

$$(A \cap B) = \{(m,z) \in R \times R : m > 1.8 \wedge \neg(m > z)\}$$

odpowiada sytuacji w której mąż co prawda mierzy 180 cm wzrostu, ale nie jest wyższy od żony. Następnie,

$$A \cap \overline{B} \cap C = \{(m,z) \in R \times R : m > 1.8 \wedge m \leq z \wedge z > 1.8\}$$

jest zdarzeniem odpowiadającym sytuacji, w której oboje małżonkowie mierzą więcej niż 180 cm wzrostu i żona jest wyższa od męża, jak w poprzednim przykładzie.

c) $A \cap \overline{C} = \{(m,z) \in R \times R : m > 1.8 \wedge z \leq 1.8\}$, z czego wynika że do zbioru $A \cap \overline{C}$ należą te pary (m,z) dla których $m > 1.8 \leq z$ czyli w szczególności pary spełniające $m > z$, które należą do B. ponieważ każda para z $A \cap \overline{C}$ jest jakąś parą ze zbioru B, otrzymaliśmy pożądane zawieranie: $A \cap \overline{C} \subset B$.

4.3. Zdarzenie $A \cap B$ polega na otrzymaniu na obu kostkach nieparzystej sumy oczek i otrzymaniu jedynki wyłącznie na jednej kostce. Zdarzenie $A \cup B$ polega na tym, że suma oczek jest nieparzysta albo chociaż na jednej kostce pojawia się '1'. Zdarzenie $A \cap \overline{B}$ polega na otrzymaniu jako sumy oczek liczby nieparzystej przy jednoczesnym wykluczeniu jedynki na jakiejkolwiek kostce. Zbiór zdarzeń elementarnych składa się z następujących jednakowo możliwych zdarzeń:

$$\{(i,j) : (1 \geq i \geq 6) \wedge (1 \geq j \geq 6)\}.$$

Zbiór $A \cap B$ składa się z następujących zdarzeń elementarnych: $(1,2),(1,4),(1,6),(2,1),(4,1),(6,1)$. Korzystając z klasycznej definicji prawdopodobieństwa, mamy, że $P(A \cap B) = \frac{6}{36} = \frac{1}{6}$. Analogicznie, liczba zdarzeń elementarnych sprzyjających zdarzeniu $A \cup B$ wynosi 23, stąd $P(A \cup B) = \frac{23}{36}$ — zauważmy, że $A \cap B \subset A \cup B$ i $P(A \cap B) < P(A \cup B)$; zbiór $A \cap \overline{B}$ składa się z 12 zdarzeń elementarnych, stąd $P(A \cap \overline{B}) = \frac{1}{3}$ — zauważmy, że $A \cap \overline{B} \subset A \cup B$ i $P(A \cap \overline{B}) < P(A \cup B)$.

4.5. Zbiór zdarzeń elementarnych składa się ze wszystkich możliwych par postaci (i,j), $i \neq j$, $i,j \in \{1,2,3,4,5\}$. Z założenia, każde ze zdarzeń elementarnych jest jednakowo prawdopodobne. Oznaczmy przez A, B i C zbiory zdarzeń elementarnych sprzyjających zajściu zdarzenia wymienionego odpowiednio w punktach (a),(b) i (c). Mając na uwadze liczbę zdarzeń elementarnych sprzyjającą każdemu ze zdarzeń, otrzymujemy $P(A) = \frac{12}{20} = \frac{3}{5}$, $P(B) = \frac{12}{20} = \frac{3}{5}$ i $P(C) = \frac{6}{20} = \frac{3}{10} = P(A \cap B)$.

4.6. Oznaczmy ilość czarnego towaru przez x. Wtedy białego towaru będzie $3x$, a niebieskiego $\frac{3}{5}x$. Wszystkiego towaru jest więc $\frac{23}{5}x$. Stąd szukane prawdopodobieństwo jest równe

$$p = \frac{x}{\frac{23}{5}x} = \frac{5}{23}.$$

4.7. Sprzyjające są tu te przypadki, w których otrzymuje się kule w następujących układach: $(1,2)$, $(2,3)$, $(3,4)$ i $(4,5)$. Wszystkich możliwych przypadków jest tyle, ile można utworzyć różnych zbiorów dwuelementowych ze zbioru pięcioelementowego, w których do tego kolejność jest istotna, tzn. $\binom{5}{2} \cdot 2! = 20$. Zatem szukane prawdopodobieństwo to $p = \frac{4}{20} = \frac{1}{5}$.

4.8. Na parzystość sumy nie ma wpływu kolejność składników, a cyfry w danej sumie nie będą się powtarzały. Ilość wszystkich możliwych trójek (składników sumy) jest, bez uwzględnienia porządku, równa $\binom{5}{3}$. Ilość przypadków sprzyjających zdarzeniu jest równa ilości sposobów wylosowania dwóch cyfr nieparzystych i jednej spośród parzystych, co ostatecznie daje

$$p = \frac{\binom{3}{2} \cdot \binom{2}{1}}{\binom{5}{3}} = \frac{3}{5}.$$

4.9. Wypiszmy wszystkie możliwe permutacje i zliczmy dla każdej z nich ilość inwersji, i tak w permutacji $a_1a_2a_3$ jest 0 inwersji, $\underline{a_1a_3a_2}$ jest 1 inwersja, $\underline{a_2a_1a_3}$ jest 1 inwersja, $a_2a_3a_1$ są 2 inwersje, $a_3a_1a_2$ są 2 inwersje, $a_3a_2a_1$ są 3 inwersje. Element a_2 tworzy inwersję w permutacjach podkreślonych. Korzystając z założenia losowego wyboru permutacji i klasycznej definicji prawdopodobieństwa otrzymamy $p_1 = \frac{1}{2}$ i $p_2 = \frac{1}{3}$.

4.11. Zastrzelenie zająca mogło nastąpić bądź przez pierwszego myśliwego – zdarzenie A_1, bądź przez drugiego myśliwego – zdarzenie A_2, bądź przez obu myśliwych jednocześnie – zdarzenie $A_1 \cap A_2$. Oznaczając fakt zastrzelenia zająca przez A, mamy

$$P(A) = P(A_1) + P(A_2) - P(A_1 \cap A_2) = \frac{1}{3} + \frac{1}{3} - \frac{1}{9} = \frac{5}{9}.$$

Istnieje potrzeba uzasadnienia wzoru $P(A_1 \cap A_2) = P(A_1) \cdot P(A_2)$, ale załóżmy, że tak zachodzi (bo zdarzenia są niezależne).

4.12. Jeżeli przez E oznaczymy zdarzenie polegające na tym, że w n losowaniach przynajmniej raz pojawi się kula czarna, to $\overline{E}$ oznaczać będzie zdarzenie, że wśród tych n losowań pojawiły się kule wyłącznie białe. Z warunku zadania mamy, że $P(\overline{E}) = (\frac{20}{22})^n$, co tym samym daje $P(E) = 1 - (\frac{10}{11})^n > \frac{1}{2}$. Stąd otrzymujemy, że $(\frac{10}{11})^n < \frac{1}{2}$, czyli po zlogarytmowaniu $n > 7$, a więc $n = 8$.

4.13. Po pierwsze, jako że $P(A) = 1 - P(\overline{A})$, mamy $P(A) = \frac{2}{3}$. Następnie, mając na uwadze wzór $P(A \cup B) = P(A) + P(B) - P(A \cap B)$, otrzymujemy, że $P(B) = \frac{1}{4}$, a stąd $P(\overline{B}) = \frac{3}{4}$. Idąc dalej, jako że $P(A \cap \overline{B}) = P(A \setminus B) = P(A) - P(A \cap B)$ (bo zdarzenia $A \setminus B$ i $P(A \cap B)$ są rozłączne), mamy $P(A \cap \overline{B}) = \frac{5}{12}$. Podobnie, $P(B \setminus A) = 0$. (Wniosek: $B \subset A$.)

4.14. Po pierwsze, mając na uwadze wzór $P(A \cup B) = P(A) + P(B) - P(A \cap B)$, otrzymujemy, że $P(A) + P(B) = \frac{3}{4}$ (1). Z zależności $P(A \setminus B) = P(B \setminus A)$ otrzymujemy, że $P(A) = P(B)$. Ostatecznie z (1) daje to $P(B) = \frac{3}{8}$. Otrzymujemy również $P(B \setminus A) = P(B) - P(A \cap B) = \frac{1}{8}$.

4.16. Korzystając z klasycznej definicji prawdopodobieństwa, otrzymujemy:

a) $P(A) = \frac{1}{6}$;

b) $P(B) = \frac{11}{36}$;

c) $P(A \cap B) = \frac{1}{12}$.

d) Mając na uwadze wzór $P(A|B) = \frac{P(A \cap B)}{P(B)}$, otrzymujemy, że

$$P(A|B) = \frac{\frac{1}{12}}{\frac{11}{36}} = \frac{3}{11}.$$

4.17.

a) Z klasycznej definicji prawdopodobieństwa, otrzymujemy, że $P(A_c) = \frac{11}{20}$.

b) $P(A_c|A_n) = \frac{10}{12} > P(A_c)$, $P(A_c|A_z) = \frac{1}{8} < P(A_c)$.

4.18. Oznaczmy przez B_1 zdarzenie polegające na wylosowaniu kuli białej za pierwszym razem, a przez B_2 – kuli białej za drugim razem. Jak widać zajście zdarzenia B_2 jest zależne od zajścia zdarzenia B_1, gdyż po wylosowaniu pierwszej kuli białej zmniejsza się ilość kul białych w urnie (bo z def., A jest niezależne od B, jeśli $P(A|B) = P(A)$ i $P(B) > 0$, lub $P(B) = 0$). Zajście zdarzenia B polega na łącznym zajściu zdarzeń B_1 i B_2. Stąd $P(B) = P(B_1 \cap B_2) = P(B_1) \cdot P(B_2|B_1)$, a ponieważ $P(B_1) = \frac{3}{7}$ oraz $P(B_2|B_1) = \frac{1}{3}$, stąd $P(B) = \frac{1}{7}$.

4.19.

$$\begin{aligned} P(A) \cdot P(\overline{B}) &= P(A) \cdot (1 - P(B)) = P(A) - P(A \cap (B)) \\ &= P(A \setminus B) + P(A \cap B) - P(A \cap B) = P(A \setminus B) = P(A \cap \overline{B}). \end{aligned}$$

Podobnie, zachodzi:

$1 - P(A \cup B) = P(\overline{A} \cap \overline{B})$ oraz

$$\begin{aligned} P(\overline{A})P(\overline{B}) &= (1 - P(A))(1 - P(B)) = 1 - P(A) - P(B) + P(A \cap B) \\ &= 1 - P(A) - P(B) + P(A)P(B) = 1 - P(A \cup B), \end{aligned}$$

a stąd $P(\overline{A} \cap \overline{B}) = P(\overline{A})P(\overline{B})$.

4.21. W ogólnym przypadku, analizując możliwe zdarzenia elementarne otrzymamy, że $P(A) = \frac{1}{2}$, $P(B) = \frac{1}{4}$, $P(C) = \frac{1}{2}$, $P(D) = \frac{1}{2^{n-1}}$. Zdarzenia te nie są parami niezależne, bo np. $P(A \cap B) = \frac{1}{4} \neq P(A) \cdot P(B) = \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$.

4.23. Niech A oznacza zdarzenie polegające na wybraniu urny typu pierwszego, a B – wybraniu urny typu drugiego. Niech C oznacza wylosowanie kuli białej. Wówczas z twierdzenia o prawdopodobieństwie zupełnym otrzymujemy

$$P(C) = P(A) \cdot P(C|A) + P(B) \cdot P(C|B) = \frac{5}{13} \cdot \frac{2}{5} + \frac{8}{13} \cdot \frac{9}{15} = \frac{34}{65}.$$

4.24. Niech A oznacza zdarzenie polegające na wybraniu urny typu A, a B – wybraniu urny typu B. Niech C oznacza wylosowanie kuli białej. Wówczas z twierdzenia o prawdopodobieństwie zupełnym otrzymujemy

$$P(C) = P(A) \cdot P(C|A) + P(B) \cdot P(C|B) = \frac{1}{5} \cdot \frac{7}{10} + \frac{4}{5} \cdot \frac{4}{10} = \frac{23}{50}.$$

4.25. Niech $K_{1,2}$ oznacza zdarzenie polegające na wypadnięciu na kostce 1 lub 2, a $\overline{K_{1,2}}$ – zdarzenie doń przeciwne. Niech B oznacza wylosowanie kuli białej. Wówczas z twierdzenia o prawdopodobieństwie zupełnym otrzymujemy

$$P(B) = P(B|K_{1,2}) \cdot P(K_{1,2}) + P(B|\overline{K_{1,2}}) \cdot P(\overline{K_{1,2}}) = \frac{1}{3} \cdot \frac{1}{3} + \frac{1}{2} \cdot \frac{2}{3} = \frac{4}{9}.$$

4.26. Losowanie kuli z urny o ustalonym składzie pociąga za sobą następującą alternatywę wykluczających się zdarzeń: albo wylosowano kulę białą – zdarzenie B, albo kulę czarną – zdarzenie C. Wówczas zdarzenie Z o którym mowa w zadaniu, polega na wylosowaniu kuli białej w następnym ciągnięciu. Z twierdzenia o prawdopodobieństwie całkowitym mamy zatem

$$\begin{aligned} P(Z) &= P(B) \cdot P(B|B) + P(C) \cdot P(B|C) = \tfrac{b}{b+c} \cdot \tfrac{b-1}{b+c-1} + \tfrac{c}{b+c} \cdot \tfrac{b}{b+c-1} \\ &= \tfrac{b \cdot (b-1+c)}{(b+c) \cdot (b+c-1)} = \tfrac{b}{b+c}. \end{aligned}$$

4.27. Zdarzenie B polegające na wylosowaniu kuli białej z drugiej urny może zajść na skutek jednego z dwu wykluczających się zdarzeń — wylosowania albo kuli białej za pierwszym razem — zdarzenie B_1, albo odpowiednio kuli czarnej – zdarzenie przeciwne do $\overline{B_1}$. Tym samym, otrzymujemy

$$P(B) = P(B_1) \cdot P(B_2|B_1) + P(\overline{B_1}) \cdot P(B_2|\overline{B_1}) = \frac{b}{b+c} \cdot \frac{b_1+1}{b_1+c_1+1} + \frac{c}{b+c} \cdot \frac{b_1}{b_1+c_1+1}.$$

4.28. Patrz Zadanie 26.

4.29. Zdarzenie A_{n+1} polega na zajściu jednego z dwóch zdarzeń wykluczających się: $A_n \cap A_{n+1}$ i $\overline{A_n} \cap A_{n+1}$, a zatem $A_n = (A_n \cap A_{n+1}) \cup (\overline{A_n} \cap A_{n+1})$. Korzystając z twierdzenia o prawdopodobieństwie całkowitym mamy, że

$$P(A_{n+1}) = P(A_n) \cdot (A_{n+1}|A_n) + P(\overline{A_n}) \cdot P(A_{n+1}|\overline{A_n}).$$

Po wprowadzeniu podanych oznaczeń mamy, że $p_{n+1} = p_n \cdot a_n + q_n \cdot b$. Wyznaczając p_{n+1} otrzymujemy, że

$$p_{n+1} = p_1 c^n + b \cdot (1 + c + \ldots + c^{n-1}) = (p_1 - \frac{b}{1-c}) \cdot c^n + \frac{b(1-c^n)}{1-c},$$

gdzie $c = a - b$. Zauważmy, że uzyskany tutaj ciąg prawdopodobieństw jest najprostszym przypadkiem tzw. „łańcucha Markowa". Przy przejściu granicznym, gdy $n \to \infty$, otrzymujemy

$$p = \lim_{n \to \infty} p_{n+1} = \frac{b}{1-a+b}.$$

Ciekawym jest fakt, że p nie zależy od początkowej wartości p_1.

4.30. Korzystając ze wzoru otrzymanego w Zadaniu 4.29 otrzymujemy:

a) $p_3 = \frac{0{,}95(1-(1-0{,}1+0{,}95)^3)}{1-0{,}1+0{,}95} + (0,5 - \frac{0{,}95}{1-0{,}1+0{,}95}) \cdot (0,1-0,95)^3 \approx 0,837174$;

b) w granicy liczby skrzyżowań zbiegającej do nieskończoności: $p = \lim_{n\to\infty} p_{n+1} \approx 0,513514$.

4.32. Doświadczenie polega na rzucie kostką i monetą. Będziemy uważać je za udane, jeżeli otrzymamy piątkę i orła. Prawdopodobieństwo, że doświadczenie się uda $p = P(\text{piątka i orzeł})$. Ponieważ zdarzenia polegające na wyrzuceniu piątki i orła się niezależne, otrzymujemy $p = P(\text{piątki}) \cdot P(\text{orła}) = \frac{1}{6} \cdot \frac{1}{2} = \frac{1}{12}$. W naszym przypadku $n = 3$ i $k = 1$, zatem w myśl twierdzenia Bernoulliego

$$P_{3,1} = \binom{3}{1} \cdot (\frac{1}{12}) \cdot (\frac{11}{12})^2 = \frac{121}{576}.$$

4.33. Założenie równej siły gry pociąga za sobą, że prawdopodobieństwo wygrania p równe jest prawdopodobieństwu porażki $q = \frac{1}{2}$. Rozegranie partii można uważać za przeprowadzenie doświadczenia. Zakładając dodatkowo, że wynik jednej partii nie wpływa na wynik kolejnej, otrzymujemy doświadczenia niezależne. W celu obliczenia odpowiednich prawdopodobieństw można zatem zastosować wzór Bernoulliego.

a) $P_{4,3} = \binom{4}{3} \cdot (\frac{1}{2})^3 \cdot (\frac{1}{2}) = \frac{1}{4}$; $\quad P_{8,5} = \binom{8}{5} \cdot (\frac{1}{2})^5 \cdot (\frac{1}{2})^3 = \frac{7}{32}$.
Zatem $P_{4,3} > P_{8,5}$.

b) $P_{4,3\le k\le 4} = P_{4,3} + P_{4,4} = (\frac{1}{2})^4 \cdot \left(\binom{4}{3} + \binom{4}{4}\right) = \frac{5}{16}$.
$P_{8,5\le k\le 8} = P_{8,5} + P_{8,6} + P_{8,7} + P_{8,8} = (\frac{1}{2})^8 \cdot \left(\binom{8}{5} + \binom{8}{6} + \binom{8}{7} + \binom{8}{8}\right) = \frac{93}{256}$.
Zatem $P_{4,3\le k\le 4} < P_{8,5\le k\le 8}$.

4.34. Sukces oznacza zdarzenie wypadnięcia 4, 5 lub 6, zatem prawdopodobieństwo sukcesu wynosi $\frac{1}{2}$. Mamy n=7 prób, liczba sukcesów k spełnia $k \le 3$, stąd otrzymujemy prawdopodobieństwo wypadnięcia co najwyżej 3krotnie 4 5 lub 6 równe:

$$\begin{aligned} P_{0,7} + ... + P_{3,7} &= \binom{7}{0} \cdot (\tfrac{1}{2})^0 \cdot (\tfrac{1}{2})^7 + \binom{7}{1} \cdot (\tfrac{1}{2})^1 \cdot (\tfrac{1}{2})^6 + \binom{7}{2} \cdot (\tfrac{1}{2})^2 \cdot (\tfrac{1}{2})^5 + \binom{7}{3} \cdot (\tfrac{1}{2})^3 \cdot (\tfrac{1}{2})^4 \\ &= \tfrac{1}{2}^7 \cdot (1 + 7 + 21 + 35) = \tfrac{64}{2^7} = \tfrac{1}{2}. \end{aligned}$$

Zestaw zadań nr 5

Funkcje boolowskie

Zadanie 5.1. Które z poniższych równości są tożsamościowe w algebrze Boole'a $B = \{0, 1\}$?

a) $p + qr = q + pr$
b) $(r \oplus q)r = r \oplus qr$
c) $(p + q)r = pr(q + r) + qr$
d) $p \Rightarrow q = \neg p \Rightarrow \neg q$

Zadanie 5.2. Dla jakich wartości logicznych zmiennych zdaniowych p, q oraz r poniższe formuły są (i) prawdziwe; (ii) fałszywe?

a) $\neg(p \Rightarrow q)$
b) $\neg pq \Leftrightarrow p$
c) $((p \Rightarrow qr) \Rightarrow (\neg q \Rightarrow \neg p)) \Rightarrow \neg q$

Przykład 5.3. Przedstaw implikację $x \Rightarrow y$ za pomocą operatora `NAND` (dysjunkcja).

Rozwiązanie. Przypomnijmy, że

$$\texttt{NAND}(x, y) = \neg(x \wedge y), \;\; \texttt{NOR}(x, y) = \neg(x \vee y), \;\; \neg x = \texttt{NAND}(x, x) = \texttt{NOR}(x, x).$$

Z definicji wiemy, że $x \Rightarrow y$ jest równoważne $\neg x \vee y$. Następnie, korzystając z podwójnego zaprzeczenia oraz faktu, że $\neg(a \vee b) \equiv \neg a \wedge \neg b$, otrzymujemy

$$\neg x \vee y \equiv \neg(\neg((\neg x) \vee y)) \equiv \neg(\neg(\neg x) \wedge \neg y) \equiv \neg(x \wedge \neg y) \equiv \texttt{NAND}(x, \neg y) \equiv \texttt{NAND}(x, \texttt{NAND}(y, y)). \;\; \sharp$$

Zadanie 5.4. Przedstaw:

a) zaprzeczenie implikacji $y \Rightarrow x$ za pomocą operatora `NOR`,
b) $f(x, y) = x \vee y$ za pomocą operatora `NOR`,
c) $f(x, y) = x \wedge y$ za pomocą operatora `NOR`,
d) $f(x, y) = \neg x \vee y$ za pomocą operatora `NOR`,
e) $f(x, y) = x \wedge y$ za pomocą operatora `NAND`,
f) $f(x, y) = x \vee y$ za pomocą operatora `NAND`.

Definicja 5.3 Funkcja progowa $T_k^n(x_1, \ldots, x_n)$ *o* n *zmiennych z progiem* k *osiąga wartość* 1, *jeżeli liczba jedynek wśród (wartości) argumentów* $x_1, x_2, \ldots, x_n$ *wynosi przynajmniej* k, *tj. liczba jedynek osiągnie lub przekroczy* próg k. *Formalnie funkcja progowa* $T_k^n(x_1, \ldots, x_n)$ *określona jest następująco:*

$$T_k^n(x_1, \ldots, x_n) = \begin{cases} 1 & \text{gdy liczba jedynek wśród } x_1, \ldots, x_k \text{ jest równa lub większa od } k, \\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

W naszych rozważaniach zakładamy, że $1 \leq k \leq n$.

Przykład 5.5. Funkcje progowe dwóch zmiennych:

$$T_1^2(x, y) = x + y, \qquad T_2^2(x, y) = xy.$$

Załóżmy, że mamy już wyznaczone funkcje progowe $n-1$ zmiennych. Za ich pomocą możemy skonstruować wyrażenia dla funkcji progowych n zmiennych.

- $k = 1$: $T_1^n(x_1, \ldots, x_{n-1}, x_n) = \bigvee_{i=1}^n x_i$.
- $1 < k < n$: $T_k^n(x_1, \ldots, x_{n-1}, x_n) = T_k^{n-1}(x_1, \ldots, x_{n-1}) + T_{k-1}^{n-1}(x_1, \ldots, x_{n-1}) \cdot x_n$.

  Powyższa zależność wynika z następującej obserwacji: próg k jest osiągnięty wśród zmiennych $x_1, \ldots, x_{n-1}, x_n$ wtedy i tylko wtedy, gdy jest on osiągnięty albo tylko wśród zmiennych $x_1, \ldots, x_{n-1}$ albo jeżeli $x_n = 1$ i osiągnięty jest próg $k-1$ wśród zmiennych $x_1, \ldots, x_{n-1}$.
- $k = n$: $T_n^n(x_1, \ldots, x_{n-1}, x_n) = \bigwedge_{i=1}^n x_i$.

Zadanie 5.6. Napisz wyrażenia dla wszystkich funkcji progowych

a) trzech zmiennych,

b) czterech zmiennych.

Definicja 5.4 *Wprowadźmy oznaczenie* $x^1 = x$ *oraz* $x^0 = x$. *Następnie, dla dowolnego wektora* $a \in \{0,1\}^n$, *niech* $a(i)$ *oznacza* i*-tą współrzędną wektora* a. *Rozważmy teraz wyrażenie* $m_a(x) = x_1^{a(1)} \wedge x_2^{a(2)} \wedge \ldots \wedge x_n^{a(n)}$. *Zauważmy, że* $m_a(x) = 1$ *wtedy i tylko wtedy, gdy dla każdego* i *zachodzi* $x_i = a(i)$, *czyli dla* $x = a$. *Wówczas* dysjunkcyjna postać normalna *(ozn. DNF) funkcji* f *dana jest wzorem:*

$$f(x) = \bigvee_{a \in f^{-1}(1)} m_a(x).$$

Rozważmy teraz wyrażenie $s_a(x) = x_1^{\neg a(1)} \vee x_2^{\neg a(2)} \vee \ldots \vee x_n^{\neg a(n)}$. *Zauważmy, że* $s_a(x) = 0$ *wtedy i tylko wtedy, gdy dla każdego* i *zachodzi* $x_i = a(i)$, *czyli dla* $x = a$. *Wówczas* koniunkcyjna postać normalna *(ozn. CNF) funkcji* f *dana jest wzorem:*

$$f(x) = \bigwedge_{a \in f^{-1}(0)} s_a(x).$$

Przykład 5.7. Funkcja $f : B^3 \to B$ przyjmuje wartości równe 1 tylko dla wektorów $(1,0,0)$, $(0,1,0)$ i $(0,0,1)$. Przedstaw tą funkcję w postaciach normalnych (dysjunkcyjna – DNF i koniunkcyjna – CNF).

Rozwiązanie. W praktyce oznacza to, że aby przedstawić funkcję f w postaci DNF istotne są te argumenty, dla których przyjmuje ona wartość 1.

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	$\underline{1}$
0	1	0	$\underline{1}$
0	1	1	0
1	0	0	$\underline{1}$
1	0	1	0
1	1	0	0
1	1	1	0

x	y	z	$m_a(\cdot)$
0	0	0	
0	0	1	$\neg x \wedge \neg y \wedge z$
0	1	0	$\neg x \wedge y \wedge \neg z$
0	1	1	
1	0	0	$x \wedge \neg y \wedge \neg z$
1	0	1	
1	1	0	
1	1	1	

Ostatecznie postać dysjunkcyjna wygląda następująco:

$$f(x,y,z) = (\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z).$$

Natomiast, aby przedstawić funkcję f w postaci CNF istotne są te argumenty, dla których przyjmuje ona wartość 0.

x	y	z	$f(x,y,z)$
0	0	0	$\underline{0}$
0	0	1	1
0	1	0	1
0	1	1	$\underline{0}$
1	0	0	1
1	0	1	$\underline{0}$
1	1	0	$\underline{0}$
1	1	1	$\underline{0}$

x	y	z	$s_a(\cdot)$
0	0	0	$x \vee y \vee z$
0	0	1	
0	1	0	
0	1	1	$x \vee \neg y \vee \neg z$
1	0	0	
1	0	1	$\neg x \vee y \vee \neg z$
1	1	0	$\neg x \vee \neg y \vee z$
1	1	1	$\neg x \vee \neg y \vee \neg z$

Ostatecznie postać koniunkcyjna wygląda następująco:

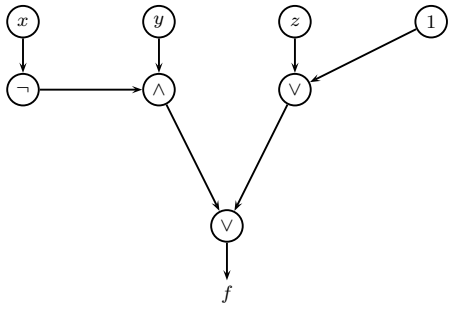
$$f(x,y,z) = (x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee z) \wedge (\neg x \vee \neg y \vee \neg z). \quad \sharp$$

Zadanie 5.8. Przedstaw poniższe funkcje w postaciach normalnych DNF i CNF:

a) $f(x,y,z) = (x \vee \neg y) \wedge (y \vee \neg z)$,
b) $f(x,y,z) = x \vee (\neg(y \Rightarrow z))$,
c) $f(x,y,z) = (\neg x \Rightarrow y) \wedge z$,
d) $f(x,y,z) = [(x \vee y) \wedge (x \vee z)] \oplus (x \wedge z)$,
e) $f(x,y,z) = (x \wedge y) \oplus (x \wedge y)$.

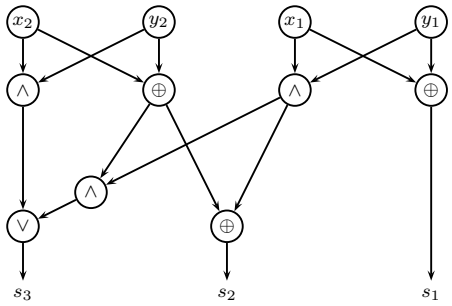
Przykład 5.9. Narysuj sieć boolowską dla funkcji $f(x,y,z) = \neg x \wedge y \vee z \vee 1$. Jaki jest koszt i głębokość otrzymanej sieci?

Rozwiązanie. Przykładową sieć boolowską przedstawia poniższy rysunek (należy wspomnieć, że postać sieci nie jest określona jednoznacznie). *Koszt* poniższej sieci (liczba tzw.*bramek*) wynosi 8, a jej *głębokość* (długość najdłuższej ścieżki) wynosi 4. ♯



Zadanie 5.10. Narysuj sieć boolowską dla funkcji z zadania 5.10 przed i po zamianie na postacie normalne. Jaki jest koszt i głębokość otrzymanych sieci?

Zadanie 5.11. Dla poniższej sieci sprawdź wynik przy $x_1 = 0, x_2 = 1, y_1 = 1, y_2 = 1$.



Zadanie 5.12. Jaki zbiór przedstawia wyrażenie $W(x, y, z) = xy + xz + yz$, jeżeli $x = \{1, 2, 4\}$, $y = \{1, 3, 5\}$ oraz $z = \{2, 3, 5\}$.

Zadanie 5.13. Niech X będzie zbiorem studentów, K – podzbiorem studentów grających w koszykówkę, S – grających w siatkówkę, P – uprawiających pływanie. Przedstaw wyrażenia boolowskie opisujące nastepujące podzbiory:

a) studentów uprawiających tylko jedną dyscyplinę sportu,

b) studentów uprawiających co najmniej jedną dyscyplinę sportu,

c) siatkarzy, którzy nie grają w koszykówkę.

Zadanie 5.14. Jaki ciąg przedstawia wyrażenie $W(x, y, z) = xy+xz+yz$, jeżeli $x = (1, 0, 0, 1, 1, 0, 1)$, $y = (1, 1, 1, 0, 0, 1, 0)$ oraz $z = (0, 0, 1, 1, 0, 1, 1)$.

Przykład 5.15. Dla wektorów $x = (1, 0, 0, 1, 1), r_1 = (0, 1, 1, 0, 0), r_2 = (1, 0, 1, 0, 0)$, policzyć $Par(x)$ i $Par_{r_i}(x), i = 1, 2$.

Rozwiązanie. Zgodnie z definicją:

$$Par(x) = \bigoplus_{i=1}^{5} x_i = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5, \text{ gdzie } x = x_1x_2x_3x_4x_5.$$

Zatem $Par(x) = 1$. Następnie korzystając z definicji

$$Par_r(x) = \bigoplus_{i=1}^{5}(x_i \wedge r_i) = (x_1 \wedge r_1) \oplus (x_2 \wedge r_2) \oplus (x_3 \wedge r_3) \oplus (x_4 \wedge r_4) \oplus (x_5 \wedge r_5), \text{ gdzie } x = x_1x_2x_3x_4x_5.$$

otrzymujemy, że $Par_{(0,1,1,0,0)}((1,0,0,1,1)) = 0$ oraz $Par_{(1,0,1,0,0)}((1,0,0,1,1)) = 1$. ♯

Zadanie 5.16. Dla wektorów $x = (0,1,1), r_1 = (0,0,1), r_2 = (0,1,0), r_3 = (1,0,1), r_4 = (1,1,0)$, policzyć $Par(x)$ i $Par_{r_i}(x), i = 1,2,3,4$.

Przykład 5.17. Dany jest wektor $x = (0,1,1)$. Dla jakich wektorów $r \in B^3$, $Par_r(x) = 1$?

Rozwiązanie. Zgodnie z definicją otrzymujemy, że

$$Par_{(r_1,r_2,r_3)}((0,1,1)) = \bigoplus_{i=1}^{3}(x_i \wedge r_i) = (0 \wedge r_1) \oplus (1 \wedge r_2) \oplus (1 \wedge r_3) = 0 \oplus r_2 \oplus r_3 = r_2 \oplus r_3 = 1.$$

Równość ta pociąga za sobą, że albo $r_2 = 1$ i $r_3 = 0$ albo $r_2 = 0$ i $r_3 = 1$; zauważmy, że r_1 jest dowolne. Zatem szukane $r \in \{(0,0,1),(1,0,1),(0,1,0),(1,1,0)\}$. ♯

Zadanie 5.18. Dane są 2 wektory:

a) $x = (1,0,1)$ i $y = (0,1,0)$. Dla jakich wektorów $r \in B^3$ zachodzi $Par_r(x) = Par_r(y)$?
b) $x = (1,1,0)$ i $y = (0,0,1)$. Dla jakich wektorów $r \in B^3$ zachodzi $Par_r(x) = Par_r(y)$?
c) $x = (0,1,0)$ i $y = (0,0,1)$. Dla jakich wektorów $r \in B^3$ zachodzi $Par_r(x) \neq Par_r(y)$?

Odpowiedzi do zadań

5.1.

TAK: b) c)
NIE: a) d)

5.2.

a) i) $(p, q) = (1, 0)$
ii) pozostałe przypadki

b) i) $(p, q) = (1, 0)$
ii) pozostałe przypadki

c) i) $(p, q) \in \{(0, 0, 0), (0, 0, 1), (1, 0, 0), (1, 0, 1)\}$
ii) pozostałe przypadki

5.4.

a) $\neg(y \Rightarrow x) \equiv \texttt{NOR}(\texttt{NOR}(y, y), x)$

b) $x \vee y \equiv \texttt{NOR}(\texttt{NOR}(x, y), \texttt{NOR}(x, y))$

c) $x \wedge y \equiv \neg(\neg(x \wedge y)) \equiv \texttt{NOR}(\texttt{NOR}(x, x), \texttt{NOR}(y, y))$

d) $\neg x \vee y \equiv \texttt{NOR}(\texttt{NOR}(\texttt{NOR}(x, x), y), \texttt{NOR}(\texttt{NOR}(x, x), y))$

e) $x \wedge y \equiv \texttt{NAND}(\texttt{NAND}(x, y), \texttt{NAND}(x, y))$

f) $x \vee y \equiv \texttt{NAND}(\texttt{NAND}(x, x), \texttt{NAND}(y, y))$

5.7.

$T_1^3(x, y, z) = x + y + z$
$T_2^3(x, y, z) = xy + yz + xz$
$T_3^3(x, y, z) = xyz$
$T_1^4(x, y, z, t) = x + y + z + t$
$T_2^4(x, y, z, t) = xy + yz + xz + xt + yt + zt$
$T_3^4(x, y, z, t) = xyz + xyt + yzt + xzt$
$T_4^4(x, y, z, t) = xyzt$

5.10.

a) DNF: $f(x, y, z) = (\neg x \wedge \neg y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge \neg z) \vee (x \wedge y \wedge z)$
CNF: $f(x, y, z) = (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee \neg z)$

b) DNF: $f(x, y, z) = (\neg x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge y \wedge \neg z) \vee (x \wedge y \wedge z)$
CNF: $f(x, y, z) = (x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee \neg z)$

c) DNF: $f(x,y,z) = (\neg x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z) \vee (x \wedge y \wedge z)$
CNF: $f(x,y,z) = (x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee z)$

d) DNF: $f(x,y,z) = (\neg x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge \neg z)$
CNF: $f(x,y,z) = (x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee \neg z)$

e) CNF: $f(x,y,z) = (x \vee y \vee z) \wedge (x \vee y \vee \neg z) \wedge (x \vee \neg y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee y \vee z) \wedge (\neg x \vee \neg y \vee z) \wedge (\neg x \vee y \vee \neg z) \wedge (\neg x \vee \neg y \vee \neg z)$

5.13. $s_1 = 1, s_2 = 0, s_3 = 1$

5.14. $W(x,y,z) = \{1,2,3,5\}$

5.15.

a) $(K \wedge \neg S \wedge \neg P) \vee (\neg K \wedge S \neg P) \vee (\neg K \wedge \neg S \wedge P)$

b) $K \vee S \vee P$

c) $S \wedge \neg K$

5.16. $W(x,y,z) = (1,0,1,1,0,1,1)$.

5.18. $Par(x) = 0, Par_{r_1}(x) = Par_{r_2}(x) = Par_{r_3}(x) = Par_{r_4}(x) = 1$

5.20.

a) $r \in \{(0,1,1),(1,1,0),(1,0,1),(0,0,0)\}$

b) $r \in \{(0,1,1),(1,1,0),(1,0,1),(0,0,0)\}$

c) $r \in \{(0,1,0),(1,1,0),(0,0,1),(1,0,1)\}$

Zestaw zadań nr 6

Teoria liczb

Przykład 6.1. Niech r będzie resztą z dzielenia b przez a. Załóżmy, że $c|a$ i $c|b$. Wykaż, że $c|r$.

Rozwiązanie. Niech $b = a \cdot q + r$. Mamy $a = c \cdot n$, $b = c \cdot m$, a zatem $r = b - a \cdot q = c \cdot (m - n \cdot q)$. Tym samym c jest dzielnikiem r. ♯

Zadanie 6.2. Załóżmy, że $a|b$, gdzie a i b są dowolnymi liczbami dodatnimi. Niech r będzie resztą z dzielenia c przez a i niech s będzie resztą z dzielenia c przez b. Co jest resztą z dzielenia s przez a?

Twierdzenie 6.3 *Niech $a = b \bmod m$, $c = d \bmod m$. Wówczas:*

$$\begin{aligned} (a + c) &= (b + d) \bmod m, \\ (a - c) &= (b - d) \bmod m, \\ ac &= bd \bmod m. \end{aligned}$$

Przykład 6.4. Oblicz $(50 \cdot 51 + 15) \bmod 7$.

Rozwiązanie. Jako że $50 = 1 \bmod 7$, $51 = 2 \bmod 7$ oraz $15 = 1 \bmod 7$, na mocy powyższego twierdzenia otrzymujemy

$$(50 \cdot 51 + 15) \bmod 7 = (1 \cdot 2 + 1) \bmod 7 = 3 \bmod 7.$$ ♯

Zadanie 6.5. Oblicz:

a) $15 \cdot 36 \bmod 7$,
b) $15^3 \cdot (37)^3 \bmod 7$,
c) $(26^4 \cdot 18 + 2004) \bmod 5$,
d) $7000 \bmod 9$,
e) $1958 \bmod 17$,
f) $10^{39} \bmod 11$,
g) $2^{39} \bmod 5$,
h) $7^{40} \bmod 10$.

Zadanie 6.6. Oblicz ostatnią cyfrę liczby 2^{100}.

Dla relacji przystawania modulo m zdefiniujmy klasy abstrakcji – dla dowolnej liczby całkowitej x, *klasę abstrakcji* elementu x definiujemy w następujący sposób: $[x] = \{y \mid y = x \bmod m\}$. Zauważmy, że klasy abstrakcji mają następujące własności:

– Jeżeli $x = y \bmod m$, to $[x] = [y]$.
– Jeżeli $[x] \cap [y] \neq \emptyset$, to $[x] = [y]$.

Zadanie 6.7. Wyznacz klasy abstrakcji relacji kongruencji dla $m = 6$.

Zadanie 6.8. Jak wyglądają działania dodawania i mnożenia w pierścieniu $\mathbb{Z}_6$.

Zadanie 6.9. W pierścieniu $\mathbb{Z}_8$ rozwiąż następujące równania:

a) $1 + x_1 = 0$,
b) $1 + x_2 = 2$,
c) $5 + x_3 = 0$,
d) $5 + x_4 = 2$.

Rozważmy dowolny element a należący do pierścienia $\mathbb{Z}_m$. Mówimy, że $b \in \mathbb{Z}_m$ jest *elementem odwrotnym do* a (ozn. a^{-1}), jeśli $a \cdot b = 1$.

Zadanie 6.10. Przedstaw tabliczkę dodawania i mnożenia w ciele $\mathbb{Z}_7$, a następnie podaj elementy odwrotne do 5 i 6 w $\mathbb{Z}_7$.

6.1 Największy wspólny dzielnik, elementy odwrotne

Algorytm Euklidesa wyznaczania $NWD(a, b)$.

1. Dopóki $a \neq b$ wykonuj:

   1.a Jeśli $a > b$, podstaw $a := a - b$;

   1.b w przeciwnym wypadku podstaw $b := b - a$.

2. Zwróć a.

Szybki algorytm wyznaczania $NWD(a, b)$.

1. Dopóki $a \cdot b \neq 0$ wykonuj:

   1.a Jeśli $a > b$, podstaw $a := a \bmod b$;

   1.b w przeciwnym wypadku podstaw $b := b \bmod a$.

2. Zwróć $\max\{a, b\}$.

Przykład 6.11. Oblicz $NWD(32, 12)$ używając powyższych dwóch algorytmów.

Rozwiązanie.

- Algorytm 1.

a	b
32	12
20	12
8	12
8	4
4	4

  Otrzymujemy zatem $NWD(32, 12) = 4$.

- Algorytm 2.

a	b	
32	12	$\underline{32} = 2 \cdot \underline{12} + 8$
8	12	$\underline{12} = 1 \cdot \underline{8} + 4$
8	4	$\underline{8} = 2 \cdot \underline{4} + 0$
0	4	

Otrzymujemy zatem $NWD(32, 12) = 4$. ♯

Zadanie 6.12. Oblicz $NWD(a, b)$, gdzie:

a) $a = 68, b = 36$,
b) $a = 600, b = 1050$,
c) $a = 1547, b = 560$.

Twierdzenie 6.13 *Niech d będzie największym wspólnym dzielnikiem dodatnich naturalnych liczb a i b. Wówczas istnieją liczby całkowite x i y takie, że $xa + yb = d$.*

Przykład 6.14. Podaj x i y (całkowite), dla których $NWD(32, 12) = x \cdot 32 + y \cdot 12$.

Rozwiązanie. Aby rozwiązać powyższe równanie korzystamy z szybkiego algorytmu wyznaczania $NWD(a, b)$. Przypomnijmy wyliczenia tego algorytmu poczynione w zadaniu 6.11 w celu wyznaczenia $NWD(32, 12)$.

$$\begin{aligned} \underline{32} &= 2 \cdot \underline{12} + 8 \\ \underline{12} &= 1 \cdot \underline{8} + 4 \\ \underline{8} &= 2 \cdot \underline{4} + 0 \end{aligned}$$

Rozważając teraz kolejne kroki od przedostatniego równania, otrzymamy:

$$\begin{aligned} 4 &= 12 - 1 \cdot 8 \\ &= 12 - 1 \cdot (32 - 2 \cdot 12) \\ &= (-1) \cdot 32 + 3 \cdot 12. \end{aligned}$$

A zatem szukanymi liczbami są $x = -1$ i $y = 3$. ♯

Zadanie 6.15. Zastosuj powyższy algorytm w celu rozwiązania następujących równań:

a) $68x + 36y = NWD(68, 36)$,
b) $600x + 1050y = NWD(600, 1050)$,
c) $1547x + 560y = NWD(1547, 560)$.

Zauważmy, że jeżeli liczba a z przedziału $1 \leq a \leq m - 1$ jest względnie pierwsza z m, tzn. $NWD(a, m) = 1$, wówczas a ma w $\mathbb{Z}_m$ element odwrotny względem mnożenia:

$$NWD(a, m) = 1, \text{ a zatem}$$

$$\text{istnieją } x \text{ i } y \text{ takie, że } x \cdot a + y \cdot m = 1$$

$$x \cdot a + y \cdot m = 1 \quad / \bmod m$$

$$x \cdot a = 1 \bmod m$$
$$x = a^{-1}.$$

Przykład 6.16. Znajdź element odwrotny do 7 w $\mathbb{Z}_{26}$.

Rozwiązanie. Aby znaleźć rozwiązanie, znowu korzystamy z roszerzonego algorytmu Euklidesa.

Rozszerzony algorytm Euklidesa.

Wejście: dwie liczby naturalne a i b.
Wyjście: $NWD(a,b)$ oraz liczby całkowite x, y takie, że $xa + yb = NWD(a,b)$.

1. Podstaw $c := 0$; $x_a := 1$; $y_a := 0$; $x_b = 0$; $y_b = 1$.
2. Dopóki $a \cdot b \neq 0$, wykonuj:
   2.a Jeśli $a \geq b$, to
      2.a.1 $c := a \div b$;
      2.a.2 $a := a \bmod b$;
      2.a.3 $x_a = x_a - x_b \cdot c$;
      2.a.4 $y_a = y_a - y_b \cdot c$.
   2.b W przeciwnym wypadku
      2.b.1 $c := b \div a$;
      2.b.2 $b := b \bmod a$;
      2.b.3 $x_b = x_b - x_a \cdot c$;
      2.b.4 $y_b = y_b - y_a \cdot c$.
3. Jeśli $a > 0$, to $x := x_a$; i $y := y_a$.
   w przeciwnym wypadku, jeśli $b > 0$, to $x := x_b$; i $y := y_b$.
4. Zwróć $NWD(a,b) := a + b$ oraz liczby x i y.

Wykonanie algorytmu ilustruje poniższa tabela.

a	b	c	x_a	y_a	x_b	y_b
7	26	0	1	0	0	1
7	5	3	1	0	-3	1
2	5	1	4	-1	-3	1
2	1	2	4	-1	-11	3
0	1	2	26	-7	-11	3

Otrzymujemy $NWD(26,7) = 1$, a zatem będzie istniał element odwrotny do 7 w $\mathbb{Z}_{26}$. Ponadto odczytujemy, że $1 = (-11) \cdot 7 + 3 \cdot 26$. Stąd $7^{-1} = -11 \bmod 26 = 15$, czyli 15 jest elementem odwrotnym do 7 w $\mathbb{Z}_{26}$. ♯

Zadanie 6.17. Znajdź elementy odwrotne do wszystkich elementów odwracalnych w $\mathbb{Z}_8$.

Zadanie 6.18. Znajdź element odwrotny do 11 w $\mathbb{Z}_{19}$.

Zadanie 6.19. W pierścieniu $\mathbb{Z}_8$ rozwiąż równania $3 \cdot x_1 = 1$ oraz $3 \cdot x_2 = 2$.

Zadanie 6.20. W pierścieniu $\mathbb{Z}_{17}$ rozwiąż równania $8 \cdot x_1 = 2$ oraz $9 \cdot x_2 = 4$.

Zadanie 6.21. Znajdź całkowite rozwiązanie (x, y) spełniające równanie $17x + 40y = 1$.

6.2 Układy równań, szyfry liniowe

Twierdzenie 6.22 *Rozważmy funkcję liniową* $(\star)$ *postaci* $ax = b \bmod m$, *gdzie* $0 \leq a$ *i* $b < m$. *Wówczas:*

1) *Jeżeli* $NWD(a, m) = 1$, *wówczas istnieje rozwiązanie, które możemy wyznaczyć znajdując* a^{-1}, *ponieważ* $x = a^{-1}ax = a^{-1}b \bmod m$.

2) *Jeśli* $NWD(a, m) = d$, *wówczas rozwiązanie istnieje wtt* $d|b$. *I w tym przypadku kongruencja* $(\star)$ *jest równoważna kongruencji* $a'x = b' \bmod m'$, *gdzie* $a' = (a/d)$, $b' = (b/d)$, $m' = (m/d)$.

Przykład 6.23. Niech $a = 7$ i $b = 12$. Korzystając z przekształcenia afinicznego

$$C(x) = (ax + b) \bmod n$$

zaszyfruj wiadomość AZURE RAY w 26-literowym alfabecie.

Rozwiązanie. Przyjmując $A = 0, Z = 25, U = 20, R = 17, E = 4, Y = 24$, otrzymujemy:

$C(0) = (7 \cdot 0 + 12) \bmod 26 = 12$, czyli M,
$C(25) = (7 \cdot 25 + 12) \bmod 26 = 5$, czyli F,
$C(20) = (7 \cdot 20 + 12) \bmod 26 = 22$, czyli W,
$C(17) = (7 \cdot 17 + 12) \bmod 26 = 1$, czyli B,
$C(4) = (7 \cdot 4 + 12) \bmod 26 = 14$, czyli O,
$C(24) = (7 \cdot 24 + 12) \bmod 26 = 24$, czyli Y,

a tym samym zaszyfrowana wiadomość brzmi MFWBO BMY. ♯

Zadanie 6.24. Niech $a = 7$ i $b = 12$. Korzystając z przekształcenia afinicznego

$$C(x) = (ax + b) \bmod n$$

zaszyfruj wiadomość INFORMA w 26-literowym alfabecie.

Przykład 6.25. W przechwyconym kryptogramie najczęściej występującą literą jest K, potem D. Wiedząc, że w języku angielskim najczęściej występują litery E i T oraz że użyto funkcji kodującej postaci $C(x) = (ax + b) \bmod m$, wyznacz tę funkcję oraz funkcję dekodującą.

Rozwiązanie. Z warunków zadania otrzymujemy, że $C(4) = 10$ oraz $C(19) = 3$, czyli — przyjmując $C(x) = ax + b$ — otrzymujemy następujący układ równań:

$$\begin{cases} 4a + b = 10 \bmod 26 \\ 19a + b = 3 \bmod 26 \end{cases}.$$

Odejmując stronami, otrzymujemy równanie $15a = -7 \bmod 26 = 19 \bmod 26$, a stąd $a = 15^{-1} \cdot 19 \bmod 26$. Korzystając z rozszerzonego algorytmu Euklidesa wyznaczamy 15^{-1} w $\mathbb{Z}_{26}$, otrzymując $15^{-1} = 7$. A zatem $a = 7 \cdot 19 \bmod 26 = 3$. Następnie np. z drugiego równania wyznaczamy b:

$$b = 10 - 4a \bmod 26 = 10 - 4 \cdot 3 \bmod 26 = -2 \bmod 26 = 24 \bmod 26.$$

A zatem funkcja kodująca $C(x)$ jest postaci $C(x) = 3x + 24$.

Funkcję dekodującą $D(y) = ay+b$ możemy wyznaczyć w podobny sposób przyjmując $D(10) = 4$, a tym samym otrzymując następujący układ równań:

$$\begin{cases} 10a + b = 4 \bmod 26 \\ 3a + b = 19 \bmod 26 \end{cases}.$$

Otrzymamy w rezultacie $D(y) = 9y + 18$.

Innym sposobem jest spojrzenie na funkcję dekodującą jako na funkcję odwrotną do funkcji $C(x)$, a tym samym policzenie $D(y)$ ze wzoru na $C(x)$. A dokładnie, przekształcamy:

$$y = 3x + 24$$

$$y - 24 = 3x$$

$$3^{-1} \cdot y - 3^{-1} \cdot 24 = x.$$

Jako że $3^{-1} = 9$ w $\mathbb{Z}_{26}$, otrzymujemy $x = 9y + 18$. Stąd $D(y) = 9y + 18$. ♯

Zadanie 6.26. W długim kryptogramie zaszyfrowanym za pomocą przekształcenia afinicznego najczęściej występuje litera H, potem C.

a) Odszyfruj fragment wiadomości ...WVB... .

b) Zaszyfruj wiadomość HIGH.

Przykład 6.27. Rozwiąż poniższy układ równań:

$$\begin{cases} 14x + y = 1 \bmod 26 \\ 24x + y = 15 \bmod 26 \end{cases}.$$

Rozwiązanie. Odejmując stronami (II−I) otrzymujemy równanie $10x = 14 \bmod 26$. Zauważmy, że zachodzi $NWD(10, 26) = 2$ oraz i $2|14$, a zatem zgodnie z twierdzeniem 6.22 rozważamy równanie

$$5x = 7 \bmod 13.$$

Jako że $5^{-1} = 8$ w $\mathbb{Z}_{13}$, otrzymujemy

$$x = 5^{-1} \cdot 7 \bmod 13 = 8 \cdot 7 \bmod 13 = 4 \bmod 26.$$

Zauważmy, że jest to rozwiązanie w $\mathbb{Z}_{13}$, a my szukamy rozwiązań w $\mathbb{Z}_{26}$. Jako że rozwiązaniami równania $5x = 7 \bmod 13$ są dowolne liczby postaci $x = 4 + 13n$, gdzie $n \in \mathbb{Z}$, rozwiązań równania $10x = 14 \bmod 26$ szukamy właśnie pośród liczb postaci $(4 + 13n) \bmod 26$. W konsekwencji otrzymujemy, że drugim rozwiązaniem w $\mathbb{Z}_{26}$, oprócz $x = 4$, jest także $x = 4 + 13 = 17$.

Pozostaje wyznaczyć y np. z pierwszego równania:

– dla $x = 4$ otrzymujemy $y = 1 - 14x \bmod 26 = 1 - 14 \cdot 4 \bmod 26 = 23$;

– dla $x = 17$ otrzymujemy $y = 1 - 14x \bmod 26 = 1 - 14 \cdot 17 \bmod 26 = 23$.

A zatem szukanymi rozwiązaniami w $\mathbb{Z}_{26}$ są $x = 4$ i $y = 23$ oraz $x = 17$ i $y = 23$. ♯

Zadanie 6.28. Rozwiąż poniższy układ równań.

$$\begin{cases} 3x + y = 1 \bmod 27 \\ 9x + y = 13 \bmod 27 \end{cases}$$

Przykład 6.29. Rozwiąż równanie $x^2 - 3x + 2 = 0 \bmod 53$.

Rozwiązanie. Równanie $x^2 - 3x + 2 = 0 \bmod 53$ równoważne jest równaniu

$$(x-2)(x-1) = 0 \bmod 53.$$

Zatem rozwiązania są następujące: $x = 2 \bmod 53$ oraz $x = 1 \bmod 53$. ♯

Zadanie 6.30. Rozwiąż następujące równania:

a) $x^2 - 2x = 0 \bmod 11$,
b) $x^2 = 4 \bmod 23$.

6.3 Chińskie twierdzenie o resztach

Zadanie 6.31. Dla jakich par reszt a_1 i a_2 istnieją liczby spełniające poniższe układy kongruencji?

$$a) \begin{cases} a_1 = a \bmod 4 \\ a_2 = a \bmod 6 \end{cases} \qquad b) \begin{cases} a_1 = a \bmod 3 \\ a_2 = a \bmod 6 \end{cases} \qquad c) \begin{cases} a_1 = a \bmod 3 \\ a_2 = a \bmod 5 \end{cases}$$

Uwaga. Uprzedzając rozwiązanie, zauważmy, że ilość par reszt, dla których istnieje liczba spełniająca układ kongruencji wynosi $(a_1 \cdot a_2)/d$, gdzie $d = NWD(a_1, a_2)$.

Twierdzenie 6.32 (Chińskie twierdzenie o resztach) *Niech $m_1, \ldots, m_r$ będą dodatnimi liczbami względnie pierwszymi, to znaczy dla każdej pary $1 \leq i < j \leq r$ mamy $NWD(m_i, m_j) = 1$, oraz niech $a_1, \ldots, a_r$ będą dowolnymi resztami. Wtedy istnieje liczba całkowita a taka, że*:

$$\begin{cases} a_1 = a \bmod m_1 \\ a_2 = a \bmod m_2 \\ \ldots \\ a_r = a \bmod m_r \end{cases}.$$

W szczególności, rozwiązaniem powyższego układu jest $a = \sum_{i=1}^{r} a_i M_i N_i$, gdzie:

$M_i = M/m_i$,
$M = \prod_{i=1}^{r} m_i$,
a N_i spełnia $N_i M_i = 1 \bmod m_i$.

Ponadto, jeżeli liczby a i b są rozwiązaniami powyższego układu kongruencji, to ich różnica $a - b$ dzieli się przez iloczyn wszystkich liczb m_i, czyli przez $M = \prod_{i=1}^{r} m_i$.

Przykład 6.33. Rozwiąż poniższy układ kongruencji.

$$\begin{cases} 2 = a \bmod 3 \\ 0 = a \bmod 4 \end{cases}$$

Rozwiązanie. Zgodnie z twierdzeniem 6.32, wyznaczamy:

$M = 3 \cdot 4 = 12$, czyli $M_1 = 12/3 = 4$, zatem $N_1 \cdot 4 = 1 \bmod 3$, stąd $N_1 = 1$.
$M = 3 \cdot 4 = 12$, czyli $M_2 = 12/4 = 3$, zatem $N_2 \cdot 3 = 1 \bmod 4$, stąd $N_2 = 3$.

Zatem $a_1 = 2$, $a_2 = 0$, a stąd $a = 2 \cdot 4 \cdot 1 + 0 \cdot 3 \cdot 3 \bmod 12 = 8$. ♯

Zadanie 6.34. Rozwiąż poniższe układy kongruencji.

$$a) \quad \begin{cases} 1 = a \bmod 3 \\ 4 = a \bmod 5 \end{cases} \qquad b) \quad \begin{cases} 2 = a \bmod 3 \\ 3 = a \bmod 5 \end{cases} \qquad c) \quad \begin{cases} 2 = a \bmod 3 \\ 3 = a \bmod 5 \\ 5 = a \bmod 7 \end{cases}$$

Zadanie 6.35. Niech m_1 i m_2 będą dowolnymi liczbami całkowitymi. Dla jakich par reszt a_1 i a_2 istnieje liczba a spełniająca poniższy układ kongruencji?

$$\begin{cases} a_1 = a \bmod m_1 & (0 \le a_1 \le m_1 - 1) \\ a_2 = a \bmod m_2 & (0 \le a_2 \le m_2 - 1) \end{cases}$$

Przykład 6.36. Ile wynosi reszta z dzielenia 1997199919 przez 15?

Rozwiązanie. Rozważmy układy kongruencji:

$$\begin{cases} 1 = M \bmod 3 \\ 4 = M \bmod 5 \end{cases} \qquad \begin{cases} 1 = x \bmod 3 \\ 4 = x \bmod 5 \end{cases}$$

Mając na uwadze Chińskie twierdzenie o resztach, zachodzi $(3 \cdot 5) | (M - x)$, a stąd $M - x = k \cdot 3 \cdot 5$, czyli $M = k \cdot 15 + x$. Pozostaje zatem wyznaczyć x. Rozważmy poniższy układ kongruencji.

$$\begin{cases} 1 = x \bmod 3 \\ 4 = x \bmod 5 \end{cases}$$

Układ ten występuje w zadaniu 6.32(a) — otrzymujemy zatem, że $x = 4$. Jako że 4 jest jedyną liczbą ze zbioru $\{0, \ldots, 14\}$, która spełnia kongruencję (bo 3 i 5 są względnie pierwsze), zatem otrzymujemy, że $1997199919 \bmod 15 = 4$. ♯

Zadanie 6.37. Ile wynosi reszta z dzielenia 19831583279 przez 20?

6.4 Pierwiastki kwadratowe

Liczbę y nazywamy *pierwiastkiem kwadratowym* liczby x w pierścieniu $\mathbb{Z}_m$, jeśli

$$x = y^2 \bmod m.$$

Na przykład łatwo sprawdzić, że w $\mathbb{Z}_5$ pierwiastkami 4 są 2 i 3, ponieważ $2^2 \bmod 5 = 3^2 \bmod 5 = 4$, a np. liczba 2 nie posiada pierwiastka. Ponadto zauważmy, że jeśli y jest pierwiastkiem x, wówczas $m - y$ także:

$$(m - y)^2 = m^2 - 2my + y^2 \equiv_m y^2 = x.$$

W ogólnym przypadku rozważmy liczbę m, która jest iloczynem k różnych liczb pierwszych $p_1 < p_2 < \ldots < p_k$. Weźmy teraz dowolną liczbę y, dla której:

$$y \bmod p_1 = 1 \quad \text{lub} \quad y \bmod p_1 = -1,$$

$$y \bmod p_2 = 1 \quad \text{lub} \quad y \bmod p_2 = -1,$$

$$\ldots$$

$$y \bmod p_k = 1 \quad \text{lub} \quad y \bmod p_k = -1.$$

Wówczas $y^2 \bmod p_i = 1$, $i = 1, \ldots k$, i z Chińskiego twierdzenia o resztach wynika, że

$$y^2 = 1 \bmod p_1 \cdot \ldots \cdot p_k.$$

Jeśli $2 < p_1 < p_2 < \ldots < p_k$, wówczas $1 \neq -1 \bmod p_i$, $i = 1. \ldots, k$ i tym samym będziemy mieli 2^k różnych pierwiastków z 1:

$y_1 : \quad y \bmod p_i = 1,\ i = 1, \ldots, k.$
$y_2 : \quad y \bmod p_1 = -1,\ y \bmod p_i = 1,\ i = 2, \ldots, k.$
$\ldots$
$y_{2^k} : \quad y \bmod p_i = -1,\ i = 1, \ldots, k.$

Przykład 6.38. Ile jest pierwiastków kwadratowych z 1 w $\mathbb{Z}_{30}$? Wskaż je.

Rozwiązanie. Jako że $30 = 2 \cdot 3 \cdot 5$, wszystkie szukane pierwiastki wyznaczyć można z kolejnych układów równań:

1. $y_1 \bmod 2 = 1,\ y_1 \bmod 3 = 1,\ y_1 \bmod 5 = 1$;
2. $y_2 \bmod 2 = 1,\ y_2 \bmod 3 = 1,\ y_2 \bmod 5 = -1$;
3. $y_3 \bmod 2 = 1,\ y_3 \bmod 3 = -1,\ y_3 \bmod 5 = 1$;
4. $y_4 \bmod 2 = 1,\ y_4 \bmod 3 = -1,\ y_4 \bmod 5 = -1$;
5. $y_5 \bmod 2 = -1,\ y_5 \bmod 3 = 1,\ y_5 \bmod 5 = 1$;
6. $y_6 \bmod 2 = -1,\ y_6 \bmod 3 = 1,\ y_6 \bmod 5 = -1$;
7. $y_7 \bmod 2 = -1,\ y_7 \bmod 3 = -1,\ y_7 \bmod 5 = 1$;
8. $y_8 \bmod 2 = -1,\ y_8 \bmod 3 = -1,\ y_8 \bmod 5 = -1$.

Zauważmy jednak, że $p_1 = 2$ i $1 = -1 \bmod 2$, a tym samym będą tylko cztery różne pierwiastki kwadratowe, tzn. wystarczy wyznaczyć tylko liczby y_1, y_2, y_3 oraz y_4.

1. Liczbą y_1 spełniającą
$$\begin{cases} y_1 \bmod 2 = 1 \\ y_1 \bmod 3 = 1 \\ y_1 \bmod 5 = 1 \end{cases}$$
jest $y_1 = 1$.

2. Liczbą y_2 spełniającą
$$\begin{cases} y_2 \bmod 2 = 1 \\ y_2 \bmod 3 = 1 \\ y_2 \bmod 5 = -1 = 4 \end{cases}$$
jest $y_2 = 19$.

3. Liczbą y_3 spełniającą

$$\begin{cases} y_3 \bmod 2 = 1 \\ y_3 \bmod 3 = -1 = 2 \\ y_3 \bmod 5 = 1 \end{cases}$$

jest $y_3 = 11$.

4. Liczbą y_4 spełniającą

$$\begin{cases} y_4 \bmod 2 = 1 \\ y_4 \bmod 3 = -1 = 2 \\ y_4 \bmod 5 = -1 = 4 \end{cases}$$

jest $y_4 = 29$.

A zatem wszystkimi pierwiastkami kwadratowymi z 1 w $\mathbb{Z}_{30}$ są $1, 11, 19$ oraz 29. ♯

Zadanie 6.39. Pokaż, że w $\mathbb{Z}_{105}$ jest osiem pierwiastków kwadratowych z 1.

6.5 Algorytmy mnożenia i potęgowania

Algorytm mnożenia liczb (Algorytm rosyjskich chłopów)

Wejście: dwie liczby naturalne a i b.
Wyjście: iloczyn $a \cdot b$.

1. Podstaw $A := a$; $B := b$.
2. Dopóki $B \neq 0$, wykonuj:
   2.a $A := 2 \cdot A$;
   2.b $K := K$ div 2;
3. Dodaj te wyrazy z kolumny odpowiadającej wartościom A,
   dla których w kolumnie odpowiadającej wartościom B jest liczba nieparzysta.

Przykład 6.40. Zastosuj powyższy algorytm w celu obliczenia $24 \cdot 20$.

Rozwiązanie. Kolejne kroki algorytmu przedstawia poniższa tabela.

A	B
24	20
48	10
<u>96</u>	<u>5</u>
192	2
<u>384</u>	<u>1</u>
768	0

A zatem $24 \cdot 20 = 96 + 384 = 480$. ♯

Zadanie 6.41. Czy w powyższym algorytmie ma znaczenie, że $a > b$? Sprawdź tezę dla $20 \cdot 24$.

Zadanie 6.42. Zastosuj powyższy algorytm w celu obliczenia

a) $36 \cdot 15$,
b) $41 \cdot 21$.

Algorytm mnożenia modulo.

Wejście: liczby naturalne a, b i m.
Wyjście: $a \cdot b \bmod m$.

1. Podstaw $A := a$; $B := b$.
2. Dopóki $B \neq 0$, wykonuj:

   2.a $A := 2 \cdot A \bmod m$;

   2.b $B := B \text{ div } 2$;

3. Dodaj te wyrazy z kolumny odpowiadającej wartościom A, dla których w kolumnie odpowiadającej wartościom B jest liczba nieparzysta.

Przykład 6.43. Zastosuj powyższy algorytm w celu obliczenia $24 \cdot 20 \bmod 7$.

Rozwiązanie. Kolejne kroki algorytmu przedstawia poniższa tabela.

A	B
24	20
6	10
$\underline{5}$	$\underline{5}$
3	2
$\underline{6}$	$\underline{1}$
5	0

Otrzymujemy zatem, że $24 \cdot 20 \bmod 7 = (6 + 5) \bmod 7 = 4$. ♯

Zadanie 6.44. Zastosuj powyższy algorytm w celu obliczenia:

a) $36 \cdot 15 \bmod 7$,
b) $41 \cdot 21 \bmod 5$.

Algorytm szybkiego potęgowania modulo.

Wejście: podstawa a oraz wykładnik k.
Wyjście: $a^k \bmod m$.

1. Podstaw $A := a$; $K := k$.
2. Dopóki $K \neq 0$, wykonuj:

   2.a $A := A^2 \bmod m$;

   2.b $B := B \text{ div } 2$;

3. Wymnóż te wyrazy w kolumnie A, dla których w kolumnie K jest liczba nieparzysta.

Przykład 6.45. Zastosuj powyższy algorytm w celu obliczenia $8^{11} \bmod 21$.

Rozwiązanie. Kolejne kroki algorytmu przedstawia poniższa tabela.

A	K
$\underline{8}$	$\underline{11}$
$\underline{1}$	$\underline{5}$
1	2
$\underline{1}$	$\underline{1}$
1	0

Otrzymujemy zatem, że $8^{11} \bmod 21 = 8 \cdot 1 \cdot 1 \bmod 21 = 8$. ♯

Zadanie 6.46. Zastosuj powyższy algorytm w celu obliczenia:

a) $4^{14} \bmod 15$,
b) $8^{64} \bmod 65$,
c) $12^{64} \bmod 65$,
d) $10^{32} \bmod 33$.

6.6 Funkcja Eulera

Niech n będzie dowolną liczbą dotatnią. *Funkcję Eulera* definiujemy następująco:

$$\phi(n) = |\{1 \leq b < n \ : \ NWD(b,n) = 1\}|,$$

czyli $\phi(n)$ jest to liczba liczba elementów względnie pierwszych z n. Funkcja Eulera ma następujące własności:

1) $\phi(1) = 1$.
2) $\phi(p) = p - 1$, gdzie p jest liczbą pierwszą.
3) $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, gdzie p jest liczbą pierwszą.
4) $\phi(p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_r^{\alpha_r} - p_r^{\alpha_r - 1})$, gdzie p_i jest liczbą pierwszą, $i = 1, \ldots, r$.

Przykład 6.47. Ile jest dodatnich liczb względnie pierwszych z 1200?

Rozwiązanie. Jako że $1200 = 2^4 \cdot 3 \cdot 5^2$, interesują nas liczby dodatnie niepodzielne przez $2, 3$ lub 5 i nie większe od 1200. Z zasady włączania/wyłączania tych liczb jest

$$\begin{aligned} &1200 - (N(2) + N(3) + N(5) - N(2,3) - N(2,5) - N(3,5) + N(2,3,5)) = \\ &= 1200 \cdot (1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2 \cdot 3} + \frac{1}{2 \cdot 5} + \frac{1}{3 \cdot 5} - \frac{1}{2 \cdot 3 \cdot 5}) = \\ &= 1200 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5}) = 320. \end{aligned}$$

Możemy również zastosować tutaj funkcję Eulera:

$$\phi(1200) = \phi(2^4 \cdot 3 \cdot 5^2) = \phi(2^4) \cdot \phi(3) \cdot \phi(5^2) = 8 \cdot 2 \cdot 20 = 320. \ ♯$$

Zadanie 6.48.* Korzystając z rozumowania przeprowadzonego w powyższym zadaniu, wykaż własności (3) i (4).

Twierdzenie 6.49 (Małe Twierdzenie Fermata) *Jeśli* $NWD(a,m)=1$, *to* $a^{\phi(m)}=1 \bmod m$.

Przykład 6.50. Korzystając z funkcji Eulera oblicz 7^{-1} w $\mathbb{Z}_{20}$.

Rozwiązanie. Zauważmy, że z Małego Twierdzenia Fermata wynika następujący wniosek:

$$\textit{Jeśli } NWD(a,m)=1, \textit{ wówczas w } \mathbb{Z}_m \textit{ zachodzi } a^{-1}=a^{\phi(m)-1}.$$

Tym samym otrzymujemy, że

$$\begin{aligned} 7^{-1} &= 7^{\phi(20)-1}=7^{\phi(2^2\cdot 5)-1}=7^{(2^2-2)\cdot(5-1)-1} \\ &= 7^7=7^1\cdot 7^2\cdot(7^2)^2 \equiv_{20} 7\cdot 9\cdot 9^2 \equiv_{20} 7\cdot 9\cdot 1 \equiv_{20} 63 \equiv_{20} 3. \end{aligned}$$ ♯

Zadanie 6.51. Korzystając z funkcji Eulera oblicz 5^{-1} w $\mathbb{Z}_{21}$.

Przykład 6.52. Udowodnij, że 10-a potęga każdej liczby całkowitej jest postaci $11k$ lub $11k+1$.

Rozwiązanie. Jeśli $11|a$, to oczywiście $11|a^{10}$. Załóżmy zatem, że 11 nie dzieli a. Wówczas $NWD(a,11)=1$ i z Małego Twierdzenia Fermata otrzymujemy, że $a^{\phi(11)}=1 \bmod 11$, czyli $a^{10}=1 \bmod 11$, a zatem $a^{10}=11k+1$ dla pewnego k. ♯

Zadanie 6.53. Udowodnij, że kwadrat liczby całkowitej jest zawsze postaci $5k$, $5k+1$ lub $5k-1$.

Zadanie 6.54. Udowodnij, że 9-ta potęga każdej liczby całkowitej jest postaci $19k$ lub $19k+1$ lub $19k-1$.

Zadanie 6.55. Udowodnij, że 20-a potęga każdej liczby całkowitej jest postaci $25k$ lub $25k+1$.

Wskazówka. $a^{20}-1=(a^4-1)(a^{16}+a^{12}+a^8+a^4+1)$.

6.7 Szyfry RSA

Przykład 6.56. Korzystając z algorytmu RSA zaszyfruj wiadomość $x=10$ od Boba do Alicji. Klucz, który upubliczniła Alicja, to $(e,n)=(9,87)$.

Rozwiązanie. W algorytmie RSA klucz do szyfrowania (e,n) jest jawny i funkcja szyfrująca jest następująca:

$$C(x)=x^e \bmod n.$$

Zatem należy wyliczyć $10^9 \bmod 87$. Korzystając z algorytmu szybkiego potęgowania modulo otrzymujemy $C(10)=76$, czyli zaszyfrowana wiadomość, którą Bob prześle Alicji, to 76. ♯

Przykład 6.57. Odszyfruj wiadomość $y=76$, którą otrzymała Alicja. Klucz prywatny Alicji to $(n,d)=(87,25)$.

Rozwiązanie. Funkcja deszyfrująca, której powinna użyć Alicja to

$$D(y)=y^d \bmod n.$$

Zatem musimy wyliczyć $D(76)=76^{25} \bmod 87$. Korzystając z algorytmu szybkiego potęgowania modulo otrzymujemy $D(76)=10$. Stąd wiadomość, która została przesłana Alicji, to 10. ♯

Przykład 6.58. Spróbuj odszyfrować wiadomość $y=29$ przeznaczoną dla Alicji, znając tylko jej klucz publiczny $(e,n)=(9,33)$.

Rozwiązanie. Aby odszyfrować wiadomość, musimy spróbować wyliczyć wartość d. Aby to uczynić, musimy poznać rozkład liczby n na dwa czynniki pierwsze p oraz q. W naszym przypadku zachodzi $n = 33 = 3 \cdot 11$. Zatem $p = 3$ i $q = 11$. (W rzeczywistości liczba n zawiera kilkaset bitów i poznanie jej rozkładu nie jest prostą sprawą). Teraz musimy wyliczyć $\phi(n) = \phi(33) = 2 \cdot 10 = 20$. Liczba d w algorytmie RSA jest liczbą odwrotną do e w $\mathbb{Z}_{\phi(n)}$. Stosując jedną z poznanych metod, wyliczamy $9^{-1} = 9 \bmod 20$. Zatem znamy już klucz prywatny Alicji $(n, d) = (33, 9)$ i wykorzystując funkcję deszyfrującą $D(y) = y^d \bmod n$, wyliczamy $D(29) = 8 \bmod 33$. ♯

Zadanie 6.59. Klucz publiczny Alicji to $(e, n) = (11, 85)$ ($p = 5$, $q = 17$).

a) Zaszyfruj wiadomość 6.
b) Zaszyfruj wiadomość 23.
c) Odszyfruj wiadomość 22.
d) Odszyfruj wiadomość 29.

6.8 Test Fermata

Algorytm testu pierwszości (test Fermata).

1. Losuj liczbę $2 \leq a < n$, $d := NWD(a, n)$.
2. Jeśli $d > 1$, to *liczba n nie jest pierwsza*; Stop.
3. Jeśli $d = 1$, to niech $p := a^{n-1} \pmod n$.

   3.a Jeżeli $p \neq 1$, to *liczba n nie jest pierwsza*; Stop.

   3.b Jeżeli $p = 1$, to *liczba n jest prawdopodobnie pierwsza*; Stop.

Przykład 6.60. Zastosuj powyższy test dla $n = 21$ oraz:

a) $a = 2$;
b) $a = 8$.

Rozwiązanie.

a) Jako że $NWD(2, 21) = 1$, korzystając np. z algorytmu szybkiego potęgowania, obliczamy $p = 2^{20} \bmod 21$, otrzymując $p = 4$. A zatem algorytm zwróci odpowiedź «*liczba* 21 *nie jest pierwsza*».

b) Natomiast w przypadku, gdy $a = 8$, otrzymamy $NWD(8, 21) = 1$ oraz $p = 8^{20} \bmod 21 = 1$. Zatem algorytm zwróci odpowiedź: *liczba* 21 *jest prawdopodobnie pierwsza*. ♯

Zadanie 6.61. Zastosuj test Fermata dla liczb:

a) $a = 5$ oraz $n = 39$,
b) $a = 12$ oraz $n = 65$.
c) $a = 17$ oraz $n = 561$.

6.9 Zadania dodatkowe

Przykład 6.62. Udowodnij, że liczba $\sqrt{2}$ jest niewymierna.

Rozwiązanie. Załóżmy, że liczba $\sqrt{2}$ jest wymierna, a zatem może być zapisana jako $\frac{a}{b}$. Z równości $\sqrt{2} = \frac{a}{b}$ otrzymujemy, że $2b^2 = a^2$. Rozważmy teraz faktoryzację obudwu stron, a w szczególności liczbę wystąpień dwójki. Załóżmy, że w rozkładzie b dwójka występuje m razy, a w rozkładzie a – odpowiednio n razy. Wówczas 2 występuje $2m+1$ razy w rozkładzie $2b^2$ i $2n$ razy w rozkładzie a^2. Tym samym, $2m+1 = 2n$. Ale że jest to niemożliwe dla dowolnych liczb naturalnych m i n, otrzymujemy sprzeczność. ♯

Zadanie 6.63.* Udowodnij, że liczba $\sqrt{p}$, gdzie p jest liczbą pierwszą, jest niewymierna. Udowodnij fakt bardziej ogólny: liczba $\sqrt{n}$, gdzie n jest dowolną liczbą naturalną nie będącą kwadratem żadnej innej liczby, jest liczbą niewymierną.

Zadanie 6.64.* Analogicznie do zadania powyżej, sformułuj i udowodnij twierdzenie o niewymierności odpowiednich liczb postaci $\sqrt[k]{n}$.

Zadanie 6.65.* Wykaż, że wśród dowolnych n liczb ze zbioru $\{1, 2, \ldots, 2n-1\}$ znajdą się dwie względnie pierwsze.

Zadanie 6.66.* Udowodnij, że istnieje nieskończenie wiele liczb pierwszych.

Wskazówka. Rozważyć liczbę liczbę $n! + 1$ i dowolny jej dzielnik p będący liczbą pierwszą.

Zadanie 6.67.* Udowodnij, że dla dowolnej liczby dodatniej k istnieje ciąg k kolejnych liczb złożonych.

Wskazówka. Rozważyć ciąg liczb $(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + (k+1)$.

Zadanie 6.68.* Niech n będzie liczbą naturalną. Policzmy $\phi(d)$ dla każdego z dzielników n oraz zsumujmy wszystkie uzyskane wartości. Czym jest ta suma? Sformułuj wniosek i go udowodnij.

Zadanie 6.69.* Dla danego n rozważmy sumę $\sum_{NWD(d,n)=1} d$. Czym jest ta suma? Sformułuj wniosek i go udowodnij.

Twierdzenie 6.70 (The Prime Number Theorem)
Niech $\pi(n)$ oznacza liczbę liczb pierwszych pomiędzy $1, 2, \ldots, n$. Wówczas $\pi(n) \simeq \frac{n}{\ln n}$.

Przykład 6.71. Ile jest 200-cyfrowych liczb pierwszych?

Rozwiązanie. Z powyższego twierdzenia wynika, że liczb pierwszych co najwyżej 200-cyfrowych jest około $\frac{10^{200}}{200 \ln 10}$, a liczb pierwszych co najwyżej 199-cyfrowych jest $\frac{10^{199}}{199 \ln 10}$. Otrzymujemy zatem, że liczb pierwszych 200-cyfrowych jest około

$$\frac{10^{200}}{200 \ln 10} - \frac{10^{199}}{199 \ln 10} \simeq 1.95 \cdot 10^{197}.$$

Zauważmy, że liczba dowolnych liczb 200-cyfrowych wynosi $10^{200} - 10^{199} = 9 \cdot 10^{199}$, czyli 200-cyfrowych liczb pierwszych jest dużo. ♯

Algorytm testu pierwszości (test Millera-Rabina).

1. Sprawdzamy, czy n jest potęgą jakiejś liczby naturalnej.
   Jeśli *jest*, to *liczba n nie jest pierwsza*; STOP.
2. Losujemy liczbę $2 \leq a < n$ i sprawdzamy:
   jeśli $d = NWD(a, n) > 1$, to *liczba n nie jest pierwsza*; STOP.
3. Znajdujemy liczby m i k takie, że $n - 1 = m \cdot 2^k$, gdzie m jest nieparzyste.
4. Obliczamy $p = a^m \bmod n$.

   4.a Jeśli $p = 1$, to *liczba n jest pierwsza*; STOP.

   4.b Obliczamy po kolei:

   $$a^{2m} \bmod n, \quad a^{2^2 m} \bmod n, \quad \ldots, \quad a^{2^k m} \bmod n.$$

   4.c Jeśli żadna z tych liczb nie jest równa 1, to *n nie jest pierwsza*; STOP.

   4.d Załóżmy, że $a^{2^i m} \bmod n = 1$. Rozważmy $p' = a^{2^{i-1} m} \bmod n$.

      4.d.1 Jeśli $p' \neq -1$, to *liczba n nie jest pierwsza*; STOP.

      4.d.2 W przeciwnym wypadku — *liczba n jest pierwsza*.

PRZYKŁAD 6.72. Zastosuj powyższy test dla $n = 21$ oraz $a = 8$.

Rozwiązanie. Sprawdzamy, czy 21 nie jest potęgą żadnej liczby — nie jest. Otrzymujemy następnie $NWD(8, 21) = 1$, a zatem przechodzimy do kroku 3.: dla $a = 8$ i $n = 21$ wyznaczone m i k są równe odpowiednio 5 i 2. Wyznaczamy teraz $p = 8^5 \bmod 21 = 8$, a następnie wyliczamy po kolei:

$8^{2 \cdot 5} \bmod 21 = 1$,
$8^{2^2 \cdot 5} \bmod 21 = 1$.

Otrzymujemy, że $i = 1$. A że $p' = 8^{2^0 \cdot 5} \bmod 21 = 8^5 \bmod 21 = p = 8 \neq -1$, stąd «*liczba* 21 *nie jest pierwsza*». ♯

ZADANIE 6.73. Zastosuj test Millera-Rabina dla liczb:

a) $a = 5$ oraz $n = 39$,
b) $a = 12$ oraz $n = 65$,
c) $a = 17$ oraz $n = 561$.

Odpowiedzi do zadań

6.2. Resztą z dzielenia s przez a jest r.

6.5. a) 1; b) 1; c) 2; d) 7; e) 3; f) 10; g) 3; h) 1.

6.6. Ostatnią cyfrą liczby 2^{100} jest 6.

6.7.

$[0] = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$,
$[1] = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$,
$[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$,
$[3] = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$,
$[4] = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$,
$[5] = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$.

6.9. a) $x_1 = 7$; b)$x_2 = 1$; c) $x_3 = 3$; d) $x_4 = 5$.

6.10. $5^{-1} = 3$, $6^{-1} = 6$.

6.12. a) 4; b) 150; c) 7.

6.15. a) $d = 4, x = -1, y = 2$; b) $d = 150, x = 2, y = -1$.

6.17. Elementy odwrotne: $3^{-1} = 3$, $5^{-1} = 5$, $7^{-1} = 7$.

6.18. $11^{-1} = 7$.

6.19. $x_1 = 3, x_2 = 6$.

6.20. $x_1 = 13$, $x_2 = 8$.

6.21. $x = -7$, $y = 3$.

6.24. QZVGBM.

6.26. a) LOW, b) GXPG.

6.28. $x = 2$ i $y = 22$, $x = 11$ i $y = 22$, oraz $x = 20$ i $y = 22$.

6.30.

a) $x = 0 \bmod 11$ lub $x = 2 \bmod 11$,
b) $x = 2 \bmod 23$ lub $x = 21 \bmod 23$.

6.31.

a) $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$, $(0,4)$, $(1,5)$, $(2,0)$, $(3,1)$, $(0,2)$, $(1,3)$, $(2,4)$, $(3,5)$.

b) $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$, $(0,3)$, $(1,4)$, $(2,5)$.
c) Wszystkie pary.

6.34. a) $a = 4$; b) $a = 8$; c) $a = 68$.

6.35. Pary postaci $(a_1, (a_1 + d \cdot i) \bmod m_2)$.

6.37. 19.

6.39. Pierwiastki: $1, 29, 34, 41, 64, 71, 76, 104$.

6.44. a) 1; b) 1.

6.46. a) 1; b) 1; c) 1; d) 1.

6.51. 17.

6.59. a) 29; b) 22; c) 23; d) 79.

6.61.

a) $n = 39$ nie jest pierwsza.
b) $n = 65$ jest prawdopodobnie pierwsza.
c) $n = 561$ nie jest pierwsza.

6.73.

a) $n = 39$ nie jest pierwsza.
b) $n = 65$ nie jest pierwsza.
c) $n = 561$ nie jest pierwsza.

Wskazówki dla Prowadzących

6.2. Mamy $b = a \cdot m$, $c = a \cdot q + r$ i $c = b \cdot t + s$. Zatem $s = c - b \cdot t = (a \cdot q + r) - (a \cdot m) \cdot t = (q - m \cdot t) \cdot a + r$. Jako że $0 \leq r < a$, resztą z dzielenia s przez a jest r.

6.6. Należy policzyć $2^{100} \bmod 10$.

6.26.

a) Funkcja deszyfrująca $D(y) = (ax + b) \bmod 26$ spełnia następujący układ równań.

$$\begin{cases} 7a + b = 4 \bmod 26 \\ 2a + b = 19 \bmod 26 \end{cases}.$$

Odejmując stronami otrzymujemy $(-15) \equiv_{26} 11 = 5a \bmod 26$. Zatem $a = 5^{-1} \cdot 11 \bmod 26$. Wyznaczamy element odwrotny do 5 w $\mathbb{Z}_{26}$: $5^{-1} = 21$. Stąd $a = 21 \cdot 11 \bmod 26 = 23$. Ponadto $b = (19 - 2 \cdot 23) \bmod 26 = 19 - 46 \bmod 26 = 25$. Stąd $D(y) = 23y + 25 \bmod 26$, a zatem fragment wiadomości brzmi ...LOW....

b) Funkcję szyfrującą $C(x)$ wyznaczamy albo z odpowiedniego układu równań, albo z faktu, że jest ona funkcją odwrotną do funkcji $D(y)$. Otrzymujemy zatem, że $C(x) = 17x + 17$, a tym samym zaszyfrowana wiadomość to GXPG.

6.28. Odejmując stronami (II−I) otrzymujemy równanie $6x = 12 \bmod 27$. Zauważmy, że zachodzi $NWD(6, 27) = 3$ oraz i $3|12$, a zatem zgodnie z twierdzeniem 6.22 rozważamy równanie

$$2x = 4 \bmod 9.$$

Jako że $2^{-1} = 5$ w $\mathbb{Z}_9$, otrzymujemy

$$x = 2^{-1} \cdot 4 \bmod 9 = 5 \cdot 4 \bmod 9 = 2 \bmod 9.$$

Zauważmy, że jest to rozwiązanie w $\mathbb{Z}_9$, a my szukamy rozwiązań w $\mathbb{Z}_{27}$. Jako że rozwiązaniami równania $2x = 4 \bmod 9$ są dowolne liczby postaci $x = 2+9n$, gdzie $n \in \mathbb{Z}$, rozwiązań równania $6x = 12 \bmod 27$ szukamy właśnie pośród liczb postaci $(2 + 9n) \bmod 27$. W konsekwencji otrzymujemy, że drugim i trzecim rozwiązaniem w $\mathbb{Z}_{27}$, oprócz $x = 4$, jest odpowiednio także $x = 2 + 9 = 11$ oraz $x = 2 + 18 = 20$.

Pozostaje wyznaczyć y np. z pierwszego równania:
– dla $x = 2$ otrzymujemy $y = 1 - 3x \bmod 26 = 1 - 3 \cdot 2 \bmod 27 = 22$;
– dla $x = 11$ otrzymujemy $y = 1 - 3x \bmod 26 = 1 - 3 \cdot 11 \bmod 27 = 22$;
– dla $x = 20$ otrzymujemy $y = 1 - 3x \bmod 26 = 1 - 3 \cdot 20 \bmod 27 = 22$.

A zatem szukanymi rozwiązaniami w $\mathbb{Z}_{26}$ są $x = 2$ i $y = 22$, $x = 11$ i $y = 22$ oraz $x = 20$ i $y = 22$.

6.30.

a) Równanie $x^2 - 2x = 0 \bmod 11$ równoważne jest równaniu $(x - 2)x = 0 \bmod 11$. Zatem rozwiązania są następujące: $x = 2 \bmod 11$ i $x = 0 \bmod 11$.

b) Równanie $x^2 = 4 \bmod 21$ równoważne jest równaniu $(x-2)(x+2) = 0 \bmod 23$. Zatem rozwiązania są następujące: $x = 2 \bmod 23$ i $x = 21 \bmod 23$.

6.31.

a) Wystarczy sprawdzić kolejnych 24 liczb (bo mamy mod 4 oraz mod6). Zatem sprawdzając kolejne liczby np. od 0 do 23 otrzymamy pary: $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$, $(0,4)$, $(1,5)$, $(2,0)$, $(3,1)$, $(0,2)$, $(1,3)$, $(2,4)$ i $(3,5)$.

	4	**6**
...	...	...
0	0	0
1	1	1
2	2	2
3	3	3
4	0	4
5	1	5
6	2	0
7	3	1
8	0	2
9	1	3
10	2	4
11	3	5

	4	**6**
12	0	0
13	1	1
14	2	2
15	3	3
16	0	4
17	1	5
18	2	0
19	3	1
20	0	2
21	1	3
22	2	4
23	3	5
...	...	...

b) Analogicznie — otrzymamy pary: $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$, $(0,3)$, $(1,4)$, $(2,5)$.

c) Analogicznie — otrzymamy wszystkie pary.

6.34.

a)
$M = 3 \cdot 5 = 15$, czyli $M_1 = 15/3 = 5$, zatem $N_1 \cdot 5 = 1 \bmod 3$, stąd $N_1 = 2$.
$M = 3 \cdot 5 = 15$, czyli $M_2 = 15/5 = 3$, zatem $N_2 \cdot 3 = 1 \bmod 5$, stąd $N_2 = 2$.
$a_1 = 1$, $a_2 = 4$, stąd $a = 1 \cdot 5 \cdot 2 + 4 \cdot 3 \cdot 2 = 34 \bmod 15 = 4$.

b)
$M = 3 \cdot 5 = 15$, czyli $M_1 = 15/3 = 5$, zatem $N_1 \cdot 5 = 1 \bmod 3$, stąd $N_1 = 2$.
$M = 3 \cdot 5 = 15$, czyli $M_2 = 15/5 = 3$, zatem $N_2 \cdot 3 = 1 \bmod 5$, stąd $N_2 = 2$.
$a_1 = 2$, $a_2 = 3$, stąd $a = 2 \cdot 5 \cdot 2 + 3 \cdot 3 \cdot 2 = 38 \text{mod} = 8$.

c)
$M = 3 \cdot 5 \cdot 7 = 105$, czyli $M_1 = 105/3 = 35$, zatem $N_1 \cdot 35 = 1 \bmod 3$, stąd $N1 = 2$.
$M = 3 \cdot 5 \cdot 7 = 105$, czyli $M_2 = 105/5 = 21$, zatem $N_2 \cdot 21 = 1 \bmod 5$, stąd $N_2 = 1$.
$M = 3 \cdot 5 \cdot 7 = 105$, czyli $M_3 = 105/7 = 15$, zatem $N_3 \cdot 15 = 1 \bmod 7$, stąd $N_3 = 1$.
$a_1 = 2$, $a_2 = 3$, $a_3 = 5$, stąd $a = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 \bmod 105 = 68$.

6.35. $a_1 = a \bmod m_1$, czyli $a_1 \bmod m_1 = a$, stąd $a = a_1 + m_1 \cdot l_1$. Analogicznie $a = a_2 + m_2 * l_2$. Otrzymujemy zatem, że $a_1 + m_1 \cdot l_1 = a_2 + m_2 \cdot l_2$, czyli $a_2 = a_1 + m_1 \cdot l_1 - m_2 \cdot l_2$. Niech $NWD(m_1, m_2) = d$, wówczas $a_2 = a_1 + d \cdot [(m_1/d) \cdot l_1 - (m_2/d) \cdot l_2]$. Jako że każdy ze składników różnicy w nawiasie jest całkowity, różnica również, stąd $a_2 = a_1 + d \cdot i$, po uwzględnieniu założenia o a_2, dochodzi mod m_2, czyli pary są postaci $(a_1, (a_1 + d \cdot i) \bmod m_2)$.

6.37. Rozważmy poniższe dwa układy kongruencji.

$$\begin{cases} 3 = M \bmod 4 \\ 4 = M \bmod 5 \end{cases} \qquad \begin{cases} 3 = x \bmod 4 \\ 4 = x \bmod 5 \end{cases}$$

Mając na uwadze Chińskie twierdzenie o resztach, zachodzi $(4 \cdot 5)|(M - x)$, a stąd $M - x = k \cdot 4 \cdot 5$, czyli $M = k \cdot 20 + x$. Pozostaje zatem wyznaczyć x. Rozważmy poniższy układ kongruencji.

$$\begin{cases} 3 = x \bmod 4 \\ 4 = x \bmod 5 \end{cases}$$

Zachodzi:

$M = 4 \cdot 5 = 20$, czyli $M_1 = 20/4 = 5$, zatem $N_1 \cdot 5 = 1 \bmod 4$, stąd $N_1 = 1$;
$M = 4 * 5 = 20$, czyli $M_2 = 20/5 = 4$, zatem $N_2 \cdot 4 = 1 \bmod 5$, stąd $N_2 = 4$;
$a_1 = 3$, $a_2 = 4$, stąd $x = 3 \cdot 5 \cdot 1 + 4 \cdot 4 \cdot 4 = 15 + 64 = 79 \equiv_{20} 19$.

Otrzymujemy $x = 19$. Jako że 19 jest jedyną liczbą ze zbioru $\{0, \ldots, 19\}$, która spełnia kongruencję (bo 4 i 5 są względnie pierwsze), zatem reszta wynosi 19.

6.39. Jako że $105 = 3 \cdot 5 \cdot 7$, wszystkie pierwiastki kwadratowe wyznaczyć można z następujących zależności:

1. $y_1 \bmod 3 = 1$, $y_1 \bmod 5 = 1$, $y_1 \bmod 7 = 1$.
2. $y_2 \bmod 3 = 1$, $y_2 \bmod 5 = 1$, $y_2 \bmod 7 = -1$.
3. $y_3 \bmod 3 = 1$, $y_3 \bmod 5 = -1$, $y_3 \bmod 7 = 1$.
4. $y_4 \bmod 3 = 1$, $y_4 \bmod 5 = -1$, $y_4 \bmod 7 = -1$.
5. $y_5 \bmod 3 = 1$, $y_5 \bmod 5 = 1$, $y_5 \bmod 7 = 1$.
6. $y_6 \bmod 3 = 1$, $y_6 \bmod 5 = 1$, $y_6 \bmod 7 = -1$.
7. $y_7 \bmod 3 = 1$, $y_7 \bmod 5 = -1$, $y_7 \bmod 7 = 1$.
8. $y_8 \bmod 3 = 1$, $y_8 \bmod 5 = -1$, $y_8 \bmod 7 = -1$.

Jako że $1 \neq -1 \bmod p$, $p \in \{3, 5, 7\}$, otrzymamy osiem różnych pierwiastków: $1, 76, 64, 34, 71, 41, 29, 104$.

6.48.

(3) Jako że $n = p^\alpha$, interesują nas tylko liczby niepodzielne przez p. Z zasady włączania/wyłączania tych liczb jest

$$p^\alpha - N(p) = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1}.$$

(4) Jeśli $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, to interesują nas liczby niepodzielne przez żadne z p_i, $i = 1, \ldots, r$. Z zasady włączania/wyłączania tych liczb jest

$$n - ((N(p_1) + \ldots + N(p_r)) - (N(p_1, p_2) + \ldots + N(p_{r-1}, p_r)) + (-1)^r N(p_1, \ldots, p_r)) =$$
$$= n - \Big(1 - (\frac{1}{p_1} + \ldots + \frac{1}{p_r}) + (\frac{1}{p_1 \cdot p_2} + \ldots + \frac{1}{p_{r-1} \cdot p_r}) + (-1)^r \frac{1}{p_1 \cdot \ldots \cdot p_r}\Big) =$$
$$= n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_r}) =$$
$$= p_1^{\alpha_1} \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot p_r^{\alpha_r} \cdot (1 - \frac{1}{p_r}) =$$
$$= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_r^{\alpha_r} - p_r^{\alpha_r - 1}).$$

Zadanie 6.74. 51 Jako że $a = 5$ oraz $m = 21 = 3 \cdot 7$, otrzymujemy $\phi(21) = (3-1) \cdot (7-1) = 12$ oraz $NWD(5, 21) = 1$. Zatem z Małego Twierdzenia Fermata otrzymujemy, że

$$\begin{aligned} 5^{-1} &= 5^{\phi(21)-1} = 5^{\phi((3-1)\cdot(7-1))-1} = 5^{11} \\ &= 5^1 \cdot 5^2 \cdot ((5^2)^2)^2 \equiv_{21} 5 \cdot 4 \cdot (4^2)^2 \equiv_{21} 20 \cdot 16^2 \equiv_{21} (-1) \cdot (-5)^2 \equiv_{21} -4 \equiv_{21} 17. \end{aligned}$$

6.53. Jeśli $5|a$, to oczywiście $5|a^2$. Załóżmy zatem, że 5 nie dzieli a. Wówczas $NWD(a, 5) = 1$ i z Małego Twierdzenia Fermata otrzymujemy, że $a^{\phi(5)} = 1 \bmod 5$, czyli $a^4 = 1 \bmod 5$. A zatem $5|(a^4 - 1)$, czyli $5|(a^2 - 1) \cdot (a^2 + 1)$. Jako że 5 jest liczbą pierwszą, więc albo $5|(a^2 - 1)$ albo $5|(a^2 + 1)$. Stąd $a = 5k + 1$ lub $a = 5k - 1$ dla pewnego k.

6.54. Jeśli $19|a$, to oczywiście $19|a^9$. Załóżmy zatem, że 19 nie dzieli a. Wówczas $NWD(a, 19) = 1$, a z Małego Twierdzenia Fermata, $a^{\phi(19)} = 1 \bmod 19$, czyli $a^{18} = 1 \bmod 19$. A zatem $19|(a^{18} - 1)$, czyli $19|(a^9 - 1) \cdot (a^9 + 1)$. Jako że 19 jest liczbą pierwszą, więc albo $19|(a^9 - 1)$ albo $19|(a^9 + 1)$. Stąd $a = 19k + 1$ lub $a = 19k - 1$ dla pewnego k.

6.55. Jeśli $5|a$, to oczywiście $5^2|a^2$ i wówczas $25|a^{20}$. Załóżmy zatem, że 5 nie dzieli a. Wówczas $NWD(a, 5) = 1$, a z Małego Twierdzenia Fermata, $a^{\phi(5)} = 1 \bmod 5$, czyli $a^4 = 1 \bmod 5$, a stąd $a^{4n} = 1 \bmod 5$) dla dowolnego n.

Skorzystajmy teraz ze wskazówki. Skoro $a^{20} - 1 = (a^4 - 1) \cdot (a^{16} + a^{12} + a^8 + a^4 + 1)$ i z poprzednich rozważań mamy, że zarówno $(a^4 - 1) = 0 \bmod 5$, jak i $(a^{16} + a^{12} + a^8 + a^4 + 1) = 0 \bmod 5$, zatem $(a^{20} - 1) = 0 \bmod 25$. Stąd $a^{20} = 1 \bmod 25$, czyli $a = 25k + 1$ dla pewnego k.

6.61.

a) $d = NWD(5, 39) = 1$, zatem musimy obliczyć p równe $5^{38} \bmod 39$. Korzystając np. z algorytmu szybkiego potęgowania otrzymamy, że $p = 25$. Zatem algorytm zwróci odpowiedź «*liczba* 39 *nie jest pierwsza*».

b) $d = NWD(12, 65) = 1$, $p = 12^{64} \bmod 65 = 1$, zatem algorytm zwróci odpowiedź «*liczba* 65 *jest prawdopodobnie pierwsza*».

c) $d = NWD(17, 561) = 17$, zatem algorytm zwróci odpowiedź «*liczba* 561 *nie jest pierwsza*».

6.63. Załóżmy, że liczba $\sqrt{p}$ jest wymierna, a zatem może być zapisana jako $\frac{a}{b}$. Z równości $\sqrt{p} = \frac{a}{b}$ otrzymujemy, że $pb^2 = a^2$. Rozważmy teraz faktoryzację obudwu stron, a w szczególności liczbę wystąpień liczby p. Załóżmy, że w rozkładzie b liczba **pierwsza** p występuje m razy, a w rozkładzie a – odpowiednio n razy. Wówczas p występuje $2m+1$ razy w rozkładzie pb^2 i $2n$ razy w rozkładzie a^2. Tym samym, $2m+1 = 2n$. Ale że jest to niemożliwe dla dowolnych liczb naturalnych m i n, otrzymujemy sprzeczność: liczba $\sqrt{p}$ nie jest wymierna.

W ogólnym przypadku, jeśli n jest liczbą złożoną nie będącą potęgą innej liczby naturalnej, wówczas w rozkładzie n istnieje liczba pierwsza p, która występuje nieparzystą liczbę razy. Z równości $\sqrt{n} = \frac{a}{b}$ wynika, że $nb^2 = a^2$. Rozważmy teraz faktoryzację obudwu stron, a w szczególności liczbę wystąpień liczby p. Załóżmy, że w rozkładzie b liczba **pierwsza** p występuje m razy, a w rozkładzie a – odpowiednio n razy. Wówczas p występuje $2m+k$ razy w rozkładzie nb^2, gdzie k jest liczbą nieparzystą, i $2n$ razy w rozkładzie a^2. Tym samym, $2m+k = 2n$. Ale że jest to niemożliwe dla dowolnych liczb naturalnych m i n (k nieparzyste), otrzymujemy sprzeczność: liczba $\sqrt{n}$ nie jest wymierna.

6.64. Niech n będzie liczbą naturalną nie będącą k-tą potęgą innej liczby naturalnej. Załóżmy, że $\sqrt[k]{n}$ jest wymierna. Wówczas, niezależnie od tego, czy n jest liczbą złożoną czy pierwszą, z założenia o niebyciu k-ta potęgą innej liczby naturalnej wynika, że w rozkładzie n istnieje liczba pierwsza p, która występuje t razy oraz $k \not| t$. Z równości $\sqrt[k]{n} = \frac{a}{b}$ mamy, że $nb^k = a^k$, a zatem liczba wystąpień p w rozkładzie lewej strony nie będzie podzielna przez k, w przeciwieństwie do liczby wystąpień po prawej stronie. Otrzymujemy sprzeczność.

6.65. Rozważmy szufladki $\{1\}, \{2,3\}, \{4,5\}, \ldots, \{2n-2, 2n-1\}$. Wówczas albo spośród n liczb znajdą się dwie, które będą w tej samej szufladce $\{i, i+1\}$, co oznacza, że są względnie pierwsze, albo też jedna z nich równa jest 1 i jest ona względnie pierwsza z każdą inną.

6.66. Wystarczy pokazać, że dla dowolnej liczby naturalnej n istnieje liczba pierwsza p większa od n. Rozważmy zatem liczbę $n!+1$ i dowolny jej dzielnik $p \neq 1$ będący liczbą pierwszą. Załóżmy, że $p \leq n$. Wówczas z definicji $n!$ mamy, że $p \mid n!$. Ale to prowadzi do wniosku, że p dzieli różnicę $(n!+1) - n! = 1$. Sprzeczność, zatem $p > n$.

6.67. Niech $n = k+1$ i rozważmy ciąg $n!+2, n!+3, \ldots, n!+n$. Czy możliwe jest, aby któraś z tych liczb była pierwsza? Otóż nie. Po pierwsze, pierwsza liczba jest parzysta, ponieważ $n!$ i 2 są parzyste. Druga liczba jest podzielna przez 3 ($n > 2$), itd. W ogólności, $n! + i$ jest podzielne przez i, $i = 2, 3, \ldots, n$. Zatem liczby te nie są pierwsze i jest ich dokładnie $n - 1 = k$.

6.68. Sprawdzenie dla paru liczb prowadzi do przypuszczenia, że sumą jest n. Aby to udowodnić, rozważmy ułamki postaci $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$ i uprośćmy je najbardziej jak to możliwe. Najpierw zauważmy, że mianowniki w rozważanych nieskracalnych ułamkach są wyłącznie podzielnikami n. Rozważmy zatem dowolny z otrzymanych nieskracalnych ułamków – jest on postaci $\frac{a}{d}$, gdzie d jest dzielnikiem n, a $1 \leq a \leq d$ i $NWD(a,d) = 1$, jako że ułamek jest nieskracalny (oznaczmy te własności a przez $(*)$).

- Ile w danym ciągu jest nieskracalnych ułamków z tym samym mianownikiem d? Otóż co najwyżej $\phi(d)$ – tyle ile jest liczb względnie pierwszych z d.

- Pytanie, czy dla dowolnego $\frac{a}{d}$ spełniającego $(*)$ w pierwotnym ciągu ułamków występuje skracalny do niego? Niech $n = k \cdot d$ i niech a spełnia $(*)$. Wówczas ułamek $\frac{ka}{kd} = \frac{ka}{n} \leq 1$ występuje w naszym ciągu.

Tym samym istnieje wzajemna jednoznaczność pomiędzy wszystkimi możliwymi ułamkami postaci $\frac{a}{d}$ spełniającymi $(*)$ a nieskracalnymi ułamkami powstałymi z pierwotnego ciągu. Jako że liczba wszystkich ułamków wynosiła n, teza zachodzi.

6.69. Sprawdzamy dla kilku liczb, np. dla $n = 1$ oraz $n = 2$ suma wynosi 1, ... Załóżmy, że $n > 2$. Jeśli k jest względnie pierwsze z n, wówczas $n-k$ także: suma tych liczb daje n. Zauważmy, że $k \neq n/2$. Jako że jest $\phi(n)/2$ takich par, rozważana suma wynosi $\frac{n \cdot \phi(n)}{2}$.

6.73.

a) 39 nie jest potęgą żadnej liczby naturalnej oraz $NWD(5, 39) = 1$. Zatem dla $a = 5$ i $n = 39$ wyznaczone m i k są równe odpowiednio 19 i 1. Następnie, $p = 5^{19} \bmod 39 = 8$, a zatem wyliczmy:

$5^{2 \cdot 19} \bmod 39 = 25 \neq 1.$

Stąd «39 *nie jest pierwsza*».

b) 65 nie jest potęgą żadnej liczby naturalnej oraz $NWD(12, 65) = 1$. Zatem dla $a = 12$ i $n = 65$ wyznaczone m i k są równe odpowiednio 1 i 6. Następnie, $p = 12^1 \bmod 65 = 12$, a zatem wyliczmy kolejno:

$12^2 \bmod 65 = 14 \text{mod} \neq 1.$
$12^4 \bmod 65 = 1.$
...

Otrzymujemy, że $i = 2$. A że $p' = 12^{2^1} \bmod 65 = 14 \neq -1$, stąd «65 *nie jest pierwsza*».

c) 561 nie jest potęgą żadnej liczby naturalnej oraz $NWD(17, 561) = 17$, a zatem «561 *nie jest pierwsza*».

Zestaw zadań nr 7

Stosy, kolejki, drzewa

Operacje na stosie.
→ Dodanie elementu na wierzch stosu.
→ Zdjęcie elementu z wierzchu stosu.
→ Sprawdzenie, czy stos jest pusty.

Operacje na kolejce.
→ Dodanie elementu na koniec kolejki.
→ Usunięcie elementu z początku kolejki.
→ Sprawdzenie, czy kolejka jest pusta.

Drzewa. *Drzewo* posiada wierzchołek wyróżniony zwany *korzeniem*. Ponadto dowolny wierzchołek może mieć *dziecko/syna* (relacja *ojciec-syn*), ale – za wyjątkiem korzenia – dowolny wierzchołek jest synem dokładnie jednego innego wierzchołka. Wierzchołki nie posiadające synów zwane są *liśćmi*. *Wysokość/głębokość drzewa* to długość najdłuższej ścieżki od korzenia do liścia. Zauważmy, że przy tak określonej definicji, dla każdego elementu w drzewie istnieje dokładnie jedna ścieżka prowadząca od korzenia do tego wierzchołka.

Drzewa binarne. W *drzewie binarnym* każdy wierzchołek ma co najwyżej dwóch synów. Wierzchołki można etykietować ciągami złożonymi z 0 i 1. Wówczas korzeń drzewa oznaczony jest przez λ, natomiast jeśli jakiś wierzchołek oznaczony jest przez x, to jego lewego syna etykietujemy $x0$, prawego $x1$. Przy takim etykietowaniu wierzchołków kolejne bity wierzchołka wyznaczają ścieżkę od korzenia do tegoż wierzchołka: 0 – w lewego syna, 1 – w prawego syna.

7.1 Algorytmy przeszukiwania drzew

Algorytm przeszukiwania drzewa binarnego w głąb.

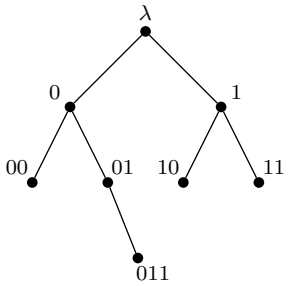
1. Odwiedzamy korzeń, wkładamy go na STOS, i zaznaczamy jako odwiedzony.
2. Dopóki STOS nie jest pusty, powtarzamy:
   2.a. jeżeli v jest wierzchołkiem na wierzchu stosu, to sprawdzamy, czy istnieje syn u wierzchołka v, który nie był jeszcze odwiedzony (najpierw lewy, potem prawy syn);
   2.b. jeżeli u jest takim wierzchołkiem, to odwiedzamy u, wkładamy go na STOS i zaznaczamy jako odwiedzony;
   2.c. jeżeli takiego u nie ma, to zdejmujemy v ze stosu.

Uwaga. Zauważmy, że w dowolnym kroku wierzchołki na STOSIE tworzą ścieżkę od korzenia do wierzchołka aktualnie odwiedzanego.

Algorytm przeszukiwania drzewa binarnego wszerz.

1. Odwiedzamy korzeń, wstawiamy go do KOLEJKI i zaznaczamy jako odwiedzony.
2. Dopóki KOLEJKA nie jest pusta, powtarzamy:
   2.a bierzemy wierzchołek v z początku KOLEJKI;
   2.b wstawiamy wszystkich synów v na koniec KOLEJKI i zaznaczamy je jako odwiedzone.

Przykład 7.1. Przeszukaj metodą „w głąb" i „wszerz" poniższe drzewo binarne.



Rozwiązanie.

w głąb

etykieta	stos
λ	λ
0	$\lambda, 0$
00	$\lambda, 0, 00$
0	$\lambda, 0$
01	$\lambda, 0, 01$
011	$\lambda, 0, 01, 011$
01	$\lambda, 0, 01$
0	$\lambda, 0$
λ	λ
1	$\lambda, 1$
10	$\lambda, 1, 10$
1	$\lambda, 1$
11	$\lambda, 1, 11$
1	$\lambda, 1$
λ	λ
–	–

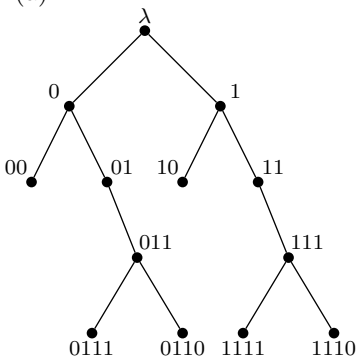
wszerz

etykieta	kolejka
λ	λ
$0, 1$	$0, 1$
$00, 01$	$1, 00, 01$
$10, 11$	$00, 01, 10, 11$
–	$01, 10, 11$
011	$10, 11, 011$
–	$11, 011$
–	011
–	–

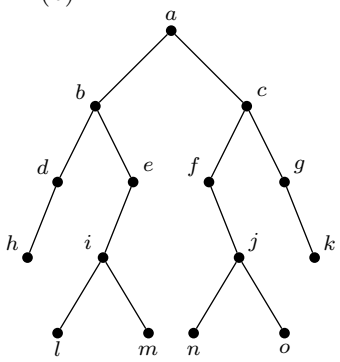
♯

Zadanie 7.2. Przeszukaj metodą „w głąb" i „wszerz" poniższe drzewa.

(a)



(b)



Przeszukiwanie drzewa w kolejności postorder.

Aby przeszukać (pod)drzewo mające swój korzeń w wierzchołku x:
1. Przeszukujemy jego lewe poddrzewo (z korzeniem w $x0$).
2. Przeszukujemy jego prawe poddrzewo (z korzeniem w $x1$).
3. Odwiedzamy wierzchołek x (korzeń drzewa).

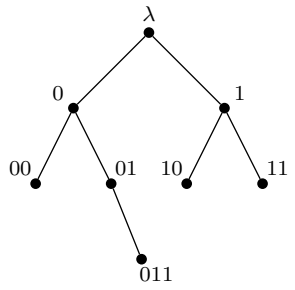
Przeszukiwanie drzewa w kolejności inorder.

Aby przeszukać (pod)drzewo mające swój korzeń w wierzchołku x:
1. Przeszukujemy jego lewe poddrzewo (z korzeniem w $x0$).
2. Odwiedzamy wierzchołek x (korzeń drzewa).
3. Przeszukujemy jego prawe poddrzewo (z korzeniem w $x1$).

Przeszukiwanie drzewa w kolejności preorder.

Aby przeszukać (pod)drzewo mające swój korzeń w wierzchołku x:
1. Odwiedzamy wierzchołek x (korzeń drzewa).
2. Przeszukujemy jego lewe poddrzewo (z korzeniem w $x0$).
3. Przeszukujemy jego prawe poddrzewo (z korzeniem w $x1$).

Przykład 7.3. Wypisz etykiety kolejno przeszukiwanych wierzchołków przy przeszukiwaniu rekurencyjnymi metodami postorder, inorder i preorder podanego obok drzewa binarnego.



Rozwiązanie. Etykiety kolejno przeszukiwanych wierzchołków są następujące:
- postorder: $00, 011, 01, 0, 10, 11, 1, \lambda$;
- inorder: $00, 0, 01, 011, \lambda, 10, 1, 11$;
- preorder: $\lambda, 0, 00, 01, 011, 1, 10, 11$. ♯

Zadanie 7.4. Wypisz etykiety kolejno przeszukiwanych wierzchołków przy przeszukiwaniu rekurencyjnymi metodami postorder, inorder i preorder drzew z zadania 7.2.

7.2 Drzewa wyrażeń arytmetycznych

Przykładem zastosowań drzew binarnych są *drzewa wyrażeń arytmetycznych*. W takim drzewie liście etykietowane są stałymi albo zmiennymi. Pozostałe wierzchołki etykietowane są operacjami arytmetycznymi. Każdemu wierzchołkowi w drzewie możemy przypisać wyrażenie arytmetyczne według zasady:

→ dla liści wyrażeniami są etykiety tych liści (stałe lub zmienne);

→ jeżeli wierzchołek x ma etykietę *op*, a jego synom $x0$ i $x1$ przypisano odpowiednio wyrażenia $W(x0)$ i $W(x1)$, to wierzchołkowi x przypisujemy wyrażenie $W(x) = W(x0)\ op\ W(x1)$.

Postacie wyrażeń arytmetycznych (postać pre- jak i postfixowa nie wymagają nawiasowania):

→ notacja infixowa: $((2 \cdot a) + (3/d))$;

→ notacja prefixowa: $+ \cdot\ a\ 2\ /\ 3\ d$;

→ notacja postfixowa: $2\ a\ \cdot\ 3\ d\ /\ +$.

Mając drzewo wyrażenia arytmetycznego, aby otrzymać postać postfixową/infixową/prefixową

tego wyrażenia, należy przeszukać to drzewo odpowiednio metodą postorder/inorder/preorder i wypisać po kolei etykiety odwiedzanych wierzchołków. Przy czym w celu otrzymania postaci infixowej, przy przeszukiwaniu inorder za każdym pójściem w lewo wstawiamy nawias otwierający, przy powrocie z prawej i wyjściu z wierzchołka nawias zamykający.

Algorytm obliczania wartości wyrażenia w postaci postfixowej.

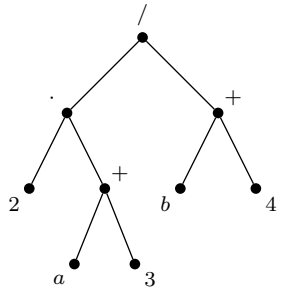
Dla kolejnych elementów zapisu wyrażania powtarzamy:

1. Jeżeli element jest stałą albo zmienną, to wkładamy jego wartość na stos.
2. Jeżeli element jest znakiem operacji, to zdejmujemy dwie wartości ze stosu, wykonujemy operację na tych wartościach, a następnie obliczoną wartość wkładamy na wierzch stosu.
3. Po przejściu całego wyrażenia, jego wartość znajduje się na stosie.

Przykład 7.5.

a) Narysuj drzewo dla wyrażenia $((2 \cdot (a+3))/(b+4))$.
b) Przedstaw to wyrażenie w postaci prefixowej i postfixowej.
c) Następnie oblicz wartość tego wyrażenia dla postaci postfixowej przy $a = 2$ oraz $b = 1$.

Rozwiązanie. (a) Analizując nawiasowanie otrzymamy następujące drzewo wyrażenia.



(b) Szukane postacie prefixowa i postfixowa otrzymywane są przez wypisanie etykiet wierzchołków przy przeszukiwaniu drzewa w kolejności preorder i odpowiednio metodą postorder.

- Postać prefixowa: $/ \cdot 2 + a\ 3 + b\ 4$.
- Postać postfixowa: $2\ a\ 3 + \cdot b\ 4 + /$.

(c) Zgodnie z algorytmem obliczania wartości wyrażenia w postaci postfixowej dla kolejnych elementów wyrażenia $2\ 2\ 3\ +\ \cdot\ 1\ 4\ +\ /$ powtarzamy:

	stos
2	2
2	2, 2
3	2, 2, 3
+	2, 5
·	10
1	10, 1
4	10, 1, 4
+	10, 5
/	2.

Wartość wyrażenia dla $a + 2$ i $b = 1$ wynosi 2. ♯

Zadanie 7.6. Dla wyrażeń (a) $2\ 3\ +\ 5\ /\ 7\ \cdot\ 3\ 1\ -\ \cdot$ oraz (b) $1\ 3\ +\ 5\ 8\ 7\ -\ -\ /$ oblicz ich wartość, narysuj odpowiednie drzewa oraz przedstaw te wyrażenia w postaci infixowej i prefixowej.

7.3 Drzewa przeszukiwań binarnych

Niech $W(x)$ oznacza wartość przechowywaną w korzeniu o etykiecie x drzewa T_x.

Algorytm wstawiania elementu do drzewa przeszukiwań binarnych.

Niech y będzie wstawianym elementem do drzewa T_x.

1. Jeśli drzewo T_x jest puste, to $W(x) := y$ (węzeł z wartością y staje się korzeniem drzewa T_x).
2. W przeciwnym razie porównaj zawartość y z zawartością korzenia drzewa T_x:
   2.a. jeśli $y < W(x)$, to wstaw y do lewego poddrzewa T_{x0} drzewa T_x;
   2.b. jeśli $y > W(x)$, to wstaw y do prawego poddrzewa T_{x1} drzewa T_x.

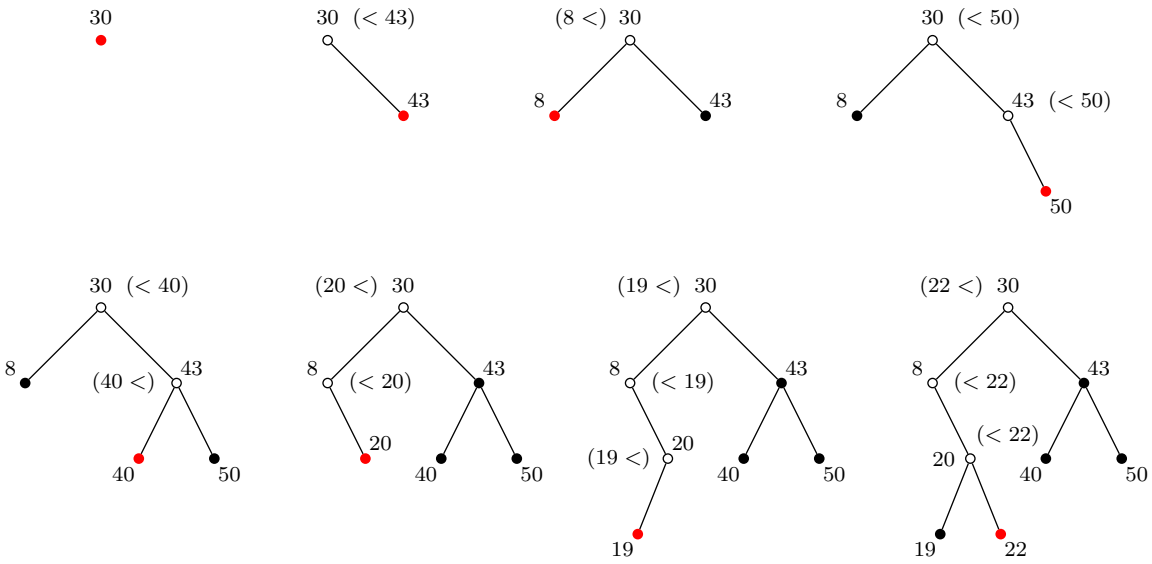
Algorytm szukania elementu w drzewie przeszukiwań binarnych.

Niech y będzie szukanym elementem w drzewie T_x.

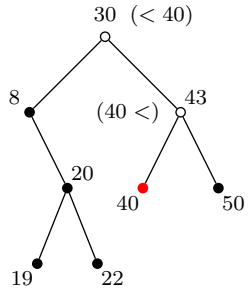
1. Jeśli drzewo T_x jest puste, to rozważanego elementu nie ma na drzewie.
2. W przeciwnym razie porównaj wartość y z wartością w korzeniu x drzewa T_x:
   2.a. jeśli $y = W(x)$, to w drzewie znaleźliśmy element y;
   2.b. jeśli $y < W(x)$, to szukaj y w lewym poddrzewie T_{x0};
   2.c. jeśli $y > W(x)$, to szukaj y w prawym poddrzewie T_{x1}

Przykład 7.7. Narysuj drzewo poszukiwań binarnych powstałe przy wstawianiu kolejnych liczb $30, 43, 8, 50, 40, 20, 19, 22$, a następnie przeszukaj to drzewo w celu sprawdzenia, czy elementy 40 i 18 należą do rozważanego drzewa.

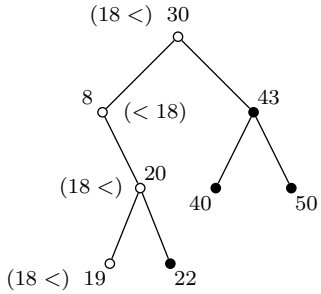
Rozwiązanie. Kolejne etapy powstawania drzewa są następujące (węzły białe to węzły odwiedzane przez algorytm, a węzeł czerwony to wstawiony węzeł).



Jeśli chodzi o wyszukanie elementów 40 oraz 18, to wykonanie algorytmu przedstawione jest na poniższych rysunkach; białe węzły są węzłami odwiedzanymi przez algorytm, a czerwony węzeł jest węzłem z szukaną wartością (o ile węzeł taki istnieje).



istnieje węzeł o wartości 40



brak węzła o wartości 18 ♯

Zadanie 7.8. Narysuj drzewo poszukiwań binarnych powstałe przy wstawianiu kolejnych liczb $15, 20, 23, 16, 13, 9, 14, 4, 1$, a następnie przeszukaj to drzewo w celu sprawdzenia, czy elementy 40 i 4 należą do rozważanego drzewa.

Zadanie 7.9. Narysuj drzewo poszukiwań binarnych powstałe przy wstawianiu kolejnych wyrazów *słowik, wróbel, kos, jaskółka, kogut, dzięcioł, gil, kukułka, szczygieł, sowa, kruk, czubatka*, a następnie wypisz kolejno przeszukiwane wierzchołki przy przeszukiwaniu rekurencyjną metodą inorder.

Odpowiedzi do zadań

7.2. Przeszukanie w głąb.

a)

etykieta	stos
λ	λ
0	$\lambda, 0$
00	$\lambda, 0, 00$
0	$\lambda, 0$
01	$\lambda, 0, 01$
011	$\lambda, 0, 01, 011$
0110	$\lambda, 0, 01, 011, 0110$
011	$\lambda, 0, 01, 011$
0111	$\lambda, 0, 01, 011, 0111$
011	$\lambda, 0, 01, 011$
01	$\lambda, 0, 01$
0	$\lambda, 0$
λ	λ
1	$\lambda, 1$
11	$\lambda, 1, 11$
111	$\lambda, 1, 11, 111$
1110	$\lambda, 1, 11, 111, 1110$
111	$\lambda, 1, 11, 111$
1111	$\lambda, 1, 11, 111, 1111$
111	$\lambda, 1, 11, 111$
11	$\lambda, 1, 11$
1	$\lambda, 1$
λ	λ
–	–

b)

etykieta	stos
a	a
b	a, b
d	a, b, d
h	a, b, d, h
d	a, b, d
b	a, b
e	a, b, e
i	a, b, e, i
l	a, b, e, i, l
i	a, b, e, i
m	a, b, e, i, m
i	a, b, e, i
e	a, b, e
b	a, b
a	a
c	a, c
f	a, c, f
j	a, c, f, j
n	a, c, f, j, n
j	a, c, f, j
o	a, c, f, j, o
j	a, c, f, j
f	a, c, f
c	a, c
a	a
–	–

Przeszukanie wszerz.

a)

etykieta	kolejka
λ	λ
$0, 1$	$0, 1$
$00, 01$	$1, 00, 01$
$10, 11$	$00, 01, 10, 11$
–	$01, 10, 11$
011	$10, 11, 011$
–	$11, 011$
111	$011, 111$
$0110, 0111$	$111, 0110, 0111$
$1110, 1111$	$0110, 0111, 1110, 1111$
–	$0111, 1110, 1111$
–	$1110, 1111$
–	1111
–	–

b)

etykieta	kolejka
a	a
b, c	b, c
d, e	c, d, e
f, g	d, e, f, g
h	e, f, g, h
i	f, g, h, i
j	g, h, i, j
k	h, i, j, k
–	i, j, k
l, m	j, k, l, m
n, o	k, l, m, n, o
–	l, m, n, o
–	m, n, o
–	n, o
–	o
–	–

7.4.

a)

Postorder: $00, 0110, 0111, 011, 01, 0, 10, 1110, 1111, 111, 11, 1, \lambda$.
Inorder: $00, 0, 01, 0110, 011, 0111, \lambda, 10, 1, 11, 1110, 111, 1111$.
Preorder: $\lambda, 0, 00, 01, 011, 0110, 0111, 1, 10, 11, 111, 1101, 1111$.

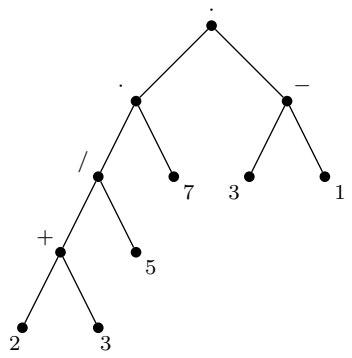
b)

Postorder: $h, d, l, m, i, e, b, n, o, j, f, k, g, c, a$.
Inorder: $h, d, b, l, i, m, e, q, f, n, j, o, c, g, k$.
Preorder: $a, b, d, h, e, i, l, m, c, f, j, n, o, g, k$.

7.6. (a) Zgodnie z algorytmem obliczania wartości wyrażenia 2 3 + 5 / 7 · 3 1 − · w postaci postfixowej dla kolejnych elementów wyrażenia powtarzamy:

	stos
2	2
3	2, 3
+	5
5	5, 5
/	1
7	1, 7
·	7
3	7, 3
1	7, 3, 1
−	7, 2
·	**14**

Otrzymujemy zatem, że wartość wyrażenia wynosi 14. Drzewo wyrażenia otrzymujemy podczas wykownywania algorytmu obliczenia tej wartości.



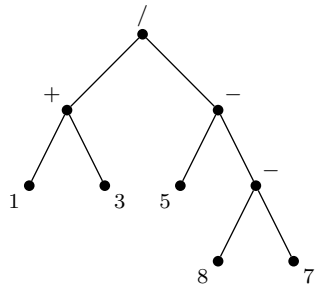
Szukane postacie otrzymywane są przez wypisanie etykiet wierzchołków przy odpowiednim przeszukiwaniu drzewa:

- postać infixowa (przeszukanie inorder): $((((2 + 3)/5) \cdot 7) \cdot (3 - 1))$;
- postać prefixowa (przeszukanie preorder): · · / + 2 3 5 7 − 3 1.

(b) Zgodnie z algorytmem obliczania wartości wyrażenia 1 3 + 5 8 7 − − / w postaci postfixowej dla kolejnych elementów wyrażenia powtarzamy:

	stos
1	1
3	1, 3
+	4
5	4, 5
8	4, 5, 8
7	4, 5, 8, 7
−	4, 5, 1
−	4, 4
/	**1**

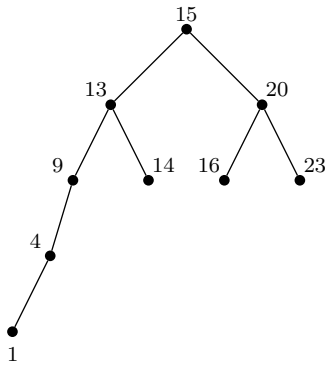
Otrzymujemy zatem, że wartość wyrażenia wynosi 1. Drzewo wyrażenia otrzymujemy podczas wykownywania algorytmu obliczenia tej wartości.



Szukane postacie otrzymywane są przez wypisanie etykiet wierzchołków przy odpowiednim przeszukiwaniu drzewa:

- postać infixowa (przeszukanie inorder): $((1 + 3)/(5 - (8 - 7)))$;
- postać prefixowa (przeszukanie preorder): / + 1 3 − 5 − 8 7.

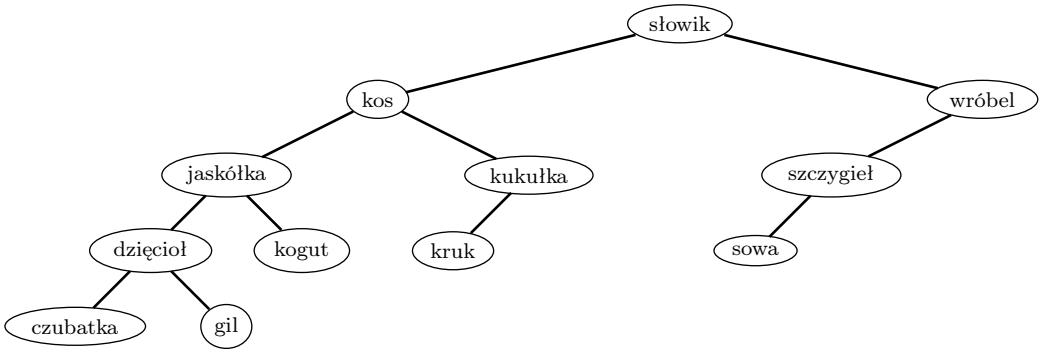
7.8.



Wyszukanie $y = 40$:
$15 \to 20 \to 23 \to$ brak.

Wyszukanie $y = 4$:
$15 \to 13 \to 9 \to 4$.

7.9. Drzewo przeszukiwań binarnych przedstawia się następująco.



Kolejne wartości węzłów w porządku inorder: *czubatka, dzięcioł, gil, jaskółka, kogut, kos, kruk, kukułka, słowik, sowa, szczygieł, wróbel.*

Zestaw zadań nr 8

Rekurencja

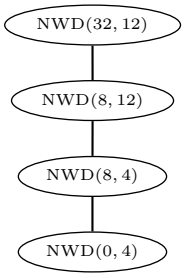
Rekurencja jest to zdolność programu (procedury lub funkcji) do wywoływania samego siebie. Działanie pocedury rekurencyjnej można zilustrować poprzez *drzewo rekursji*, w którym korzeń odpowiada początkowemu wywołaniu procedury, a dla dowolnego wierzchołka x odpowiadającemu pewnemu wywołaniu procedury, jego synowie oznaczają rekurencyjne wywołania w celu wykonania obliczeń dla x.

Przykładem *algorytmu rekurencyjnego* może być rekurencyjna wersja algorytmu Euklidesa, który oblicza największy wspólny dzielnik liczb a i b ($a, b > 0$).

Algorytm (rekurencyjny) Euklidesa NWD(a, b)**.**

1. Jeśli $a \cdot b = 0$, zwróć $a + b$;
2. W przeciwnym przypadku:
   2.a. jeżeli $a \geq b$, zwróć NWD$(a \bmod b, b)$;
   2.b. w przeciwnym przypadku, zwróć NWD$(a, b \bmod a)$.

Zauważmy, że w tym wypadku drzewo rekursji będzie miało zawsze postać ścieżki.



Innym przykładem algorytmu rekurencyjnego może być algorytm sortowania ciągu liczb (znaków). Dla uproszczenia będziemy zakładać, że długość ciągu jest potęgą dwójki.

Algorytm sortowania przez scalanie `merge-sort`(C)**.**

1. Jeśli C ma tylko jeden element, zwróć C.
2. W przeciwnym przypadku:
   2.a. podziel C na połowy C_1 i C_2;
   2.b. `merge-sort`(C_1);
   2.c. `merge-sort`(C_2);
   2.d. połącz C_1 i C_2 w jeden ciąg C^* z zachowaniem kolejności i zwróć C^*.

Uwaga. Krok (2.d) nosi nazwę *scalania* i przebiega następująco. Na początku ciąg wynikowy jest pusty i ustawiamy po jednym wskaźniku na początku każdego ze scalanych ciągów. Następnie (aż zabraknie elementów) porównujemy wskazywane elementy, a mniejszy z porównanych elementów przepisujemy na ciąg wynikowy i przesuwamy wskaźnik w tym ciągu, z którego był wzięty element do ciągu wynikowego.

Przykład 8.1. Scal następujące ciągi liczb: (2,5,10,13,16,23) i (1,3,4,7,15,20).

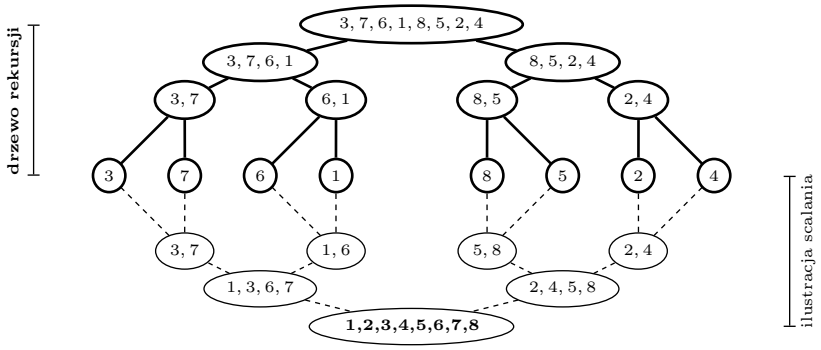
Rozwiązanie. Aktualne pozycje wskaźników oznaczone są przez pogrubienie czcionki.

(2,5,10,13,16,23) (1,3,4,7,15,20) = []
(**2**,5,10,13,16,23) (**1**,3,4,7,15,20) = [1]
(**2**,5,10,13,16,23) (1,**3**,4,7,15,20) = [1,2]
(2,**5**,10,13,16,23) (1,**3**,4,7,15,20) = [1,2,3]
(2,**5**,10,13,16,23) (1,3,**4**,7,15,20) = [1,2,3,4]
(2,**5**,10,13,16,23) (1,3,4,**7**,15,20) = [1,2,3,4,5]
(2,5,**10**,13,16,23) (1,3,4,**7**,15,20) = [1,2,3,4,5,7]
(2,5,**10**,13,16,23) (1,3,4,7,**15**,20) = [1,2,3,4,5,7,10]
(2,5,10,**13**,16,23) (1,3,4,7,**15**,20) = [1,2,3,4,5,7,10,13]
(2,5,10,13,**16**,23) (1,3,4,7,**15**,20) = [1,2,3,4,5,7,10,13,15]
(2,5,10,13,**16**,23) (1,3,4,7,15,**20**) = [1,2,3,4,5,7,10,13,15,16]
(2,5,10,13,16,**23**) (1,3,4,7,15,**20**) = [1,2,3,4,5,7,10,13,15,16,20]
(2,5,10,13,16,**23**) (1,3,4,7,15,20) = [1,2,3,4,5,7,10,13,15,16,20,23] ♯

Zadanie 8.2. Scal następujące ciągi liczb: (4,8,12,14,20,30,31) i (1,5,9,10,11,21,22).

Przykład 8.3. Używając procedury `merge-sort` posortuj ciąg liczb $3, 7, 6, 1, 8, 5, 2, 4$. Narysuj drzewo rekursji powstające podczas obliczeń.

Rozwiązanie.



Zadanie 8.4. Używając procedury `merge-sort` posortuj ciąg liczb $8, 4, 5, 2, 6, 3, 7, 1$. Narysuj drzewo rekursji powstające podczas obliczeń.

Przykład 8.5. Przypuśćmy, że mamy trzy paliki A, B i C. Na paliku A znajduje się n krążków różnej wielkości, osadzonych w porządku od największego na dole do najmniejszego na górze. Paliki B i C są początkowo puste. Należy przenieść wszystkie krążki z palika A na palik B,

posługując się w razie potrzeby palikiem C, przy czym:

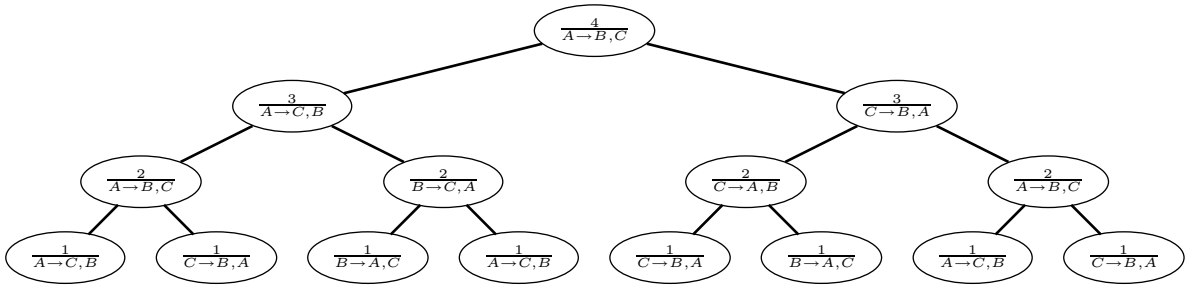
(i) można przenosić tylko po jednym krążku;
(ii) nie można umieszczać krażka większego na mniejszym.

Algorytm Przełóż(n, A, B, C)**:** przekładanie n krążków z palika A na B korzystając z palika C.

1. Jeśli $n = 1$, to przełóż krążek z A na B.
2. W przeciwnym przypadku:
   2.a. `przełóż`$(n-1, A, C, B)$;
   2.b. przełóż n-ty krążek z A na B;
   2.c. `przełóż`$(n-1, C, B, A)$.

Przykład 8.6. Zakładając, że wierzchołek o etykiecie $\frac{n}{A\to B,C}$ odpowiada wywołaniu procedury `przełóż`(n, A, B, C), narysuj drzewo rekursji dla przekładania czterech krążków z palika A na B; wypisz ciąg przełożeń.

Rozwiązanie. Drzewo rekursji przedstawia się następująco.



Sposób przekładania krążków wyznaczony jest przez przeszukanie powyższego drzewa w porządku inorder, wypisując za każdym razem, kiedy odwiedzamy węzeł, wykonanie odpowiedniego przełożenia krążka n w kroku 2.b: $\#n$: $A \to B$.

$\#1$: $A \to C$; $\#2$: $A \to B$; $\#1$: $C \to B$; $\#3$: $A \to C$; $\#1$: $B \to A$;
$\#2$: $B \to C$; $\#1$: $A \to C$; $\#4$: $A \to B$; $\#1$: $C \to B$; $\#2$: $C \to A$;
$\#1$: $B \to A$; $\#3$: $C \to B$; $\#1$: $A \to C$; $\#2$: $A \to B$; $\#1$: $C \to B$. ♯

Zadanie 8.7. Zakładając, że wierzchołek o etykiecie $\frac{n}{A\to B,C}$ odpowiada wywołaniu procedury `przełóż`(n, A, B, C), narysuj drzewo rekursji dla przekładania pięciu krążków z palika A na B; wypisz ciąg przełożeń.

Przykład 8.8. Rozważmy poniższą funkcję zdefiniowaną za pomocą wzoru rekurencyjnego

$$\begin{cases} f(0) = 1; \\ f(n) = 2 \cdot f(n-1), \ n \geq 1. \end{cases}$$

Korzystając z indukcji matematycznej wykaż, że $f(n) = 2^n$.

Rozwiązanie.

1. Krok bazowy. Dla $n = 0$ mamy $f(0) = 1 = 2^0$.
2. Założenie indukcyjne. Załóżmy, że dla pewnego $n \geq 0$ zachodzi $f(n) = 2^n$.
3. Krok indukcyjny. Rozważmy $n + 1$. Z definicji funkcji f mamy, że $f(n + 1) = 2 \cdot f(n)$. Z założenia indukcyjnego mamy, że $f(n) = 2^n$, a zatem $f(n + 1) = 2 \cdot 2^n = 2^{n+1}$. ♯

Zadanie 8.9. Dana jest funkcja $h: \mathbb{N} \to \mathbb{N}$

$$\begin{cases} h(0) = 1; \\ h(n) = 2 \cdot h(n-1) + 1, \ n \geq 1. \end{cases}$$

Oblicz $h(1), h(2), h(3)$. Co oblicza funkcja h?

Zadanie 8.10. Udowodnij indukcyjnie, że algorytm przekładania krążków wymaga $2^n - 1$ przełożeń do przeniesienia n krążków.

Przykład 8.11. Dana jest funkcja $D: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\begin{cases} D(x, 0) = x; \\ D(x, y + 1) = D(x, y) + 1, \ y \geq 0. \end{cases}$$

Oblicz $D(2, 3)$. Co oblicza funkcja D?

Rozwiązanie. Wyznaczmy najpierw $D(2, 3)$.

$$D(2,3) = D(2,2) + 1 = (D(2,1) + 1) + 1 = ((D(2,0) + 1) + 1) + 1 = 2 + 1 + 1 + 1 = 5.$$

Wyznaczając kilka innych wartości możemy wywnioskować, że funkcja $D(x, y)$ wyznacza sumę liczb x i y. Pozostaje to udowodnić — dowód indukcyjny przeprowadzimy względem y.

1. Krok bazowy. Dla dowolnego $x \geq 0$ oraz $y = 0$ mamy $D(x, 0) = x = x + 0$.
2. Założenie indukcyjne. Dla dowolnego $x \geq 0$ oraz pewnego $y \geq 0$ zachodzi $D(x, y) = x + y$.
3. Krok indukcyjny. Rozważmy dowolne $x \geq 0$ oraz $y + 1$. Z definicji funkcji D mamy, że $D(x, y + 1) = D(x, y) + 1$. Z założenia indukcyjnego otrzymujemy, że $D(x, y) = x + y$, a zatem $D(x, y + 1) = (x + y) + 1 = x + (y + 1)$. ♯

Zadanie 8.12. Dana jest funkcja $M: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$\begin{cases} M(x, 0) = 0; \\ M(x, y + 1) = M(x, y) + x, \ y \geq 0. \end{cases}$$

Oblicz $M(4, 3)$. Co oblicza funkcja M?

Zadanie 8.13. Dana jest funkcja $X: \mathbb{N} \to \mathbb{N}$

$$\begin{cases} X(1) = 1; \\ X(n) = X(X(n-1)) + 1, \ n \geq 2. \end{cases}$$

Co oblicza funkcja X?

Zadanie 8.14. Dana jest funkcja $g\colon \mathbb{N} \to \mathbb{N}$

$$\begin{cases} g(1) = 1; \\ g(n) = g(n-1) + 2n - 1, \ n \geq 2. \end{cases}$$

Wykaż, że $g(n) = n^2$.

Zadanie 8.15. Dana jest funkcja $g\colon \mathbb{N} \to \mathbb{N}$

$$\begin{cases} g(1) = 1; \\ g(n+1) = 2 \cdot g(n) - 1, \ n \geq 1. \end{cases}$$

Wykaż, że g jest funkcją stałą.

Zadanie 8.16. Funkcja Ackermanna określona jest następująco ($i, j, k \geq 1$, naturalne):

$$\begin{cases} A(1, j, k) = j + k; \\ A(i+1, j, 1) = j, \ i \geq 1; \\ A(i+1, j, k+1) = A(i, j, A(i+1, j, k)), \text{ gdy } i, k \geq 1. \end{cases}$$

a) Oblicz $A(2, j, 1)$, $A(2, j, 2)$, $A(2, j, 3)$ oraz $A(3, j, 1)$, $A(3, j, 2)$, $A(3, j, 3)$.
b) Udowodnij, że $A(2, j, k) = j \cdot k$ oraz $A(3, j, k) = j^k$.
c) Oblicz $A(4, 2, 1)$, $A(4, 2, 2)$, $A(4, 2, 3)$. Udowodnij, że $A(4, j, k) = j^{\cdot^{\cdot^{\cdot^{j}}}\}k}$.

Przykład 8.17. Zapisz definicję rekurencyjną dla ciągu $a_0, a_1, a_2, \ldots$, gdzie $a_n = (n+1)(2n+3)$.

Rozwiązanie. W oparciu o definicję „rozwińmy" wyraz a_{n+1}.

$$a_{n+1} = (n+2)(2n+5) = 2n^2+9n+10 = 2n^2+5n+3+4n+7 = (n+1)(2n+3)+4n+7 = a_n+4n+7.$$

W konsekwencji otrzymujemy, że

$$\begin{cases} a_0 = 3; \\ a_n = a_{n-1} + 4n + 3, \ n \geq 1. \end{cases}$$ ♯

Zadanie 8.18. Zapisz definicję rekurencyjną dla ciągu $a_0, a_1, a_2, \ldots$, gdzie $a_n = 2 - (-1)^n$.

Przykład 8.19. Dla $x \in \mathbb{N}^+, y \in \mathbb{N}$ przedstaw rekurencyjną definicję funkcji wykładniczej x^y i udowodnij za pomocą indukcji jej poprawność.

Rozwiązanie. Funkcję wykładniczą $p(x, y) = x^y$ można przedstawić za pomocą następującego wzoru rekurencyjnego.

$$\begin{cases} p(x, 0) = 1; \\ p(x, y+1) = p(x, y) \cdot x, \text{ gdy } y \geq 0. \end{cases}$$

1. Krok bazowy. Dla dowolnego $x \geq 0$ oraz $y = 0$ mamy $p(x, 0) =$[wzór]$= 1 = x^0$.
2. Założenie indukcyjne. Dla dowolnego $x \geq 0$ oraz pewnego $y \geq 0$ zachodzi $p(x, y) = x^y$.
3. Krok indukcyjny. Rozważmy dowolne $x \geq 0$ oraz $y + 1$.

$$p(x, y+1) =\text{[wzór]}= p(x, y) \cdot x =\text{[założenie]}= x^y \cdot x = x^{y+1}.$$ ♯

Zadanie 8.20. Przedstaw rekurencyjną definicję operacji odejmowania jedynki w liczbach naturalnych, która określona jest wzorem $\max\{x-1, 0\}$. Udowodnij za pomocą indukcji jej poprawność.

Zadanie 8.21. Przedstaw rekurencyjną definicję operacji odejmowania w liczbach naturalnych, która określona jest wzorem $\max\{x-y,0\}$. Udowodnij za pomocą indukcji jej poprawność.

Przykład 8.22. Postać funkcji rekurencyjnej można obliczyć (lub oszacować) *metodą iteracyjną*. W metodzie tej rozwijamy kolejne wyrazy funkcji. Rozważmy dla przykładu funkcję $T(n)$, o której wiemy, że

$$\begin{cases} T(1)=1; \\ T(n)\leq 2\cdot T(\frac{n}{2})+n,\ n\geq 2. \end{cases}$$

Dla uproszczenia załóżmy, że n jest pewną potęgą dwójki. Wówczas funkcję T rozwijamy w następujący sposób.

$$T(n)=n+2\cdot T(\frac{n}{2})=n+2(\frac{n}{2}+2\cdot T(\frac{n}{4}))=n+n+4\cdot T(\frac{n}{4})=n+\ldots+n+2^i\cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1)$, czyli wtedy, gdy $i=\log_2 n$. Otrzymujemy w konsekwencji, że

$$T(n)=\underbrace{n+\ldots+n}_{i}+2^i\cdot T(1)=n\sum_{i=1}^{\log_2 n}1+2^{\log_2 n}=n\log_2 n+n. \qquad \sharp$$

Przykład 8.23. Zastosuj metodę iteracyjną w celu wyznaczenia funkcji $T(n)$, o której wiemy, że

$$\begin{cases} T(1)=1; \\ T(n)\leq 3\cdot T(\lceil\frac{n}{4}\rceil)+n,\ n\geq 2. \end{cases}$$

Rozwiązanie. Dla uproszczenia załóżmy, że n jest pewną potęgą czwórki. Wówczas funkcję T rozwijamy w następujący sposób:

$$T(n)=n+3\cdot T(\frac{n}{4})=n+3(\frac{n}{4}+3\cdot T(\frac{n}{16}))=n+\frac{3}{4}n+9\cdot T(\frac{n}{16})=n+\frac{3}{4}n+\ldots+(\frac{3}{4})^{i-1}n+3^i\cdot T(\frac{n}{4^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1)$, czyli wtedy, gdy $i=\log_4 n$. Otrzymujemy wtedy, że

$$T(n)=n+\frac{3}{4}n+\ldots+(\frac{3}{4})^{i-1}n+3^i\cdot T(1)\leq n\sum_{i=0}^{\infty}(\frac{3}{4})^i+3^{\log_4 n}.$$

Jako że $\sum_{i=0}^{\infty}(\frac{3}{4})^i=4$, $3^{\log_4 n}=n^{\log_4 3}$, oraz $\log_4 3<1$, a tym samym zachodzi $n^{\log_4 3}\leq n$, otrzymujemy, że

$$T(n)\leq 4n+n=5n. \qquad \sharp$$

Zadanie 8.24. Metodą iteracyjną znajdź (dokładne) rozwiązanie poniższych zależności rekurencyjnych.

a) $\begin{cases} T(1)=1; \\ T(n)=2\cdot T(\lceil\frac{n}{2}\rceil)+1,\ n\geq 2. \end{cases}$

b) $\begin{cases} T(1)=1; \\ T(n)=4\cdot T(\frac{n}{2})+n^2,\ n\geq 2. \end{cases}$

c) $\begin{cases} T(1) = 1; \\ T(n) = 3 \cdot T(\lceil \frac{n}{2} \rceil) + n, \ n \geq 2. \end{cases}$

d) $\begin{cases} T(1) = 1; \\ T(n+1) = n \cdot T(n) + n!, \ n \geq 1. \end{cases}$

e) $\begin{cases} T(1) = A; \\ T(n) = 2 \cdot T(\frac{n}{2}) + B. \end{cases}$

f) $\begin{cases} T(1) = A; \\ T(n) = 2 \cdot T(\frac{n}{2}) + Bn, \ n \geq 2. \end{cases}$

g) $\begin{cases} T(1) = A; \\ T(n) = 2 \cdot T(\frac{n}{2}) + Bn + C, \ n \geq 2. \end{cases}$

Stałe A, B i C są dowolne (ale ustalone). W przypadkach (a-c) oraz (e-g) przyjmij, że rozwiązanie jest określone dla $n = 2^k, k \in \mathbb{N}$.

Zadanie 8.25.* Dana jest zależność rekurencyjna

$$\begin{cases} T(a) \in \mathbb{R}; \\ T(n) = T(n-a) + T(a) + n, \ n > a. \end{cases}$$

dla $a \geq 1$ oraz $n = k \cdot a$ dla pewnego $k \in \mathbb{N}$. Znajdź rozwiązanie tej rekurencji.

8.1 Zadania dodatkowe

Przykład 8.26.* Postać funkcji rekurencyjnej można obliczyć (lub oszacować) *metodą podstawiania*. W metodzie tej odgadujemy rozwiązanie ogólne, próbujemy je uściślić i wykazujemy jego poprawność. Dla przykładu oszacujmy funkcję $T(n)$ z Przykładu 8.22:

$$\begin{cases} T(1) = 1; \\ T(n) \leq 2 \cdot T(\frac{n}{2}) + n, \ n \geq 2. \end{cases}$$

Zgadujemy, że $T(n) \leq c(n \log_2 n + n)$ dla jakiejś stałej $c > 0$. Wykażemy, że powyższa nierówność zachodzi dla dowolnego $n \geq 1$ (będącego potęgą dwójki).

1. Krok bazowy.

   Dla $n = 1$ jest to prawda: mamy $T(1) = 1 \leq c \cdot (1 \cdot \log_2 1 + 1) = c$, dla $c \geq 1$.

2. Założenie indukcyjne.

   Niech $n \geq 2$ i załóżmy, że $T(n') \leq c \cdot (n' \log_2 n' + n')$ dla wszystkich $1 \leq n' < n$.

3. Krok indukcyjny.

   Wówczas z warunków na funkcję T i z założenia indukcyjnego mamy, że

   $$T(n) \leq 2 \cdot c \cdot (\frac{n}{2} \log_2 \frac{n}{2} + \frac{n}{2}) + n = cn \log_2 \frac{n}{2} + 2n.$$

   Jako że $\log_2 \frac{n}{2} \leq \log_2 n - 1$, $n \geq 2$, otrzymujemy

   $$T(n) \leq c \cdot n \log_2 n - cn + 2n \leq c \cdot n \log_2 n + n, \text{ dla } c \geq 1. \qquad \sharp$$

Przykład 8.27.* Dana jest funkcja $T\colon \mathbb{N}^+ \to \mathbb{N}$

$$\begin{cases} T(1) = A; \\ T(n) = 4 \cdot T(\lfloor \frac{n}{2} \rfloor) + n. \end{cases}$$

Udowodnij, że $T(n) \leq B \cdot (n^2 - n)$ dla $n \in \mathbb{N}^+$ oraz pewnych $A, B \in \mathbb{N}$. Jakie warunki muszą spełniać A i B?

Rozwiązanie.

1. Krok bazowy.

   Jako że $T(1) = 1$, sugerowana nierówność $T(n) \leq B \cdot (n^2 - n)$ przyjmująca postać $T(1) \leq B \cdot (1^2 - 1) = 0$ pociąga za sobą, że $A = 0$. A zatem dla $n = 1$, $A = 0$ oraz dowolnego $B \geq 0$ spełniony jest krok bazowy: $T(1) = 0 \leq B \cdot (1^2 - 1)$.

2. Założenie indukcyjne.

   Niech $n \geq 2$ i załóżmy, że dla pewnego B zachodzi $T(\bar{n}) \leq B \cdot (\bar{n}^2 - \bar{n})$ dla wszystkich $1 \leq \bar{n} < n$.

3. Krok indukcyjny.

   Rozważmy rekurencyjną postać funkcji $T(n) = 4 \cdot T(\lfloor \frac{n}{2} \rfloor) + n$. (Dla ułatwienia zakładamy, że n jest potęgą dwójki.) Z założenia indukcyjnego otrzymujemy, że

   $$\begin{aligned} T(n) &\leq [\text{założenie indukcyjne dla } T(\lfloor \tfrac{n}{2} \rfloor)] \leq 4 \cdot B \cdot ((\tfrac{n}{2})^2 - \tfrac{n}{2}) + n \\ &= 4 \cdot B \cdot (\tfrac{n^2}{4} - \tfrac{n}{2}) + n = B \cdot (n^2 - 2n) + n \leq B \cdot (n^2 - n) - Bn + n. \end{aligned}$$

   Zauważmy, że dla $B \geq 1$ zachodzi $-Bn + n \leq 0$, a tym samym dla $A = 0$ oraz $B \geq 1$ otrzymamy, że $T(n) \leq B \cdot (n^2 - n)$, co należało wykazać. ♯

Zadanie 8.28.* Dana jest funkcja $T\colon \mathbb{N} \to \mathbb{N}$

$$\begin{cases} T(0) = T(1) = T(2) = 1; \\ T(n) = T(n-2) + T(n-3), \ n \geq 3. \end{cases}$$

Udowodnij, że $T(n) \leq (\frac{4}{3})^n$ dla $n \in \mathbb{N}$.

Zadanie 8.29.* Dana jest funkcja $T\colon \mathbb{N}^+ \to \mathbb{N}$

$$\begin{cases} T(1) = 1; \\ T(n) = T(\lceil \frac{n}{2} \rceil) + 1, \ n \geq 2. \end{cases}$$

Udowodnij, że $T(n) = O(\log_2 n)$.

Zadanie 8.30.* Dana jest funkcja $T\colon \{2^k : k \in \mathbb{N}\} \to \mathbb{N}$

$$\begin{cases} T(1) = 1; \\ T(n) = 2 \cdot T(\frac{n}{2}) + 2, \ n \geq 2. \end{cases}$$

Udowodnij, że $T(n) = an + b$ dla pewnych a i b. Wyznacz te stałe.

Twierdzenie 8.71 (o rekurencji uniwersalnej) *Niech dana będzie funkcja* $T : \mathbb{N}^+ \to \mathbb{N}^+$ *określona zależnością reukrencyjną*

$$T(n) = a \cdot T(\frac{n}{b}) + f(n),$$

gdzie $a \geq 1, b > 1$, a $\frac{n}{b}$ *oznacza* $\lfloor \frac{n}{b} \rfloor$ *lub* $\lceil \frac{n}{b} \rceil$. *Wówczas:*

1. *Jeśli* $f(n) = O(n^{\log_b a - \epsilon})$ *dla pewnego* $\epsilon > 0$, *to* $T(n) = \Theta(n^{\log_b a})$.
2. *Jeśli* $f(n) = \Theta(n^{\log_b a})$, *to* $T(n) = \Theta(n^{\log_b a} \log_2 n)$.
3. *Jeśli* $f(n) = \Theta(n^{\log_b a + \epsilon})$ *dla pewnego* $\epsilon > 0$ *oraz jeśli* $af(\frac{n}{b}) \leq cf(n)$ *dla pewnej stałej* $c < 1$ *i wszystkich dostatecznie dużych* n, *to* $T(n) = \Theta(f(n))$.

Przykład 8.31.* Wskaż oszacowania rozwiązań zależności rekurencyjnych z Zadania 8.24 (za wyjątkiem pkt. d) korzystając z twierdzenia o rekurencji uniwersalnej i porównaj je z otrzymanymi dokładnymi rozwiązaniami.

Rozwiązanie.

a) $f(n) = 1$ i funkcja f rośnie wolniej niż $n^{\log_2 2} = n$, stąd $T(n) = \Theta(n)$.
b) $f(n) = n$ i funkcja f rośnie wolniej niż $n^{\log_2 3}$, stąd $T(n) = \Theta(n^{\log_2 3})$.
c) $f(n) = n^2$ i funkcja f rośnie tak samo, jak $n^{\log_2 4}$, stąd $T(n) = \Theta(n^2 \log_2 n)$.
d) nie dotyczy
e) $f(n) = B$ i funkcja f rośnie wolniej niż $n^{\log_2 2} = n$, stąd $T(n) = \Theta(n)$.
f) $f(n) = Bn$ i funkcja f rośnie tak samo, jak $n^{\log_2 2}$, stąd $T(n) = \Theta(n \log_2 n)$.
g) $f(n) = Bn + C$ i funkcja f rośnie tak samo, jak $n^{\log_2 2}$, stąd $T(n) = \Theta(n \log_2 n)$.

Zadanie 8.32.* Korzystając z twierdzenia o rekurencji uniwersalnej wskaż oszacowania rozwiązań następujących równań rekurencyjnych.

a) $T(n) = 9 \cdot T(\lfloor \frac{n}{3} \rfloor) + n$.

b) $T(n) = T(\lfloor \frac{2n}{3} \rfloor) + 1$.

c) $T(n) = 3 \cdot T(\lfloor \frac{n}{4} \rfloor) + n \log_2 n$.

d) $T(n) = 3 \cdot T(\lfloor \frac{n}{2} \rfloor) + n$.

e) $T(n) = 4 \cdot T(\lfloor \frac{n}{2} \rfloor) + n$.

f) $T(n) = 4 \cdot T(\lfloor \frac{n}{2} \rfloor) + n^2$.

g) $T(n) = 4 \cdot T(\lfloor \frac{n}{2} \rfloor) + n^3$.

Odpowiedzi do zadań

8.9. $h(n) = 2^{n+1} - 1$.

1. Krok bazowy. Dla $n = 0$ mamy $h(0) =$[wzór]$= 1 = 2^{0+1} - 1$.
2. Założenie indukcyjne. Dla pewnego $n \geq 0$ zachodzi $h(n) = 2^{n+1} - 1$.
3. Krok indukcyjny. Rozważmy $n + 1$.

$$h(n+1) =\text{[wzór]}= 2 \cdot h(n) + 1 =\text{[założenie]}= 2 \cdot (2^{n+1} - 1) + 1 = 2^{n+2} + 1.$$

8.10. $T(n) = 2^n - 1$.

1. Krok bazowy. Dla $n = 1$ mamy $T(1) =$[algorytm]$= x = 2^1 - 1$.
2. Założenie indukcyjne. Dla pewnego $n \geq 1$ zachodzi $T(n) = 2^n - 1$.
3. Krok indukcyjny. Rozważmy $n + 1$.

$$T(n+1) =\text{[algorytm]}= 2 \cdot T(n) + 1 =\text{[założenie]}= 2 \cdot (2^n - 1) + 1 = 2^{n+1} - 1.$$

8.12. $M(x, y) = x \cdot y$.

1. Krok bazowy. Dla dowolnego $x \geq 0$ oraz $y = 0$ mamy $M(x, 0) =$[wzór]$= 0 = x \cdot 0$.
2. Założenie indukcyjne. Dla dowolnego $x \geq 0$ oraz pewnego $y \geq 0$ zachodzi $M(x, y) = x \cdot y$.
3. Krok indukcyjny. Rozważmy dowolne $x \geq 0$ oraz $y + 1$.

$$M(x, y+1) =\text{[wzór]}= M(x, y) + x =\text{[założenie]}= x \cdot y + x = x \cdot (y + 1).$$

8.13. $X(n) = n$.

1. Krok bazowy. Dla $n = 1$ mamy $X(1) =$[wzór]$= 1$.
2. Założenie indukcyjne. Dla pewnego $n \geq 1$ zachodzi $X(n) = n$.
3. Krok indukcyjny. Rozważmy $n + 1$.

$$X(n+1) =\text{[wzór]}= X(X(n)) + 1 =\text{[założenie]}= X(n) + 1 =\text{[założenie]}= n + 1.$$

8.14.

1. Krok bazowy. Dla $n = 1$ mamy $g(1) =$[wzór]$= 1 = 1^2$.
2. Założenie indukcyjne. Dla pewnego $n \geq 1$ zachodzi $g(n) = n^2$.
3. Krok indukcyjny. Rozważmy $n + 1$.

$$g(n+1) =\text{[wzór]}= g(n) + 2n + 1 =\text{[założenie]}= n^2 + 2n + 1 = (n + 1)^2.$$

8.15.

1. Krok bazowy. Dla $n = 1$ mamy $g(1) =$[wzór]$= 1$.
2. Założenie indukcyjne. Dla pewnego $n \geq 1$ zachodzi $g(n) = 1$.
3. Krok indukcyjny. Rozważmy $n + 1$.

$$g(n+1) =\text{[wzór]}= 2 \cdot g(n) - 1 =\text{[założenie]}= 2 \cdot 1 - 1 = 1.$$

8.16. $A(2, j, k) = j \cdot k$.

1. Krok bazowy. Dla dowolnych $j \geq 1$ oraz $k = 1$ mamy $A(2, j, 1) =$[wzór]$= j = j \cdot 1$.
2. Założenie indukcyjne. Dla dowolnych $j \geq 1$ oraz pewnego $k \geq 1$ zachodzi $A(2, j, k) = j \cdot k$.

3. Krok indukcyjny. Rozważmy dowolne $j \geq 1$ oraz $k+1$.

$$A(2,j,k+1) = [\text{wzór}] = A(1,j,A(2,j,k)) = [\text{założenie}] = A(1,j,j\cdot k) = j + j\cdot k = j(k+1).$$

$A(3,j,k) = j^k$.

1. Krok bazowy. Dla dowolnych $j \geq 1$ oraz $k = 1$ mamy $A(3,j,1) = [\text{wzór}] = j = j^1$.
2. Założenie indukcyjne. Dla dowolnych $j \geq 1$ oraz pewnego $k \geq 1$ zachodzi $A(3,j,k) = j^k$.
3. Krok indukcyjny. Rozważmy dowolne $j \geq 1$ oraz $k+1$.

$$A(3,j,k+1) = [\text{wzór}] = A(2,j,A(3,j,k)) = [\text{założenie}] = A(2,j,j^k) = j\cdot j^k = j^{k+1}.$$

$A(4,j,k) = j^{\cdot^{\cdot^{\cdot^{j}}}\}k}$.

1. Krok bazowy. Dla dowolnych $j \geq 1$ oraz $k = 1$ mamy $A(4,j,1) = [\text{wzór}] = j^1$.
2. Założenie indukcyjne. Dla dowolnych $j \geq 1$ oraz pewnego $k \geq 1$ zachodzi $A(4,j,k) = j^{\cdot^{\cdot^{\cdot^{j}}}\}k}$.
3. Krok indukcyjny. Rozważmy dowolne $j \geq 1$ oraz $k+1$.

$$A(4,j,k+1) = [\text{wzór}] = A(3,j,A(4,j,k)) = [\text{założenie}] = A(3,j,j^{\cdot^{\cdot^{\cdot^{j}}}\}k}) = j^{j^{\cdot^{\cdot^{\cdot^{j}}}\}k}} = j^{\cdot^{\cdot^{\cdot^{j}}}\}k+1}.$$

8.18.

$$\begin{cases} a_0 = 1; \\ a_n = 4 - a_{n-1}, \ n \geq 1. \end{cases}$$

albo

$$\begin{cases} a_0 = 1; \\ a_n = a_{n-1} + 2\cdot(-1)^{n-1}, \ n \geq 1. \end{cases}$$

8.20. Postać rekurencyjna funkcji odejmowania jedynki od liczby naturalnej, tj. $\max\{x-1,0\}$:

$$\begin{cases} \text{minus}(0) = 0; \\ \text{minus}(1) = 0; \\ \text{minus}(x) = \text{minus}(x-1) + 1, \ x \geq 2. \end{cases}$$

Dowód.

1. Krok bazowy. Dla $x = 0$ mamy $\text{minus}(0) = [\text{wzór}] = 0 = \max\{0-1,0\}$.
   Dla $x = 1$ mamy $\text{minus}(1) = [\text{wzór}] = 0 = \max\{1-1,0\}$.

2. Założenie indukcyjne.

   Rozważmy pewne $x \geq 2$ (bo dla $x = 0$ i $x = 1$ już wykazaliśmy) i załóżmy, że dla wszystkich $0 \leq x' < x$ zachodzi $\text{minus}(x') = \max\{x'-1,0\}$.

3. Krok indukcyjny.

$$\begin{aligned} \text{minus}(x) &= [\text{wzór}] = \text{minus}(x-1) + 1 = [\text{założenie}] = \max\{(x-1)-1,0\} + 1 \\ &= \max\{x-1,1\} = [x \geq 2] = \max\{x-1,0\}. \end{aligned}$$

8.21. Postać rekurencyjna funkcji odejmowania dwóch liczb naturalnych, tj. $\max\{x-y,0\}$:

$$\begin{cases} \text{minus}(x,0) = x; \\ \text{minus}(0,y) = 0; \\ \text{minus}(x,y) = \text{minus}(x-1,y-1), \ x,y \geq 1. \end{cases}$$

Dowód.

1. Krok bazowy. Dla $y = 0$ mamy $\text{minus}(x, 0) =$[wzór]$= x = \max\{x - 0, 0\}$.
   Dla $x = 0$ mamy $\text{minus}(0, y) =$[wzór]$= 0 = \max\{0 - y, 0\}$.

2. Założenie indukcyjne.

   Rozważmy pewne $x, y \geq 1$ i załóżmy, że dla dowolnych $0 \leq x' < x$ oraz $0 \leq y' < y$ zachodzi

   $$\text{minus}(x', y') = \max\{x' - y', 0\}.$$

3. Krok indukcyjny.

   $$\begin{aligned} \text{minus}(x, y) &= [\text{wzór}] = \text{minus}(x - 1, y - 1) \\ &= [\text{założenie}] = \max\{(x - 1) - (y - 1), 0\} = \max\{x - y, 0\}. \end{aligned}$$

8.24.

a) Funkcję T rozwijamy w następujący sposób:

$$T(n) = 1 + 2 \cdot T(\frac{n}{2}) = 1 + 2(1 + 2 \cdot T(\frac{n}{4})) = 1 + 2 + 4 \cdot T(\frac{n}{4}) = 1 + \ldots + 2^{i-1} + 2^i \cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1)$, czyli wtedy, gdy $i = \log_2 n$. Otrzymujemy wtedy

$$T(n) = 1 + \ldots + 2^{i-1} + 2^i \cdot T(1) = n - 1 + 2^{\log_2 n} = n - 1 + n = 2n - 1.$$

b) Funkcję T rozwijamy w następujący sposób:

$$T(n) = n^2 + 4 \cdot T(\frac{n}{2}) = n^2 + 4((\frac{n}{2})^2 + 4 \cdot T(\frac{n}{4})) = n^2 + n^2 + 4^2 \cdot T(\frac{n}{4}) = n^2 + \ldots + n^2 + 4^i \cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1)$, czyli wtedy, gdy $i = \log_2 n$. Otrzymujemy wtedy

$$T(n) = \underbrace{n^2 + \ldots + n^2}_{i} + 4^i \cdot T(1) = n^2 \sum_{i=1}^{\log_2 n} 1 + 4^{\log_2 n} = n^2 \log_2 n + n^2.$$

c) Funkcję T rozwijamy w następujący sposób:

$$T(n) = n + 3 \cdot T(\frac{n}{2}) = n + 3(\frac{n}{2} + 3 \cdot T(\frac{n}{4})) = n + \frac{3}{2}n + 9 \cdot T(\frac{n}{4}) = n \cdot (1 + \ldots + (\frac{3}{2})^{i-1}) + 3^i \cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1)$, czyli wtedy, gdy $i = \log_2 n$. Otrzymujemy wtedy

$$T(n) = n \cdot (1 + \ldots + (\frac{3}{2})^{i-1}) + 3^i \cdot T(1) = n \cdot (2 \cdot n^{\log_2 \frac{3}{2}} - 2) + 3^{\log_2 n} = 3 \cdot n^{\log_2 3} - 2n.$$

d) Funkcję T rozwijamy w następujący sposób:

$$\begin{aligned} T(n) &= n! + n \cdot T(n-1) \\ &= n! + n \cdot ((n-1) \cdot T(n-2) + (n-1)!) \\ &= 2n! + n \cdot (n-1) \cdot T(n-2) \\ &= \dots \\ &= kn! + n \cdot (n-1) \cdot (n-k+1) \cdot T(n-k). \end{aligned}$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1)$, czyli wtedy, gdy $k = n-1$. Otrzymujemy wtedy

$$T(n) = (n-1) \cdot n! + n! \cdot T(1) = n \cdot n!.$$

e) Funkcję T rozwijamy w następujący sposób:

$$T(n) = B + 2 \cdot T(\frac{n}{2}) = B + 2(B + 2 \cdot T(\frac{n}{4})) = B + 2B + 2^2 \cdot T(\frac{n}{4}) = B \cdot (1 + \ldots + 2^{i-1}) + 2^i \cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1) = A$, czyli wtedy, gdy $i = \log_2 n$. Otrzymujemy wtedy

$$T(n) = B \cdot (1 + \ldots + 2^{i-1}) + 2^i \cdot T(1) = B \cdot (2^i - 1) + 2^{\log_2 n} \cdot A = (n-1) \cdot B + n \cdot A = (A+B) \cdot n - B.$$

f) Funkcję T rozwijamy w następujący sposób:

$$T(n) = Bn + 2 \cdot T(\frac{n}{2}) = Bn + 2(B\frac{n}{2} + 2 \cdot T(\frac{n}{4})) = Bn + Bn + 2^2 \cdot T(\frac{n}{4}) = Bn \cdot (1 + \ldots + 1) + 2^i \cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1) = A$, czyli wtedy, gdy $i = \log_2 n$. Otrzymujemy wtedy

$$T(n) = Bn \cdot (\underbrace{1 + \ldots + 1}_{i}) + 2^i \cdot T(1) = Bn \sum_{i=1}^{\log_2 n} 1 + 2^i \cdot T(1) = Bn \cdot \log_2 n + 2^{\log_2 n} \cdot A = Bn \log_2 n + An.$$

g) Funkcję T rozwijamy w następujący sposób:

$$T(n) = C + Bn + 2 \cdot T(\frac{n}{2}) = C + Bn + 2(C + B\frac{n}{2} + 2 \cdot T(\frac{n}{4})) = (C + 2C) + (Bn + Bn) + 2^2 \cdot T(\frac{n}{4}) =$$

$$= C \cdot (1 + \ldots + 2^{i-1}) + Bn \cdot (1 + \ldots + 1) + 2^i \cdot T(\frac{n}{2^i}).$$

Iterację powtarzamy, aż ostatni składnik będzie zawierał $T(1) = A$, czyli wtedy, gdy $i = \log_2 n$. Otrzymujemy wtedy

$$T(n) = C \cdot (1 + \ldots + 2^{i-1}) + Bn \cdot (\underbrace{1 + \ldots + 1}_{i}) + 2^i \cdot T(1) =$$

$$= C(n-1) + Bn \log_2 n + 2^{\log_2 n} A = Bn \log_2 n + (A + C)n - C.$$

8.25. Funkcję T rozwijamy w następujący sposób:

$$\begin{aligned}
T(n) &= n + T(a) + T(n-a) \\
&= n + T(a) + ((n-a) + T(a) + T(n-2a)) \\
&= 2(n + T(a)) - a + T(n-2a) \\
&= 2(n + T(a)) - a + ((n-2a) + T(a) + T(n-3a)) \\
&= 3(n + T(a)) - (a + 2a) + T(n-3a) \\
&= 3(n + T(a)) - (a + 2a) + ((n-3a) + T(a) + T(n-4a)) \\
&= 4(n + T(a)) - (a + 2a + 3a) + 4 \cdot T(a) + T(n-4a) \\
&= \ldots \\
&= i \cdot (n + T(a)) - (1 + 2 + \ldots + (i-1))a + T(n-ka) \\
&= i \cdot (n + T(a)) - \tfrac{i(i-1)}{2} \cdot a + T(n-ia).
\end{aligned}$$

Iterację powtarzamy, aż ostatni składnik będzie postaci $T(a)$, tj. gdy $n - ia = a$, czyli wtedy, gdy $i = \frac{n-a}{a} = \frac{ka-a}{a} = k - 1$. Otrzymujemy wtedy

$$T(n) = (k-1) \cdot (n + T(a)) - \frac{(k-1)(k-2)}{2} \cdot a + T(a) = (k-1) \cdot n + k \cdot T(a) - \frac{(k-1)(k-2)}{2} \cdot a.$$

8.28.

1. Krok bazowy. Dla $n = 1, 2, 3$ mamy:
   $T(1) =$[wzór]$= 1 \leq (\frac{4}{3})^1$;
   $T(2) =$[wzór]$= 1 \leq (\frac{4}{3})^2$;
   $T(3) =$[wzór]$= 1 \leq (\frac{4}{3})^3$.

2. Założenie indukcyjne. Rozważmy $n \geq 4$ i załóżmy, że dla $3 \leq n' < n$ zachodzi $T(n') \leq (\frac{4}{3})^{n'}$.
3. Krok indukcyjny.
   $T(n) =$[wzór]$= T(n-2) + T(n-3) =$[założenie]$\leq (\frac{4}{3})^{n-2} + (\frac{4}{3})^{n-3} = (\frac{4}{3} + 1) \cdot (\frac{4}{3})^{n-3}$.
   Ale zachodzi $\frac{4}{3} + 1 \leq \frac{64}{27}$, stąd $T(n) \leq \frac{64}{27} \cdot (\frac{4}{3})^{n-3} = (\frac{4}{3})^n$.

8.29. Mamy wykazać, że istnieją stałe a i b takie, że $T(n) \leq a \cdot \log_2 n + b$. Zakładamy, że n jest potęgą dwójki.

1. Krok bazowy.

   Dla $n = 1$ mamy $T(1) =$[wzór]$= 1 \leq a \cdot 0 + b = a \cdot \log_2 1 + b$, dla dowolnego a i $b \geq 1$.

2. Założenie indukcyjne.

   Rozważmy $n \geq 2$ i załóżmy, że dla $1 \leq n' < n$ zachodzi $T(n') = O(\log_2 n')$, tzn. istnieją stałe a i b takie, że

   $$T(n') \leq a \cdot \log_2 n' + b$$

   dla dowolnego $n' < n$ (n' jest potęgą dwójki).

3. Krok indukcyjny.

   $T(n) =$[wzór]$= T(\frac{n}{2}) + 1 =$[założenie]$\leq a \cdot \log_2 \frac{n}{2} + b + 1 = a \cdot (\log_2 n - \log_2 2) + b + 1$. Stąd

   $$T(n) \leq a \cdot \log_2 n + b + (1 - a) \leq a \cdot \log_2 n + b, \text{ o ile } a \geq 1.$$

   Zatem można przyjąć np. $a = 1$, $b = 1$.

8.30.

1. Krok bazowy.

   Dla $n = 1$ mamy $T(1) =$[wzór]$= 1 = a + b$, dla pewnych a i b.

2. Założenie indukcyjne.

   Rozważmy $n \geq 2$ i załóżmy, że dla $1 \leq n' < n$ zachodzi $T(n') = an' + b$ dla pewnych (tych samych, co wyżej) a i b.

3. Krok indukcyjny.

   $$T(n) =[\text{wzór}]= 2 \cdot T(\tfrac{n}{2}) + 2 =[\text{założenie}]= 2 \cdot (a \cdot \tfrac{n}{2} + b) + b = an + 2b + 2.$$

   Jako że chcemy wykazać, że $T(n) = an + b$, stąd a i b muszą spełniać $an + 2b + 2 = an + b$. Stąd $b = -2$. Uwzględniając z pkt. (1) fakt, że $a + b = 1$ otrzymujemy $a = 2$. Zatem należy przyjąć $a = 3$, $b = -2$.

8.32.

a) $f(n) = n$ i funkcja f rośnie wolniej niż $n^{\log_3 9} = n^2$, stąd $T(n) = \Theta(n^2)$.
b) $f(n) = 1$ i funkcja f rośnie tak samo, jak $n^{\log_{\frac{3}{2}} 1} = n^0$, stąd $T(n) = \Theta(\log_2 n)$.
c) $f(n) = n \log_2 n$ i funkcja f rośnie szybciej niż $n^{\log_4 3}$, oraz $3 \cdot \frac{n}{4} \log_2 \frac{n}{4} \leq \frac{3}{4} \cdot n \log_2 n$, a zatem

$$T(n) = \Theta(n \log_2 n).$$

d) $f(n) = n$ i funkcja f rośnie wolniej niż $n^{\log_2 3}$, stąd $T(n) = \Theta(n^{\log_2 3})$.
e) $f(n) = n$ i funkcja f rośnie wolniej niż $n^{\log_2 4} = n^2$, stąd $T(n) = \Theta(n^2)$.
f) $f(n) = n^2$ i funkcja f rośnie tak samo, jak $n^{\log_2 4}$, stąd $T(n) = \Theta(n^2 \log_2 n)$.
g) $f(n) = n^3$ i f rośnie szybciej niż $n^{\log_2 4} = n^2$, oraz $4 \cdot (\frac{n}{2})^3 \leq \frac{1}{2} \cdot n^3$, stąd $T(n) = \Theta(n^3)$.

Zestaw zadań nr 9

Elementy teorii grafów

Graf nieskierowany $G = (V, E)$ jest to para składająca się z niepustego skończonego zbioru wierzchołków V oraz zbioru krawędzi E, gdzie krawędzie to nieuporządkowane pary wierzchołków:

$$E \subseteq \{\{u, v\} \quad | \quad u, v \in V\}.$$

Graf *prosty* to taki graf, dla którego:

(1) jeśli $\{u, v\} \in E$, to $u \neq v$ (brak *pętli*);
(2) co najwyżej tylko jedna para $\{u, v\} \in E$ (brak *multikrawędzi*).

Dwa wierzchołki u i v są *sąsiednie*, jeśli krawędź $e = \{u, v\} \in E$. Mówimy wówczas, że wierzchołki u, v są *incydentne* z tą krawędzią. Podobnie dwie różne krawędzie są *sąsiednie*, jeśli mają przynajmniej jeden wspólny wierzchołek. *Stopień wierzchołka* v jest liczbą krawędzi z nim incydentnych (ozn. $\deg(v)$). Wierzchołek stopnia 1 nazywany jest *liściem*, a wierzchołek stopnia 0 — *wierzchołkiem izolowanym*. Ciąg liczb $c = (d_1, d_2, ..., d_n)$ nazywamy ciągiem *grafowym*, jeśli istnieje graf G o n wierzchołkach, których stopnie równe są odpowiednim wyrazom ciągu c. W dalszej części skrypu poprzez „graf" w domyśle rozumiemy „graf prosty", w przeciwnym wypadku wyraźnie mówimy „multigraf".

Fakt 9.1 *Niech* $G = (V, E)$ *będzie dowolnym multigrafem. Wówczas* $\sum_{v \in V} \deg(v) = 2|E|$.

Zauważmy, że z powyższego faktu wynika, że suma stopni w dowolnym multigrafie $G = (V, E)$ jest liczbą parzystą, a w szczególności, że liczba wierzchołków o nieparzystym stopniu jest parzysta.

Zadanie 9.2. Narysuj grafy o następujących ciągach stopni:

a) $(4, 3, 2, 2, 1)$.
b) $(3, 3, 3, 3, 3, 3)$.

Zadanie 9.3. Wykaż (np. przez odpowiedni rysunek), że:

a) dla dowolnego parzystego $n \geq 4$ istnieje n-wierzchołkowy graf, których wszystkie stopnie wynoszą 3;

b) dla dowolnego nieparzystego $n \geq 5$ istnieje graf o $n + 1$ wierzchołkach, spośród których dokładnie n jest stopnia 3;

c) dla dowolnego $n \geq 5$ istnieje graf o n wierzchołkach, których wszystkie stopnie wynoszą 4.

Twierdzenie 9.4 (Havel 1955, Hakimi 1962)
Niech $c = (s, t_1, \ldots, t_s, d_1, d_2, ..., d_k)$ będzie nierosnącym ciągiem liczb. Wówczas ciąg stopni c jest ciągiem grafowym wtedy i tylko wtedy gdy ciąg stopni $(t_1 - 1, \ldots, t_s - 1, d_1, d_2, ..., d_k)$ jest grafowym.

Przykład 9.5. Które z następujących ciągów są grafowe?

a) $(5, 5, 4, 4, 3, 2, 2, 1, 1)$.
b) $(6, 5, 4, 3, 2, 2, 2, 2)$.

Rozwiązanie. Zauważmy, że w przypadku (a) liczba wierzchołków o nieparzystym stopniu jest nieparzysta, a zatem suma stopni jest nieparzysta i w konsekwencji otrzymujemy, że dany ciąg nie jest ciągiem grafowym.

W przypadku (b) warunek konieczny — suma stopni ma być parzysta — jest spełniony:

$$6 + 5 + 4 + 3 + 2 + 2 + 2 + 2 = 26.$$

Skorzystajmy zatem z twierdzenia 9.4. Otrzymujemy:

$$(\underline{6}, 5, 4, 3, 2, 2, 2, 2) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(5-1, 4-1, 3-1, 2-1, 2-1, 2-1, 2) = (4, 3, 2, 1, 1, 1, 2) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{4}, 3, 2, 2, 1, 1, 1) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(3-1, 2-1, 2-1, 1-1, 1, 1) = (2, 1, 1, 0, 1, 1) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{2}, 1, 1, 1, 1, 0) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(1-1, 1-1, 1, 1, 0) = (0, 0, 1, 1, 0) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{1}, 1, 0, 0, 0) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(1-1, 0, 0, 0) = (0, 0, 0, 0) \text{ jest ciągiem grafowym.}$$

Jako że graf o czterech wierzchołkach i bez krawędzi ma ciąg stopni równy $(0, 0, 0, 0)$, ciąg $(0, 0, 0, 0)$ jest ciągiem grafowym, a zatem na mocy twierdzenia 9.4 ciąg $(6, 5, 4, 3, 2, 2, 2, 2)$ jest także ciągiem grafowym.

Zauważmy, że już dla ciągu $(1, 1, 0, 0, 0)$ widać, że ciąg ten jest ciągiem grafowym — graf o pięciu wierzchołkach, z których dowolne ustalone dwa wierzchołki połączone są krawędzią, ma ciąg stopni równy $(1, 1, 0, 0, 0)$ — a zatem już na tym etapie możemy skorzystać z twierdzenia 9.4. ♯

Przykład 9.6. Narysuj graf (prosty) o ciągu stopni $(6, 5, 4, 3, 2, 2, 2, 2)$.

Rozwiązanie. W poprzednim zadaniu, w oparciu o twierdzenie 9.4, wykazaliśmy, że rzeczywiście taki graf istnieje. Okazuje się, że dowód ten może być użyty do konstrukcji szukanego grafu.

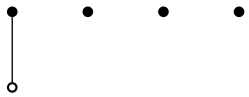
- Krok 1. Otrzymaliśmy, że ciąg $(0,0,0,0)$ jest ciągiem grafowym. Niech G_1 będzie grafem o ciągu $(0,0,0,0)$, a dokładnie, niech G_1 będzie 4-wierzchołkowym grafem o wszystkich stopniach równych zero. Z poprzednich rozważań zachodzi

$$(0,0,0,0) = (1-1,0,0,0) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{1},1,0,0,0) \text{ jest ciągiem grafowym.}$$

Zatem do grafu G_1 dodajemy jeden wierzchołek, który łączymy krawędzią z wybranym wierzchołkiem stopnia 0, otrzymując tym samym graf G_2 o ciągu stopni $(1,1,0,0,0)$.



- Z poprzednich rozważań zachodzi

$$(0,0,1,1,0) = (1-1,1-1,1,1,0) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{2},1,1,1,1,0) \text{ jest ciągiem grafowym.}$$

Zatem do grafu G_2 dodajemy jeden wierzchołek, który łączymy krawędziami z dwoma wybranymi wierzchołkami stopnia stopnia 0, otrzymując tym samym graf G_3 o ciągu stopni $(2,1,1,1,1,0)$.

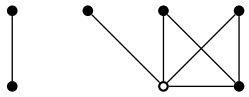
- Z poprzednich rozważań zachodzi

$$(2,1,1,0,1,1) = (3-1,2-1,2-1,1-1,1,1) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{4},3,2,2,1,1,1) \text{ jest ciągiem grafowym.}$$

Zatem do grafu G_3 dodajemy jeden wierzchołek, który łączymy krawędziami z dwoma wybranymi wierzchołkami stopnia stopnia 1, oraz z wierzchołkiem stopnia 2 i 0, otrzymując tym samym graf G_4 o ciągu stopni $(4,3,2,2,1,1,1)$.



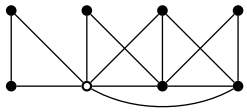
- Z poprzednich rozważań zachodzi

$$(4,3,2,1,1,1,2) = (5-1, 4-1, 3-1, 2-1, 2-1, 2-1, 2) \text{ jest ciągiem grafowym}$$

$$\Leftrightarrow$$

$$(\underline{6}, 5, 4, 3, 2, 2, 2, 2) \text{ jest ciągiem grafowym.}$$

Zatem do grafu G_4 dodajemy jeden wierzchołek, który łączymy krawędziami z trzema wierzchołkami stopnia stopnia 1, z wierzchołkiem stopnia 2, 3 oraz 4, otrzymując tym samym szukany graf (prosty) G_5 o ciągu stopni $(6,5,4,3,2,2,2,2)$.



♯

Zadanie 9.7. Które z następujących ciągów są grafowe?

a) $(4,4,4,4,3,3)$.
b) $(7,6,5,4,4,3,2,1)$.
c) $(6,6,5,5,2,2,2,2)$.
d) $(6,6,5,5,3,3,3,3)$.

Dla ciągów, które są grafowe, narysuj odpowiednie grafy (proste).

Zadanie 9.8. Wykaż indukcyjnie, że istnieje graf o ciągu stopni $(n, n, n-1, n-1, \ldots, 2, 2, 1, 1)$.

Zadanie 9.9. Niech G będzie grafem (prostym) o co najmniej dwóch wierzchołkach. Wykaż, że G zawiera co najmniej dwa wierzchołki tego samego stopnia. Czy jest to prawda dla multigrafów?

Wskazówka. Skorzystać z zasady szufladkowej Dirichleta.

Przykład 9.10. Przyjmując, że G jest grafem prostym o n wierzchołkach i m krawędziach wykaż indukcyjnie, że $m \leq \frac{n(n-1)}{2}$. Dla jakich grafów zachodzi równość?

Rozwiązanie. Dowód indukcyjny.

(1) $n = 1$. Wówczas graf G jest jednym wierzchołkiem i jako graf prosty ma $0 = \frac{1(1-1)}{2}$ krawędzi.

(2) Załóżmy, że dowolny graf prosty o $1 \leq n' < n$ wierzchołkach ma co najwyżej $\frac{n'(n'-1)}{2}$ krawędzi.

(3) Niech G będzie dowolnym grafem o $n \geq 2$ wierzchołkach. Niech v będzie dowolnym wierzchołkiem G. Usuńmy ten wierzchołek z G wraz z incydentnymi do niego krawędziami. Otrzymany graf G' ma $n' = n-1$ wierzchołków i, z założenia indukcyjnego, co najwyżej $\frac{(n-1)(n-2)}{2}$ krawędzi. Usunięty wierzchołek v w grafie G był sąsiedni z co najwyżej $n-1$ wierzchołkami z grafu G', zatem łączna liczba krawędzi w grafie G nie przekracza $\frac{(n-1)((n-2)}{2} + n - 1 = \frac{n(n-1)}{2}$ krawędzi.

Równość $m = \frac{n(n-1)}{2}$ zachodzi dla grafów pełnych. ♯

Zadanie 9.11. Niech $k \geq 0$. Ustal, dla jakich wartości n istnieje chociaż jeden n-wierzchołkowy graf prosty posiadający dokładnie:

a) k wierzchołków izolowanych;
b) k wierzchołków wiszących (liści).

Zadanie 9.12. Jaka jest maksymalna i minimalna liczba krawędzi w n-wierzchołkowym grafie prostym posiadającym dokładnie:

a) k wierzchołków izolowanych;
b) k wierzchołków wiszących (liści).

9.1 Drogi i cykle

Niech dany będzie dowolny multigraf $G = (V, E)$. *Marszrutą* w G nazywamy skończony ciąg krawędzi postaci $\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_k{-}1, v_k\}$; każda marszruta jednoznacznie wyznacza pewien ciąg wierzchołków $v_0, v_1, \ldots, v_k$. Liczbę krawędzi w marszrucie nazywamy jej *długością*. Marszrutę, w której wszystkie krawędzie są różne, nazywamy *łańcuchem*. Jeśli ponadto wszystkie wierzchołki są różne (za wyjątkiem ewentualnie $v_0 = v_k$), to łańcuch nazywamy *drogą* (prostą) lub *ścieżką*. Łańcuch bądź droga są *zamknięte*, gdy $v_0 = v_k$. Drogę prostą, zamkniętą i zawierającą przynajmniej jedną krawędź nazywamy *cyklem*. Multigraf $G = (V, E)$ jest *spójny*, jeżeli dla dowolnych dwóch wierzchołków $u, v \in V$ istnieje ścieżka łącząca je.

Zadanie 9.13. Znajdź/narysuj graf o pięciu wierzchołkach, który:

a) posiada jeden cykl;
b) posiada trzy cykle;
c) posiada pięć cykli.

Zadanie 9.14. Uzasadnij, że jeżeli każdy z dwóch różnych cykli grafu G zawiera krawędź e, to w G istnieje cykl, który nie zawiera krawędzi e.

Podgrafem multigrafu $G = (V, E)$ nazywamy dowolny multigraf $H = (V', E')$ taki, że $V' \subseteq V$ oraz $E' \subseteq E$. Podgrafem *indukowanym* przez podzbiór wierzchołków $V' \subseteq V$ multigrafu $G = (V, E)$ nazywamy taki podgraf $H = (V', E')$ multigrafu G, że każda krawędź $e \in E$, której obydwa końce należą do V', należy do E' (i żadna inna, z definicji podgrafu).

Zadanie 9.15.

a) Znajdź/narysuj graf o sześciu wierzchołkach i siedmiu krawędziach, który nie posiada podgrafu będącego cyklem długości 4 (ozn. C_4).

b) Znajdź/narysuj graf o sześciu wierzchołkach i dwunastu krawędziach, który nie posiada podgrafu będącego *grafem pełnym* o czterech wierzchołkach (ozn. K_4).

9.2 Izomorfizm grafów

Dwa multigrafy $G_1 = (V_1, E_1)$ i $G_2 = (V_2, E_2)$ są *izomorficzne*, jeśli istnieje wzajemnie jednoznaczna odpowiedniość $h : V_1 \to V_2$ pomiędzy wierzchołkami G_1 i wierzchołkami G_2 taka, że

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{h(u), h(v)\} \in E_2.$$

Twierdzenie 9.16 *Jeżeli dwa multigrafy $G_1 = (V_1, E_1)$ i $G_2 = (V_2, E_2)$ są izomorficzne, to:*

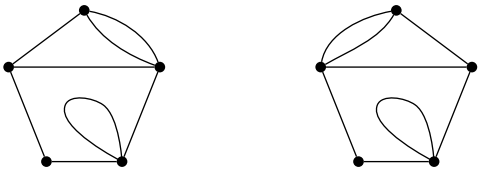
(1) *G_1 i G_2 mają tyle samo wierzchołków: $|V_1| = |V_2|$.*
(2) *G_1 i G_2 mają tyle samo krawędzi: $|E_1| = |E_2|$.*
(3) *dla dowolnego k multigrafy G_1 i G_2 mają tyle samo wierzchołków stopnia k.*

Zadanie 9.17. Narysuj wszystkie grafy ze zbiorem wierzchołków $V = \{a, b, c\}$. Które z nich są izomorficzne? Następnie narysuj wszystkie nieizomorficzne grafy o czterech wierzchołkach.

Zadanie 9.18. Narysuj dwa najmniejsze (w sensie liczby wierzchołków i krawędzi) nieizomorficzne grafy o takiej samej liczbie wierzchołków i krawędzi.

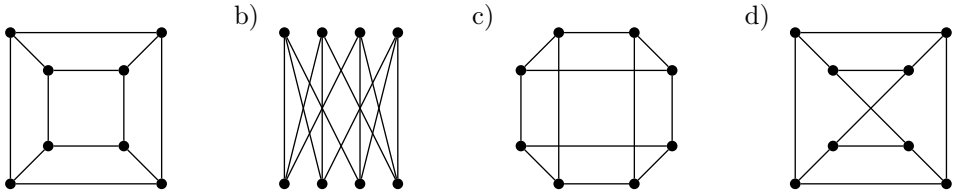
Zadanie 9.19. Wykaż, że poniższe grafy są izomorficzne.

Zadanie 9.20. Wykaż, że poniższe multigrafy nie są izomorficzne.



Zadanie 9.21. Które z poniższych grafów (b)-(d) nie są izomorficzne z grafem (a)? Uzasadnij odpowiedź.

a) b) c) d)



Zadanie 9.22. Istnieją tylko dwa nieizomorficzne grafy o ciągu stopni $(3, 3, 3, 3, 3, 3, 6)$. Wskaż je.

Niech G będzie grafem prostym ze zbiorem wierzchołków V. *Dopełnienie* $\overline{G}$ grafu G jest grafem prostym z tym samym zbiorem wierzchołków V, w którym dwa wierzchołki są sąsiednie wtedy i tylko wtedy, gdy nie są sąsiednie w G. Graf prosty, który jest izomorficzny ze swoim dopełnieniem nazywamy *samodopełniającym*.

Zadanie 9.23. Wykaż, że liczba wierzchołków grafu samodopełniającego wynosi $4k$ lub $4k + 1$.

9.3 Drzewa

Twierdzenie 9.24 *Niech T będzie grafem o n wierzchołkach. Wówczas następujące warunki są równoważne:*

(1) *T jest drzewem.*
(2) *T nie zawiera cykli i ma $n-1$ krawędzi.*
(3) *T jest spójny i ma $n-1$ krawędzi.*
(4) *T jest spójny, ale usunięcie dowolnej krawędzi e rozspaja T (każda krawędź jest* mostem*).*
(5) *Dowolne dwa wierzchołki grafu T połączone są dokładnie jedną drogą.*
(6) *T nie zawiera cykli, lecz dodanie dowolnej nowej krawędzi tworzy dokładnie jeden cykl.*

Zadanie 9.25. Znajdź/narysuj dwa nieizomorficzne drzewa o tym samym ciągu grafowym.

Przykład 9.26. Wykaż, że dowolne drzewo $T = (V, E)$, $|V| \geq 2$, posiada przynajmniej 2 liście.

Rozwiązanie. Załóżmy, że w drzewie istnieje co najwyżej jeden liść, a zatem wszystkie wierzchołki za wyjątkiem co najwyżej jednego są stopnia przynajmniej dwa. Tym samym zachodzi

$$\sum_{v \in V} \deg(v) \geq 2(|V| - 1) + 1 = 2|V| - 1.$$

Ale z drugiej strony, korzystając z zależności $\sum_{v \in V} \deg(v) = 2|E|$ oraz faktu, że w drzewie zachodzi $|E| = |V| - 1$, otrzymujemy $\sum_{v \in V} \deg(v) = 2|V| - 2$ — sprzeczność. ♯

Zadanie 9.27. Niech T będzie drzewem, którego wierzchołki są wyłącznie stopnia 3 lub 1. Jeśli T ma dziesięć wierzchołków stopnia 3, to ile wówczas ma liści?

Zadanie 9.28. W drzewie T średnia stopni wierzchołków jest równa 1.99. Ile krawędzi ma T?

Zadanie 9.29. Wykaż, że jeśli T jest drzewem, w którym wszystkie stopnie wierzchołków są nieparzyste, wówczas liczba krawędzi drzewa T jest również nieparzysta.

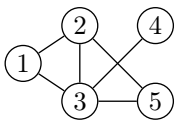
Drzewo spinające (*rozpinające*) multigrafu $G = (V, E)$ to dowolne drzewo $T = (V, E')$ takie, że $E' \subseteq E$. Zauważmy, że T ma taki sam zbiór wierzchołków co G, i każde drzewo spinające multigrafu G jest jego podgrafem. Można wykazać, że każdy spójny multigraf posiada drzewo spinające. W literaturze występują dwa szczególne drzewa spinające — są to drzewa przeszukiwań DFS i BFS, które omówione zostaną w następnej sekcji, natomiast poniżej przedstawiony jest inny prosty algorytm wyznaczania drzewa spinającego.

Algorytm konstrukcji drzewa spinającego.

Niech $G = (V, E)$ będzie spójnym (multi)grafem.

1. Dopóki (multi)graf nie jest drzewem, usuń dowolną krawędź dowolnego cyklu.

Przykład 9.30. Zastosuj powyższy algorytm i wyznacz drzewo spinajacego poniższego grafu.



Rozwiązanie. Zgodnie z algorytmem, wykonujemy:

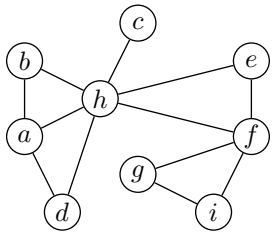
» Rozważamy cykl o wierzchołkach $1, 2, 5, 3$ i usuwamy np. krawędź $\{1, 2\}$.
» Rozważamy cykl o wierzchołkach $2, 3, 5$ i usuwamy np. krawędź $\{3, 5\}$.
» W otrzymanym grafie nie ma już cykli.

Otrzymujemy zatem następujące drzewo spinające $T = (V, E')$, gdzie

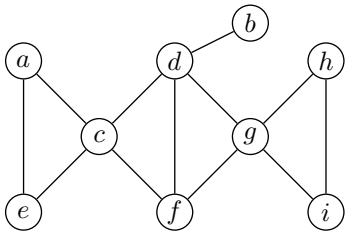
$$V = \{1, 2, 3, 4, 5\} \text{ oraz } E' = \{\{1, 3\}, \{2, 3\}, \{2, 5\}, \{3, 4\}\}. \sharp$$

Zadanie 9.31. Skonstruuj drzewa spinające dla podanych niżej grafów.

a)



b)



Niech $T = (V, E')$ będzie dowolnym drzewem spinającym grafu $G = (V, E)$. Cykl *bazowy/podstawowy* w grafie G jest to cykl, który powstaje po dodaniu dowolnej krawędzi $e \in E$ do drzewa T. Wszystkie tak powstałe cykle tworzą zbiór cykli *fundamentalnych/bazowych/podstawowych*, tzw. *bazę cykli* dla danego drzewa spinającego.

Przykład 9.32. Dla drzewa spinającego skonstruowanego w przykładzie 9.30 zbiór fundamentalnych cykli składa się z dwóch cykli C_1 i C_2, gdzie:

$C_1 = (\{1, 2, 3\}, \{\{1, 3\}, \{2, 3\}, \{1, 2\}\})$,
$C_2 = (\{2, 3, 5\}, \{\{2, 3\}, \{2, 5\}, \{3, 5\}\})$. $\sharp$

Zadanie 9.33. Wyznacz zbiór cykli fundamentalnych dla drzew skontruowanych w zadaniu 9.31.

9.4 Przeszukiwanie grafów w głąb i wszerz — drzewa DFS i BFS

Algorytm przeszukiwania grafu w głąb

Niech $G = (V, E)$ będzie danym grafem spójnym, a $v \in V$ wierzchołkiem początkowym.

1. Odwiedzamy wierzchołek v (zaznaczamy go jako odwiedzony) i wkładamy go na STOS.
2. Dopóki STOS nie jest pusty, powtarzamy:

   Jeżeli v jest wierzchołkiem na wierzchu STOSU, to sprawdzamy, czy istnieje wierzchołek sąsiedni z v, który nie był jeszcze odwiedzony.

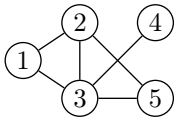
   2.1 Jeżeli u jest takim wierzchołkiem, to odwiedzamy u (zaznaczamy jako odwiedzony) i wkładamy go na STOS.
   2.2 Jeżeli takiego u nie ma, to zdejmujemy v ze STOSU.

Uwaga 1. Jeśli jest kilka wierzchołków do wyboru, to wybieramy zgodnie z ustalonym porządkiem.

Uwaga 2. Wierzchołki na STOSIE w dowolnym kroku tworzą ścieżkę od korzenia do wierzchołka aktualnie odwiedzanego.

Uwaga 3. Jeśli w powyższej procedurze w kroku 2.1, w którym odwiedzamy wierzchołek u, do początkowo pustego zbioru E' krawędzi dodawać będziemy krawędź $\{v, u\}$, to otrzymamy drzewo spinające DFS (ang. *depth-first search*).

Przykład 9.34. Przeszukaj poniższy graf $G = (V, E)$ w głąb poczynając od wierzchołka o etykiecie 3 i skonstruuj odpowiednie drzewo spinające DFS.



Rozwiązanie. Przebieg algorytmu jest następujący.

aktualny wierzchołek	STOS	zbiór krawędzi drzewa DFS
$\underline{3}$	3	$\emptyset$
$\underline{1}$	3,1	$\{\{1,3\}\}$
$\underline{2}$	3,1,2	$\{\{1,3\},\{1,2\}\}$
$\underline{5}$	3,1,2,5	$\{\{1,3\},\{1,2\},\{2,5\}\}$
2	3,1,2	$\{\{1,3\},\{1,2\},\{2,5\}\}$
1	3,1	$\{\{1,3\},\{1,2\},\{2,5\}\}$
3	3	$\{\{1,3\},\{1,2\},\{2,5\}\}$
$\underline{4}$	1,4	$\{\{1,3\},\{1,2\},\{2,5\},\{1,4\}\}$
3	3	$\{\{1,3\},\{1,2\},\{2,5\},\{1,4\}\}$
–	$\emptyset$	$\{\{1,3\},\{1,2\},\{2,5\},\{1,4\}\}$

Zatem wierzchołki były odwiedzane w kolejności $3, 1, 2, 5, 4$ i otrzymaliśmy drzewo spinające DFS $T = (V, E')$, gdzie $V = \{1, 2, 3, 4, 5\}$ oraz $E' = \{\{1,3\},\{1,2\},\{2,5\},\{1,4\}\}$. ♯

Algorytm przeszukiwania grafu wszerz

Niech $G = (V, E)$ będzie danym grafem spójnym, a $v \in V$ wierzchołkiem początkowym.

1. Odwiedzamy wierzchołek v (zaznaczamy go jako odwiedzony) i wstawiamy go do KOLEJKI.
2. Dopóki KOLEJKA nie jest pusta, powtarzamy:
   2.1 Bierzemy wierzchołek v z początku KOLEJKI.
   2.2 Odwiedzamy wszystkie do tej pory jeszcze nie odwiedzone wierzchołki sąsiednie z v (zaznaczamy je jako odwiedzone) i wstawiamy je na koniec KOLEJKI.

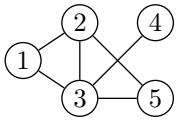
Uwaga 1. Wierzchołki wstawiamy do KOLEJKI np. w kolejności uporządkowania etykiet.

Uwaga 2. Wierzchołki przeszukiwane są w kolejności leżących najbliżej korzenia.

Uwaga 3. Jeśli w powyższej procedurze w kroku 2.2, w którym odwiedzamy wszystkie nieodwiedzone jeszcze wierzchołki sąsiednie do v, do początkowo pustego zbioru E' krawędzi dodawać

będziemy odpowiednie krawędzie $\{v, u\}$, to otrzymamy drzewo spinające BFS (ang. *breath-first search*).

Przykład 9.35. Przeszukaj poniższy graf $G = (V, E)$ wszerz poczynając od wierzchołka o etykiecie 5 i skonstruuj odpowiednie drzewo spinające BFS.



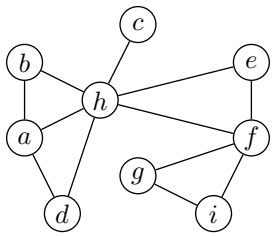
Rozwiązanie. Przebieg algorytmu jest następujący.

aktualny wierzchołek	odwiedzane wierzchołki	KOLEJKA	zbiór krawędzi drzewa DFS
5	5	5	$\emptyset$
5	2,3	2,3	$\{\{2,5\},\{3,5\}\}$
2	1	3,1	$\{\{2,5\},\{3,5\},\{1,2\}\}$
3	4	1,4	$\{\{2,5\},\{3,5\},\{1,2\},\{3,4\}\}$
1	–	4	$\{\{2,5\},\{3,5\},\{1,2\},\{3,4\}\}$
4	–	$\emptyset$	$\{\{2,5\},\{3,5\},\{1,2\},\{3,4\}\}$

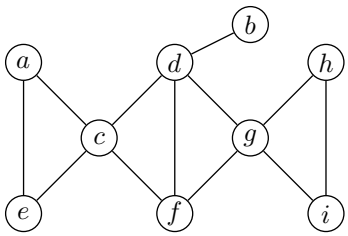
Zatem wierzchołki były odwiedzane w kolejności $5, 2, 3, 1, 4$ i otrzymaliśmy drzewo spinające BFS $T = (V, E')$, gdzie $V = \{1, 2, 3, 4, 5\}$ oraz $E' = \{\{2, 5\}, \{3, 5\}, \{1, 2\}, \{3, 4\}\}$. ♯

Zadanie 9.36. Zastosuj algorytm przeszukiwania w głąb (wszerz) do poniższych grafów i skonstruuj odpowiednie drzewa DFS i BFS; jako wierzchołek początkowy przyjmij wierzchołek o etykiecie a.

a)



b)



Zadanie 9.37.* Niech $v \in V$ będzie wierzchołkiem, z którego startuje algorytm przeszukiwania w głąb grafu $G = (V, E)$. Udowodnij, że dla każdej pary wierzchołków x i y takich, że $\{x, y\} \in E$ mamy, że albo x jest potomkiem y albo y jest potomkiem x w drzewie DFS (inaczej mówiąc, albo y leży na ścieżce z x do v w drzewie BFS albo na odwrót — x leży na ścieżce z y do v).

Zadanie 9.38.* Niech $v \in V$ będzie wierzchołkiem, z którego startuje algorytm przeszukiwania wszerz grafu $G = (V, E)$. Udowodnij, że dla dowolnego wierzchołka $x \in V$ najkrótsza droga z x do v w otrzymanym drzewie BFS jest także najkrótszą drogą z x do v w grafie G.

9.5 Grafy eulerowskie i hamiltonowskie

Niech dany będzie spójny multigraf $G = (V, E)$. Mówimy, że G jest *eulerowski*, jeśli istnieje łańcuch zamknięty zawierający każdą krawędź multigrafu; taki łańcuch nazywamy *cyklem Eulera*. Analogicznie, mówimy, że G jest *półeulerowski*, jeśli istnieje łańcuch zawierający każdą krawędź grafu; taki łańcuch nazywamy łańcuchem Eulera.

Twierdzenie 9.39

a) *Spójny multigraf $G = (V, E)$ jest eulerowski wtedy i tylko wtedy, gdy każdy jego wierzchołek jest parzystego stopnia.*

b) *Spójny multigraf G jest półeulerowski wtedy i tylko wtedy, gdy posiada co najwyżej dwa wierzchołki nieparzystego stopnia, z czego jeden z nich jest początkiem łańcucha Eulera, a drugi jego końcem.*

Niech dany będzie spójny (multi)graf $G = (V, E)$. Mówimy, że G jest *hamiltonowski*, jeśli istnieje cykl, który przechodzi przez każdy wierzchołek dokładnie raz; taki cykl nazywamy cyklem *Hamiltona*. Analogicznie, mówimy, że G jest *półhamiltonowski*, jeśli zawiera ścieżkę przechodzącą przez każdy wierzchołek dokładnie raz; taką ścieżkę nazywamy ścieżką *Hamiltona*.

Zadanie 9.40. Ustal, dla jakich wartości n graf pełny K_n posiada:

a) cykl Eulera;
b) cykl Hamiltona.

Zadanie 9.41. Ustal, dla jakich wartości n graf pełny K_n z usuniętą jedną krawędzią posiada:

a) cykl Eulera;
b) łańcuch Eulera;
c) cykl Hamiltona;
d) ścieżkę Hamiltona.

Przypomnijmy, że graf $G = (V, E)$ jest grafem *dwudzielnym*, jeżeli jego zbiór wierzchołków można rozbić na dwa rozłączne podzbiory V_1 i V_2 takie, że $V_1 \cup V_2 = V$ oraz każda krawędź $e \in E$ ma końce w obu zbiorach, tj. $|e \cap V_1| = |e \cap V_2| = 1$. *Pełny graf dwudzielny* $K_{m,n} = (V_1 \cup V_2, E)$ jest to graf, w którym $|V_1| = m$ i $|V_2| = n$ oraz krawędzie łączą każdy wierzchołek z V_1 z każdym wierzchołkiem z V_2, tj. $E = \{\{x, y\} : x \in V_1 \text{ oraz } y \in V_2\}$.

Zadanie 9.42. Ustal, dla jakich wartości n i m dwudzielny graf pełny $K_{m,n}$ posiada:

a) cykl Eulera;
b) cykl Hamiltona.

Czy dwudzielny graf G o nieparzystej liczbie wierzchołków może być grafem hamiltonowskim?

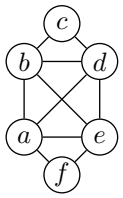
Algorytm znajdowania cyklu Eulera (o ile taki cykl istnieje)

Niech $G = (V, E)$ będzie spójnym multigrafem o wszystkich wierzchołkach parzystego stopnia.

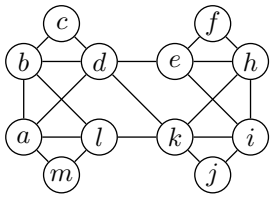
1. Zaczynamy od dowolnego wierzchołka $v \in V$.
2. Powtarzamy, aż przejdziemy wszystkie krawędzie:
   2.1 Jeżeli z bieżącego wierzchołka x odchodzi tylko jedna krawędź, to przechodzimy wzdłuż tej krawędzi do następnego wierzchołka i usuwamy tą krawędź wraz z wierzchołkiem x.
   2.2 W przeciwnym wypadku, jeżeli z x odchodzi więcej krawędzi, to wybieramy tą krawędź, której usunięcie nie rozspójnia nam grafu, i przechodzimy wzdłuż tej krawędzi do następnego wierzchołka, a następnie usuwamy tą krawędź z grafu.

Zadanie 9.43. Czy w danych niżej grafach istnieje cykl/łańcuch Eulera? Jeśli tak, wyznacz go.

a)



b)



Zadanie 9.44. Czy poniższe kamyki do gry w domino można ułożyć w ciąg tak, aby się „zamknął”? Jeśli tak, wskaż możliwe ułożenie.

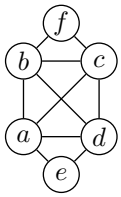
1	2		1	3		1	4		1	5
2	3		2	4		2	5			
3	4		3	5						
4	5									

Algorytm z nawrotami znajdowania drogi Hamiltona (o ile taka droga istnieje)

Niech $G = (V, E)$ będzie spójnym grafem i pewnym wyróżnionym wierzchołkiem $v \in V$.

1. Wkładamy v na STOS.
2. Powtarzamy:
   - 2.1 Jeżeli u jest wierzchołkiem na wierzchu stosu, to szukamy wierzchołka w o najniższym możliwym numerze (najwcześniejszego przy ustalonym porządku wierzchołków grafu) sąsiedniego z u i nie występującego na STOSIE, jednakże przy założeniu, że wierzchołek w jest „większy” od wierzchołka zdjętego krok wcześniej ze STOSU (o ile był taki).
   - 2.2 Jeśli takie w znajdziemy, to wkładany je na stos — jeżeli dotychczasowy STOS tworzy drogę Hamiltona, to KONIEC.
   - 2.3 Jeżeli takiego w nie znaleźliśmy, to zdejmujemy u ze stosu.

Przykład 9.45. Wypisz 25 kolejnych kroków działania algorytmu z nawrotami znajdowania drogi Hamiltona dla poniższego grafu przy założeniu, że wierzchołkiem początkowym jest wierzchołek o etykiecie a.



Rozwiązanie. Działanie algorytmu z nawrotami ilustruje poniższa tabela.

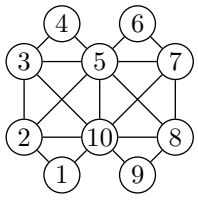
	aktualny wierzchołek	STOS
1	a	a
2	b	a, b
3	c	a, b, c
4	d	a, b, c, d
5	e	a, b, c, d, e
6	d	a, b, c, d
7	c	a, b, c
8	f	a, b, c, f
9	c	a, b, c
10	b	a, b
11	d	a, b, d
12	c	a, b, d, c
13	f	a, b, d, c, f
14	c	a, b, d, c
15	d	a, b, d
16	e	a, b, d, e
17	d	a, b, d
18	b	a, b
19	f	a, b, f
20	c	a, b, f, c
21	d	a, b, f, c, d
22	e	a, b, f, c, d, e
		KONIEC

A zatem algorytm z nawrotami zwróci drogę Hamiltona postaci a, b, f, c, d, e. ♯

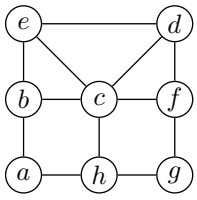
Zadanie 9.46. Wypisz 15 kolejnych kroków działania algorytmu z nawrotami znajdowania drogi Hamiltona dla poniższych grafów przy założeniu, że wierzchołkiem początkowym jest:

a) wierzchołek o etykiecie 5;
b) wierzchołek o etykiecie a.

a)



b)



Problem stwierdzenia, czy w danym grafie $G = (V, E)$ istnieje droga Hamiltona, jest problemem NP-zupełnym, tzn. nie istnieje deterministyczny algorytm rozstrzygający ten problem w czasie wielomianowym, o ile P≠NP. Zauważmy, że nie wyklucza to istnienia niewielomianowego algorytmu i właśnie przykładem takiego algorytmu jest omawiany wyżej algorytm z nawrotami.

Zadanie 9.47. Wskaż graf o n wierzchołkach, dla którego czas działania powyższego algorytmu z nawrotami jest niewielomianowy.

Wskazówka. Aby oszacować z dołu czas działania dla danego grafu, można oszacować tylko np. ile w sumie razy wkładaliśmy jakikolwiek z wierzchołków na stos.

9.6 Zadania różne

Zadanie 9.48. Udowodnij, że izomorfizm grafów jest relacją równoważności.

Graf *regularny* to graf, w którym każdy wierzchołek jest tego samego stopnia; w szczególności, graf r-regularny, $r \geq 0$, to graf, w którym każdy wierzchołek jest stopnia r.

Zadanie 9.49. Niech n będzie liczbą naturalną, a m nieujemną liczbą całkowitą. Wyznacz stopień n-wierzchołkowego grafu regularnego o m krawędziach.

Przykład 9.50. Mamy dowolny graf $G = (V, E)$. Na ile sposobów można pokolorować dwoma kolorami jego wierzchołki? Na ile sposobów można pokolorować dwoma kolorami jego wierzchołki tak, aby z góry wybrana krawędź $e = \{u, v\}$ miała końce w różnych kolorach?

Rozwiązanie. Mamy $|V|$ wierzchołków. Skoro każdemu wierzchołkowi można przypisać dwa różne kolory, np. 0 i 1, to liczba pokolorowań wynosi $2^{|V|}$.

Analogicznie, jeśli końce ustalonej krawędzi $e = \{u, v\}$ mają mieć różne kolory, wówczas albo kolor u wynosi 0, a kolor v wynosi 1, albo na odwrót, czyli kolor u wynosi 1, a kolor v wynosi 0 — natomiast pozostałe wierzchołki mogą otrzymać dowolny kolor. Tym samym w tym przypadku liczba możliwych pokolorowań wynosi $2 \cdot 2^{|V|-2} = 2^{|V|-1}$. ♯

Zadanie 9.51. Mamy dowolny graf $G = (V, E)$. Na ile sposobów można pokolorować p kolorami jego wierzchołki? Na ile sposobów można pokolorować p kolorami jego wierzchołki tak, aby z góry wybrana krawędź $e = \{u, v\}$ miała końce w różnych kolorach?

Zadanie 9.52. Rozważmy dowolne losowe pokolorowanie $k+1 \geq 1$ kolorami wierzchołków grafu $G = (V, E)$ i niech π będzie dowolną ścieżką prostą długości k w grafie G (o ile ścieżka taka istnieje). Jakie jest prawdopodobieństwo, że wszystkie wierzchołki ścieżki π są różnych kolorów?

Zadanie 9.53. Wykaż, że jeśli w spójnym grafie G średnia stopni wierzchołków jest większa niż dwa, wówczas G posiada przynajmniej dwa cykle. Co można powiedzieć o liczbie cykli, gdy (a) średnia stopni wierzchołków jest mniejsza niż 2; (b) średnia stopni wierzchołków jest równa 2?

Zadanie 9.54. Wykaż, że jeśli n-wierzchołkowy graf (prosty) G o m krawędziach spełnia warunek $m > \binom{n-1}{2}$, to G jest spójny.

> *Wskazówka.* Dowód przez sprzeczność — próbujemy oszacować maksymalną liczbę krawędzi w grafie zakładając, że graf ma przynajmniej dwie składowe spójności, z których jedna ma $k \geq 1$ wierzchołków.

9.7 Grafy ważone — minimalne drzewo spinające

Niech $G = (V, E, w)$ będzie *grafem ważonym*, tzn. każdej krawędzi $e \in E$ przyporządkowana jest pewna waga $w(e)$. Problem *Minimalnego Drzewa Spinającego* [MDS] definiujemy jako znalezienie drzewa spinającego $T = (V, E')$ w grafie G o minimalnej sumie ważonej

$$\sum_{e \in E'} w(e).$$

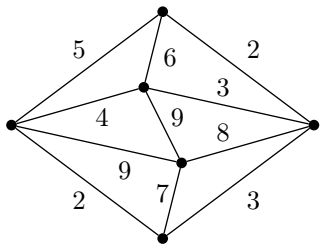
Minimalne drzewo spinające znajduje zastosowanie np. przy wyznaczeniu „najtańszej" sieci dróg, torów kolejowych, itp., która łączy danych n miast.

Algorytm konstrukcji minimalnego drzewa spinającego (algorytm Kruskala, 1956)

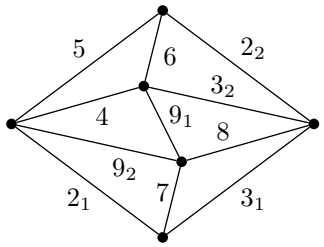
Niech $G = (V, E, w)$ będzie spójnym grafem ważonym z funkcją wagi $w\colon E \to R$.

1. $T := (V, E')$, gdzie $E' := \emptyset$.
2. Posortuj krawędzie grafu G w kolejności niemalejących wag.
3. Dla każdej krawędzi $e \in E$:
   jeśli dodanie rozważanej krawędzi e nie utworzy cyklu w T, wówczas $E' := E' \cup \{e\}$.

Przykład 9.55. Znajdź minimalne drzewo spinające dla podanego niżej grafu.



Rozwiązanie. Posortowany ciąg krawędzi wygląda następująco: $2, 2, 3, 3, 4, 5, 6, 7, 8, 9, 9$. Jako że niektóre wagi krawędzi powtarzają się, należy je rozróżnić np. dodając odpowiedni indeks dolny — otrzymujemy ciąg $2_1, 2_2, 3_1, 3_2, 4, 5, 6, 7, 8, 9_1, 9_2$ — patrz poniższy rysunek.

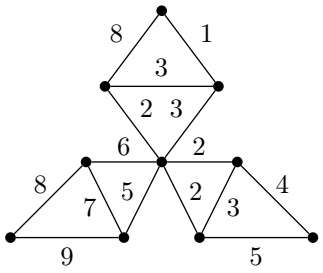


Dla ułatwienia ilustracji działania algorytmu utożsamiamy wagi krawędzi z samymi krawędziami. Przebieg algorytmu jest następujący.

rozpatrywana krawędź	cykl?	krawędzie drzewa
2_1	–	2_1
2_2	–	$2_1, 2_2$
3_1	–	$2_1, 2_2, 3_1$
3_2	–	$2_1, 2_2, 3_1, 3_2$
4	+	$2_1, 2_2, 3_1, 3_2$
5	+	$2_1, 2_2, 3_1, 3_2$
6	+	$2_1, 2_2, 3_1, 3_2$
7	–	$2_1, 2_2, 3_1, 3_2, 7$
8	+	$2_1, 2_2, 3_1, 3_2, 7$
9_1	+	$2_1, 2_2, 3_1, 3_2, 7$
9_2	+	$2_1, 2_2, 3_1, 3_2, 7$

Zauważmy, że skoro graf ma 6 wierzchołków, a z definicji drzewo spinające ma 5 krawędzi, wykonywanie algorytmu można było już przerwać, gdy dodaliśmy 5-tą krawędź o wadze 7. ♯

Zadanie 9.56. Znajdź minimalne drzewo spinające dla podanego niżej grafu.



Zadanie 9.57. Poniższa tabela przedstawia odległości pomiędzy 5 miastami A,B,C,D i E. Chcemy tak połączyć miasta, aby z każdego miasta można było dostać się do innego, niekoniecznie drogą bezpośrednią, jednakże chcemy wydać jak najmniej pieniędzy. Jaki jest minimalny koszt budowy takiej sieci dróg, jeżeli 1 km drogi kosztuje 1000000 PLN?

	A	B	C	D	E
A	–	2	6	3	7
B	2	–	6	4	8
C	6	6	–	5	8
D	3	4	5	–	9
E	7	8	8	9	–

Zadanie 9.58.* Niech $G = (V, E, w)$ będzie eulerowskim grafem ważonym takim, że

$$w(G) = \sum_{e \in E(G)} w(e) > 0.$$

Wykaż, że w G istnieje cykl C taki, że $w(C) = \sum_{e \in C} w(e) > 0$.

9.8 Grafy ważone — najkrótsze drogi w grafie

Rozważmy graf ważony $G = (V, E, w)$ z dodatnią funkcją kosztu, tj. $w\colon E \to \mathbb{R}^+$. Dla prostoty zakładamy, że jeśli $e \notin E$, to $w(e) = \infty$. Dla każdej drogi $v_0 v_1 \dots v_k$ w grafie zdefiniujmy jej *długość* jako sumę długości krawędzi, czyli

$$\sum_{i=1}^{k} (w(\{v_{i-1}, v_i\})).$$

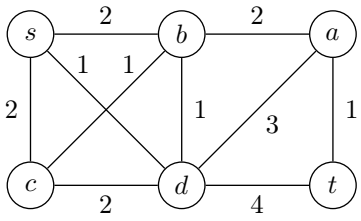
Jeżeli $k = 0$, wówczas droga składa się z pojedynczego wierzchołka i przyjmujemy wtedy, że jej długość wynosi 0.

Algorytm wyznaczania długości najkrótszych dróg (algorytm Dijkstry)

Niech $s \in V$ będzie ustalonym wierzchołkiem ważonego grafu $G = (V, E, w)$ o dodatniej funkcji kosztu. Algorytm na wyjściu zwraca macierz D, gdzie dla wierzchołka $v \in V$ wartość $D[v]$ jest długością najkrótszej ścieżki z s do v.

1. $D[s] := 0$.
2. $\bar{V} := V \setminus \{s\}$.
3. Dla każdego $v \in \bar{V}$ podstaw $D[v] := w(\{s, v\})$.
4. Dopóki $\bar{V} \neq \emptyset$, wykonuj:
   4.1 Wybierz wierzchołek $u \in \bar{V}$ taki, że $D[u] = \min_{x \in \bar{V}} D[x]$.
   4.2 $\bar{V} := \bar{V} \setminus \{u\}$.
   4.3 Dla każdego $v \in \bar{V}$ podstaw $D[v] := \min(D[v], D[u] + w(\{u, v\}))$.

Przykład 9.59. Wyznacz drzewo najkrótszych dróg w podanym niżej ważonym grafie $G = (V, E, w)$ dla wierzchołka początkowego s.



Rozwiązanie. Poniższa tabela ilustruje jak w kolejnych iteracjach zewnętrznej pętli algorytmu Dijkstry wybierany jest wierzchołek u oraz jak przedstawia się zbiór $\bar{V}$ oraz macierz D.

Iteracja	u	$\bar{V}$	$D[s]$	$D[a]$	$D[b]$	$D[c]$	$D[d]$	$D[t]$
0		$\{a, b, c, d, t\}$	0	∞	2	2	$\underline{1}$	∞
1	d	$\{a, b, c, t\}$	0	4	$\underline{2}$	2	1	5
2	b	$\{a, c, t\}$	0	3	2	$\underline{2}$	1	5
3	c	$\{a, t\}$	0	$\underline{3}$	2	2	1	5
4	a	$\{t\}$	0	3	2	2	1	$\underline{4}$
5	t	$\emptyset$	0	3	2	2	1	4

♯

Zauważmy, że algorytm Dijkstry wyznacza tylko macierz najkrótszych odległości, nie zapamiętując w czasie wykonywania żadnych dodatkowych informacji. Aby wyznaczyć najkrótszą drogę z wierzchołka s do wybranego wierzchołka v można albo zmodyfikować algorytm tak, aby za każdym razem, kiedy usuwamy wierzchołek u ze zbioru $\bar{V}$, dodawał on odpowiednią krawędź do konstruowanego drzewa najkrótszych dróg, albo też skorzystać bezpośrednio z wyznaczonej macierzy D. A dokładnie, załóżmy, że interesuje nas wyznaczenie najkrótszej ścieżki z wierzchołka s do t w grafie $G = (V, E, w)$ z przykładu 9.59.

Najkrótszą drogę wyznaczamy od końca — najpierw szukamy przedostatniego wierzchołka tej drogi, potem trzeciego od końca i tak dalej.

- Przedostatni wierzchołek x najkrótszej drogi spełnia równość $D[t] = D[x] + w(\{x, t\})$. W naszym przykładzie (tylko) wierzchołek $x = a$ spełnia tą równość:

  $$4 = D[t] = D[a] + w(\{a, t\}) = 3 + 1.$$

  A zatem przedostatnim wierzchołkiem jest wierzchołek a.

- Trzeci wierzchołek y od końca najkrótszej drogi z s do t — a przedostatni wierzchołek najkrótszej drogi z s do a — spełnia równość $D[a] = D[y]+w(\{y, a\})$. W naszym przykładzie (tylko) wierzchołek $y = b$ spełnia tą równość:

$$3 = D[a] = D[b] + w(\{b, a\}) = 2 + 1.$$

  A zatem pozostaje na znaleźć najkrótszą drogę z s do b.

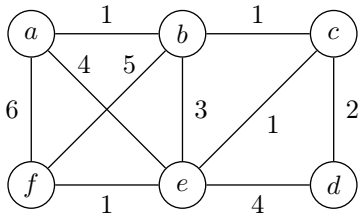
- Czwarty wierzchołek z od końca najkrótszej drogi z s do t — a przedostatni wierzchołek najkrótszej drogi z s do b — spełnia równość $D[b] = D[z]+w(\{z, b\})$. W naszym przykładzie (tylko) wierzchołek $y = s$ spełnia tą równość:

$$2 = D[b] = D[s] + w(\{s, b\}) = 0 + 2.$$

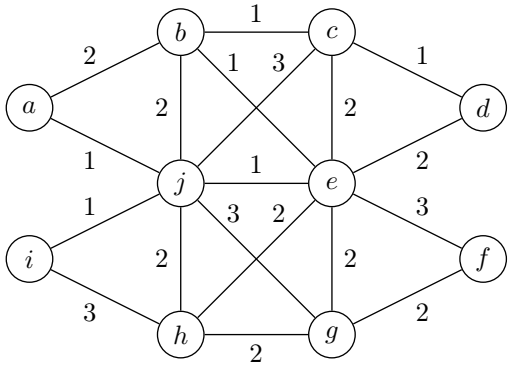
W konsekwencji najkrótsza droga z s do t długości 4 wiedzie przez wierzchołki s, b, a i t.

Zadanie 9.60. W poniższych grafach znajdź długość najkrótszej drogi z wierzchołka a do f, a następnie wyznacz tę drogę.

a)



b)



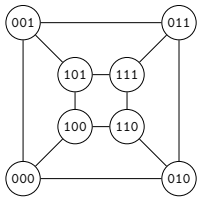
9.9 Rozsyłanie wiadomości w hiperkostce

Graf zwany *hiperkostką* H_k zdefiniowany jest rekurencyjnie. H_1 składa się z dwóch wierzchołków połączonych krawędzią. Natomiast hiperkostkę H_k wymiaru k budujemy z dwóch kostek H_{k-1} wymiaru $k - 1$. W pierwszej kostce etykietujemy wierzchołki dopisując `0` na początku nazwy każdego wierzchołka, natomiast w drugiej kostce etykietujemy wierzchołki dopisując `1` na początek. Następnie łączymy krawędziami odpowiadające sobie wierzchołki z obu kopii, czyli wierzchołek `0x` jest połączony z wierzchołkiem `1x` dla każdego `x` z $\{\texttt{0}, \texttt{1}\}^{k-1}$.

Protokół rozsyłania wiadomości w hiperkostce H_k.

1. Na początku wiadomość otrzymuje wierzchołek $\texttt{0}^k$.
2. Dla każdego i od 1 do k, wykonuj:
   2.1 Każdy wierzchołek o etykiecie $x < 2^{i-1}$
   przekazuje wiadomość do wierzchołka o etykiecie $x + 2^{i-1}$.

Przykład 9.61. Prześledźmy działanie powyższego algorytmu na hiperkostce H_3.



Hiperkostka H_3.

- W pierwszej iteracji, dla $i = 1$, wierzchołek 000 przekazuje wiadomość do 001.
- W drugiej iteracji, dla $i = 2$, wierzchołek 000 przekazuje wiadomość do 010, a wierzchołek 001 do 011.
- W trzeciej iteracji, dla $i = 3$, wierzchołek 000 przekazuje wiadomość do 100, wierzchołek 001 do 101, wierzchołek 010 do 110, a wierzchołek 011 do 111. ♯

Zadanie 9.62. Prześledź działanie algorytmu rozsyłania wiadomości na hiperkostkach H_4.

Protokół zbierania wiadomości w hiperkostce H_k.

1. Dla każdego i od 1 do k, wykonuj:
   1.1 Każdy wierzchołek o etykiecie $x = 0^{i-1}1\sigma$, gdzie $\sigma \in \{0,1\}^{k-i}$, przekazuje zebrane dane do wierzchołka o etykiecie $0^{i-1}0\sigma$.

Przykład 9.63. Prześledźmy działanie powyższego algorytmu na hiperkostce H_3.

- W pierwszej iteracji, dla $i = 1$, wierzchołek 100 przekazuje dane do 000, wierzchołek 101 do 001, wierzchołek 110 do 010, a wierzchołek 111 do 011.
- W drugiej iteracji, dla $i = 2$, wierzchołek 010 przekazuje wszystkie dane (swoje i otrzymane) do 000, a wierzchołek 011 do 001.
- W trzeciej iteracji, dla $i = 3$, wierzchołek 001 przekazuje zebrane wiadomości do 000. ♯

Zadanie 9.64. Prześledź działanie algorytmu zbierania wiadomości na hiperkostce H_4.

9.10 Pytania powtórzeniowe

Zadanie 9.65. Które z poniższych stwierdzeń jest prawdziwe? (Odpowiedź: TAK/NIE)

a) Relacja sąsiedztwa grafu prostego jest relacją symetryczną.
b) Ciąg stopni grafu prostego może być ciągiem rosnącym.
c) Ciąg stopni multigrafu może być ciągiem rosnącym.
d) Podgraf indukowany w niepustym grafie jest niepustym grafem.
e) Suma wyrazów ciągu grafowego musi być parzysta.
f) Podgraf indukowany w grafie o minimalnym stopniu $\delta > 0$ jest niepustym grafem.
g) Grafy izomorficzne mają identyczną liczbę krawędzi i wierzchołków.
h) Grafy izomorficzne mają identyczną liczbę wierzchołków wiszących.

i) Grafy o identycznej liczbie krawędzi, wierzchołków i wierzchołków wiszących są izomorficzne.
j) Ciągi stopni grafów izomorficznych są identyczne.
k) Grafy o identycznych ciągach stopni są izmorficzne.
l) Grafy o identycznej liczbie krawędzi, wierzchołków, wierzchołków wiszących i ciągach stopni są izomorficzne.
m) Spójne grafy regularne o identycznej liczbie wierzchołków i krawędzi są izomorficzne.

Odpowiedzi do zadań

9.7.

a) Tak. b) Tak. c) Nie. d) Tak.

9.8. Dowód indukcyjny.

(1.a). $n = 1$. Wówczas graf G jest pojedynczą krawędzią, ciąg stopni: $(1, 1)$.
(1.b). $n = 2$. Wówczas graf G jest ścieżką P_4, ciąg stopni: $(1, 1, 2, 2)$.
(2). Załóżmy, że ciąg stopni $(1, 1, 2, 2, \ldots, n', n')$ jest grafowy dla dowolnego $n' < n$.
(3). Rozważmy ciąg $(1, 1, 2, 2, \ldots, n, n)$, gdzie $n > 2$. Z założenia indukcyjnego istnieje graf G' realizujący ciąg grafowy $(1, 1, 2, 2, \ldots, n-2, n-2)$. Najpierw dodajmy do G' dwa nowe wierzchołki o stopniach 0 (ciąg $(0, 0, 1, 1, 2, 2, \ldots, n-2, n-2)$ jest również grafowy), a następnie dodajmy kolejne dwa wierzchołki, połączmy je krawędzią, oraz każdy z nich połączmy z każdym, ale po jednym tylko (i różnym) z wierzchołków stopnia $0, 1, 2, 3, \ldots, n-2$. Stopnie wszystkich wierzchołków należących do G' wzrosły o jeden, dwa dodane na początku wierzchołki stały się liśćmi, a dwa dodane ostatnio wierzchołki są stopnia n. Zatem otrzymany graf G ma ciąg stopni $(1, 1, 2, 2, \ldots, n-1, n-1, n, n)$.

9.9. Wystarczy zastosować zasadę szufladkową. Oczywiście w grafie prostym o n wierzchołkach nie może zaistnieć sytuacja, że jakiś wierzchołek jest stopnia 0 (nie jest sąsiedni z żadnym z wierzchołków), a jakiś inny stopnia $n-1$ (jest sąsiedni ze wszystkimi). Zatem dopuszczalne są albo stopnie $0, 1, \ldots, n-2$ albo $1, \ldots, n-1$. Jako że mamy n wierzchołków i tylko $n-1$ możliwych wartości stopni (w każdej z dwóch sytuacji), zatem istnieją dwa wierzchołki o tym samym stopniu.

9.10.

a) $n = k$ oraz $n \geq k + 2$.

b) k parzyste: $n \geq k$;
$k = 1$: $n \geq 4$;
$k \geq 3$ nieparzyste: $n \geq k + 1$.

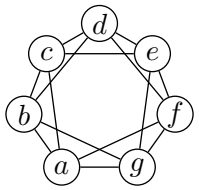
9.11.

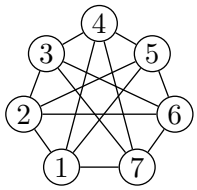
a) $n = k$: $\min = \max = 0$.
$n \geq k + 2$: $\min = \lceil \frac{n-k}{2} \rceil$, $\max = \frac{(n-k)(n-k-1)}{2}$.

b) k parzyste: $\min = \frac{k}{2}$, $\max = k + \frac{(n-k)(n-k-1)}{2}$.
$k = 1$, $n \geq 4$: $\min = 4$, $\max = 1 + \frac{(n-k)(n-k-1)}{2}$.
$k \geq 3$ nieparzyste, $n \geq k + 1$: $\min = \lceil \frac{k}{2} \rceil + 1$, $\max = k + \frac{(n-k)(n-k-1)}{2}$.

9.14. Niech $e = \{x, y\}$ będzie rozważaną krawędzią, a $C_1 = (V_1, E_1)$ i $C_2 = (V_2, E_2)$ dowolnymi różnymi cyklami zawierającymi krawędź e. Wówczas zbiór krawędzi $E_3 = E_1 \otimes E_2 = (E_1 \cup E_2) \setminus (E_1 \cap E_2)$ wraz z końcami tych krawędzi tworzy cykl C_3, który nie zawiera krawędzi e.

9.19. Rozważmy następujące etykietowanie grafów $G_1 = (V_1, E_1)$ i $G_2 = (V_2, E_2)$.

G_1 

G_2 

Zdefiniujmy funkcję h następująco:

$$h(a) = 1,\ h(b) = 4,\ h(c) = 7,\ h(d) = 3,\ h(e) = 6,\ h(f) = 2,\ h(g) = 5.$$

Zachodzi:

$$\begin{aligned}
\{a,b\} \in E_1 &\quad\Leftrightarrow\quad \{h(a),h(b)\} = \{1,4\} \in E_2;\\
\{a,c\} \in E_1 &\quad\Leftrightarrow\quad \{h(a),h(c)\} = \{1,7\} \in E_2;\\
\{a,f\} \in E_1 &\quad\Leftrightarrow\quad \{h(a),h(f)\} = \{1,2\} \in E_2;\\
\{a,g\} \in E_1 &\quad\Leftrightarrow\quad \{h(a),h(g)\} = \{1,5\} \in E_2;\\
\{b,c\} \in E_1 &\quad\Leftrightarrow\quad \{h(b),h(c)\} = \{4,7\} \in E_2;\\
\{b,d\} \in E_1 &\quad\Leftrightarrow\quad \{h(b),h(d)\} = \{4,3\} \in E_2;\\
\{b,g\} \in E_1 &\quad\Leftrightarrow\quad \{h(b),h(g)\} = \{4,5\} \in E_2;\\
\{c,d\} \in E_1 &\quad\Leftrightarrow\quad \{h(c),h(d)\} = \{7,3\} \in E_2;\\
\{c,e\} \in E_1 &\quad\Leftrightarrow\quad \{h(c),h(e)\} = \{7,6\} \in E_2;\\
\{d,e\} \in E_1 &\quad\Leftrightarrow\quad \{h(d),h(e)\} = \{3,6\} \in E_2;\\
\{d,f\} \in E_1 &\quad\Leftrightarrow\quad \{h(d),h(f)\} = \{3,2\} \in E_2;\\
\{e,f\} \in E_1 &\quad\Leftrightarrow\quad \{h(e),h(f)\} = \{6,2\} \in E_2;\\
\{e,g\} \in E_1 &\quad\Leftrightarrow\quad \{h(e),h(g)\} = \{6,5\} \in E_2;\\
\{f,g\} \in E_1 &\quad\Leftrightarrow\quad \{h(f),h(g)\} = \{2,5\} \in E_2.
\end{aligned}$$

A tym samym h jest izomorfizmem — grafy te są izomorficzne.

9.20. Załóżmy, że grafy te są izomorficzne. Jako że w każdym z grafów istnieje dokładnie jedna pętla, izomorfizm musi przekształcać odpowiednie te wierzchołki w siebie — oznaczmy je przez a_1 (w grafie pierwszym) oraz a_2 (w grafie drugim). Następnie, skoro wiemy już, że w pierwszym grafie wierzchołek a_1 musi odpowiadać wierzchołkowi a_2 w grafie drugim, to izomorfizm musi zachować własności ich sąsiadów, a w szczególności także ich stopnie. Ale a_1 jest sąsiedni do dwóch wierzchołków stopnia 2 oraz 4, podczas gdy a_2 jest sąsiedni do dwóch wierzchołków stopnia 2 oraz 3. A zatem niemożliwym jest takie przypisanie sobie tych wierzchołków, aby zachować

odpowiedniość pomiędzy ich stopniami. Otrzymujemy tym samym sprzeczność z założeniem, że grafy są izomorficzne.

9.21. (b) i (c) tak; (d) nie, bo graf ten posiada nieparzysty cykl, których brak w (a), a izomorfizm zachowuje długości cykli.

9.22. Z definicji izomorfizmu wynika, że G i $\overline{G}$ mają tyle samo krawędzi — załóżmy, że m. Jako że suma G i $\overline{G}$ jest grafem pełnym, stąd $2m = \frac{n(n-1)}{2}$. Zatem $m = \frac{n(n-1)}{4}$. Ale n i $n-1$ są kolejnymi liczbami, zatem niemożliwe jest, aby 2 dzieliła każdą z nich, co daje, że albo $4|n$ albo $4|n+1$, czyli $n = 4k$ lub $n = 4k+1$.

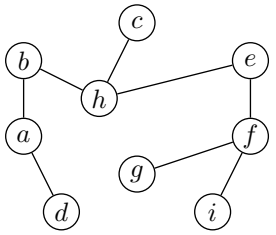
9.27. Z faktu 9.1 otrzymujemy, że $10 \cdot 3 + l \cdot 1 = 2m$, gdzie l jest liczbą liści. Z drugiej strony, jako że T jest drzewem, $2m = 2(n-1) = 2n-2 = 2 \cdot (10+l) - 2$. Tym samym otrzymujemy, że $l = 12$.

9.28. Z treści oraz z faktu 9.1 mamy, że $\frac{1}{n}\sum_{v \in V} \deg(v) = \frac{2(n-1)}{n} = 1.99$. Tym samym, po przekształceniach, otrzymujemy $n = 200$.

9.29. Z faktu 9.1 otrzymujemy, że liczba wierzchołków nieparzystego stopnia jest parzysta, a zatem n jest parzyste, co daje $m = n-1$ nieparzyste.

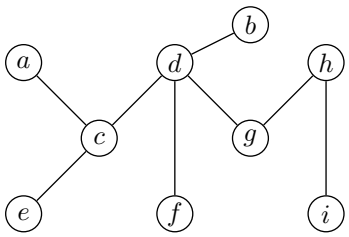
9.31.

a) Np.:



Drzewo spinające $T = (V, E)$, gdzie
$V = \{a, b, c, d, e, f, g, h, i\}$ oraz
$E = \{\{a, b\}, \{a, d\}, \{b, h\}, \{c, h\}, \{e, h\}, \{e, f\}, \{f, g\}, \{f, i\}\}$.

b) Np.:



Drzewo spinające $T = (V, E)$, gdzie
$V = \{a, b, c, d, e, f, g, h, i\}$ oraz
$E = \{\{a, c\}, \{b, d\}, \{c, e\}, \{c, d\}, \{d, f\}, \{d, g\}, \{g, h\}, \{h, i\}\}$.

9.33. Dla przykładowych drzew spinających skonstruowanych w rozwiązaniu zadania 31 zbiór cykli wyndamentalnych składa się z:

a) czterech cykli C_1, C_2, C_3 oraz C_4, gdzie

$C_1 = (\{a,b,d,h\}, \{\{a,b\},\{b,h\},\{d,h\},\{a,d\}\})$,
$C_2 = (\{a,b,h\}, \{\{a,b\},\{b,h\},\{a,h\}\})$,
$C_3 = (\{e,f,h\}, \{\{e,f\},\{f,h\},\{e,h\}\})$,
$C_4 = (\{f,g,i\}, \{\{f,g\},\{g,i\},\{f,i\}\})$.

b) czterech cykli C_1, C_2, C_3 oraz C_4, gdzie

$C_1 = (\{a,c,e\}, \{\{a,c\},\{c,e\},\{a,e\}\})$,
$C_2 = (\{c,d,f\}, \{\{c,d\},\{d,f\},\{c,f\}\})$,
$C_3 = (\{d,f,g\}, \{\{d,f\},\{f,g\},\{d,g\}\})$,
$C_4 = (\{g,h,i\}, \{\{g,h\},\{h,i\},\{g,i\}\})$.

9.36.

a) DFS:

	STOS	zbiór krawędzi drzewa DFS
$\underline{a}$	a	$\emptyset$
$\underline{b}$	a,b	$\{\{a,b\}\}$
$\underline{h}$	a,b,h	$\{\{a,b\},\{b,h\}\}$
$\underline{c}$	a,b,h,c	$\{\{a,b\},\{b,h\},\{c,h\}\}$
h	a,b,h	$\{\{a,b\},\{b,h\},\{c,h\}\}$
$\underline{d}$	a,b,h,d	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\}\}$
h	a,b,h	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\}\}$
$\underline{e}$	a,b,h,e	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\}$
$\underline{f}$	a,b,h,e,f	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\},\{e,f\}\}$
$\underline{g}$	a,b,h,e,f,g	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\},\{e,f\},\{f,g\}\}$
$\underline{i}$	a,b,h,e,f,g,i	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
g	a,b,h,e,f,g	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
f	a,b,h,e,f	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
e	a,b,h,e	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
h	a,b,h	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
b	a,b	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
a	a	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$
–	$\emptyset$	$\{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$

Zatem wierzchołki były odwiedzane w kolejności a,b,h,c,d,e,f,g,i i otrzymaliśmy drzewo spinające DFS $T = (V, E')$, gdzie
$V = \{a,b,c,d,e,f,g,h,i\}$ oraz
$E' = \{\{a,b\},\{b,h\},\{c,h\},\{d,h\},\{e,h\}\},\{e,f\},\{f,g\},\{g,i\}\}$.

BFS:

	odwiedzane wierz.	KOLEJKA	zbiór krawędzi drzewa DFS
a	a	a	$\emptyset$
a	b, d, h	b, d, h	$\{\{a,b\},\{a,d\},\{a,h\}\}$
b	—	d, h	$\{\{a,b\},\{a,d\},\{a,h\}\}$
d	—	h	$\{\{a,b\},\{a,d\},\{a,h\}\}$
h	c, e, f	c, e, f	$\{\{a,b\},\{a,d\},\{a,h\},\{c,h\},\{e,h\},\{f,h\}\}$
c	—	e, f	$\{\{a,b\},\{a,d\},\{a,h\},\{c,h\},\{e,h\},\{f,h\}\}$
e	—	f	$\{\{a,b\},\{a,d\},\{a,h\},\{c,h\},\{e,h\},\{f,h\}\}$
f	g, i	g, i	$\{\{a,b\},\{a,d\},\{a,h\},\{c,h\},\{e,h\},\{f,h\},\{f,g\},\{f,i\}\}$
g	—	i	$\{\{a,b\},\{a,d\},\{a,h\},\{c,h\},\{e,h\},\{f,h\},\{f,g\},\{f,i\}\}$
i	—	—	$\{\{a,b\},\{a,d\},\{a,h\},\{c,h\},\{e,h\},\{f,h\},\{f,g\},\{f,i\}\}$

Zatem wierzchołki były odwiedzane w kolejności $a, b, d, h, c, e, f, g, i$ i otrzymaliśmy drzewo spinające BFS $T = (V, E')$, gdzie

$V = \{a, b, c, d, e, f, g, h, i\}$ oraz

$E' = \{\{a, b\}, \{a, d\}, \{a, h\}, \{c, h\}, \{e, h\}, \{f, h\}, \{f, g\}, \{f, i\}\}$.

b) DFS:

	STOS	zbiór krawędzi drzewa DFS
$\underline{a}$	a	$\emptyset$
$\underline{c}$	a, c	$\{\{a,c\}\}$
$\underline{d}$	a, c, d	$\{\{a,c\},\{c,d\}\}$
$\underline{b}$	a, c, d, b	$\{\{a,c\},\{c,d\},\{d,b\}\}$
d	a, c, b	$\{\{a,c\},\{c,d\},\{d,b\}\}$
$\underline{f}$	a, c, d, f	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\}\}$
$\underline{g}$	a, c, d, f, g	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\}\}$
$\underline{h}$	a, c, d, f, g, h	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\}\}$
$\underline{i}$	a, c, d, f, g, h, i	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\}\}$
h	a, c, d, f, g, h	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\}\}$
g	a, c, d, f, g	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\}\}$
f	a, c, d, f	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\}\}$
d	a, c, d	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\}\}$
c	a, c	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\}\}$
$\underline{e}$	a, c, e	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\},\{c,e\}\}$
c	a, c	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\},\{c,e\}\}$
a	a	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\},\{c,e\}\}$
–	$\emptyset$	$\{\{a,c\},\{c,d\},\{d,b\},\{d,f\},\{f,g\},\{g,h\},\{h,i\},\{c,e\}\}$

Zatem wierzchołki były odwiedzane w kolejności $a, c, d, b, f, g, h, i, e$ i otrzymaliśmy drzewo spinające DFS $T = (V, E')$, gdzie

$V = \{a, b, c, d, e, f, g, h, i\}$ oraz

$E' = \{\{a, c\}, \{c, d\}, \{d, b\}, \{d, f\}, \{f, g\}, \{g, h\}, \{h, i\}, \{c, e\}\}$.

BFS:

	odwiedzane wierz.	KOLEJKA	zbiór krawędzi drzewa DFS
a	a	a	$\emptyset$
a	c, e	c, e	$\{\{a,c\},\{a,e\}\}$
c	d, f	e, d, f	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\}\}$
e	—	d, f	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\}\}$
d	b, g	f, b, g	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\}\}$
f	—	b, g	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\}\}$
b	—	g	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\}\}$
g	h, i	h, i	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\},\{h,g\},\{h,i\}\}$
h	—	i	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\},\{h,g\},\{h,i\}\}$
i	—	—	$\{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\},\{h,g\},\{h,i\}\}$

Zatem wierzchołki były odwiedzane w kolejności $a, c, e, d, f, b, g, h, i$ i otrzymaliśmy drzewo spinające BFS $T = (V, E')$, gdzie
$V = \{a, b, c, d, e, f, g, h, i\}$ oraz
$E' = \{\{a,c\},\{a,e\},\{c,d\},\{c,f\},\{b,d\},\{d,g\},\{h,g\},\{h,i\}\}$

9.40.

a) $n \geq 1$ nieparzyste.
b) $n \geq 3$.

9.41.

a) Tylko dla $n = 1$.
b) $n \geq 1$ nieparzyste oraz $n = 4$.
c) $n \geq 4$.
d) $n \geq 1$.

9.42.

a) n i m dodatnie i parzyste.
b) $n = m$.

NIE. W dowolnym grafie o nieparzystej liczbie wierzchołków cykl Hamiltona, o ile istnieje, jest nieparzystej długości. Natomiast w dowolnym grafie dwudzielnym każdy cykl jest parzystej długości — brak jest cykli nieparzystej długości. Zatem w grafie dwudzielnym o nieparzystej liczbie wierzchołków również brak jest cykli nieparzystej długości, zatem tym bardziej cykli Hamiltona.

9.43.

a) Wszystkie stopnie w grafie G są parzyste, zatem w grafie istnieje cykl Eulera. Zaczynamy np. od wierzchołka a. Kolejno wybierane/trawersowane krawędzie to np.:

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

Uwaga. Np. po wyborze krawędzi $\{e,b\}$ nie możemy wybrać krawędzi $\{a,b\}$, gdyż jest to most, a są jeszcze inne krawędzie incydentne z b.

b) W grafie istnieją dwa wierzchołki o nieparzystych stopniach (d i k), zatem w grafie istnieje łańcuch Eulera o początku i końcu w wierzchołkach d i k. Zaczynamy np. od wierzchołka d. Kolejno trawersowane krawędzie to np.:

$$\{d,a\},\{a,b\},\{b,c\},\{c,d\},\{d,b\},\{b,l\},\{l,a\},\{a,m\},\{m,l\},$$

$$\{l,k\},\{k,j\},\{j,i\},\{i,k\},\{k,h\},\{h,e\},\{e,f\},\{f,h\},\{h,i\},\{i,e\},\{e,d\},\{d,k\}.$$

Uwaga. Np. po wyborze krawędzi $\{b,l\}$ nie możemy wybrać krawędzi $\{l,k\}$, gdyż jest to most, a są jeszcze inne krawędzie incydentne z b; analogicznie, po wyborze krawędzi $\{h,e\}$ nie możemy wybrać krawędzi $\{d,e\}$, gdyż jest to most, a są jeszcze inne krawędzie incydentne z e.

9.44. Podaną sytuację należy utożsamić z grafem $G=(V,E)$ o 5 wierzchołkach ($V=1,2,3,4,5$), w którym istnieje krawędź $\{i,j\}$ wtedy i tylko wtedy, gdy istnieje kostka domina $[i,j]$ bądź $[j,i]$. Wówczas istnienie wymaganego ułożenia kostek równoważne jest istnieniu cyklu Eulera w tak skonstruowanym grafie G.

W naszym przypadku rozważany graf G jest grafem pełnym, w którym każdy wierzchołek jest stopnia 4, a zatem istnieje cykl Eulera — np.

$$\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,1\},\{1,3\},\{3,5\},\{5,2\},\{2,4\},\{4,1\},$$

co wyznacza jednoznacznie ułożenie kostek domina:

$$[1,2],[2,3],[3,4],[4,5],[5,1],[1,3],[3,5],[5,2],[2,4],[4,1].$$

9.46.

a) Startując z wierzchołka 5:

	aktualny wierzchołek	STOS
1	5	5
2	2	5, 2
3	1	5, 2, 1
4	10	5, 2, 1, 10
5	3	5, 2, 1, 10, 3
6	4	5, 2, 1, 10, 3, 4
7	3	5, 2, 1, 10, 3
8	10	5, 2, 1, 10
9	7	5, 2, 1, 10, 7
10	6	5, 2, 1, 10, 7, 6
11	7	5, 2, 1, 10, 7
12	8	5, 2, 1, 10, 7, 8
13	9	5, 2, 1, 10, 7, 8, 9
14	8	5, 2, 1, 10, 7, 8
15	7	5, 2, 1, 10, 7
...	...	...

Algorytm z nawrotami zwróci drogę Hamiltona postaci $5,4,3,2,1,10,9,8,7,6$.

b) Startując z wierzchołka a:

	aktualny wierzchołek	STOS
1	a	a
2	b	a, b
3	c	a, b, c
4	d	a, b, c, d
5	e	a, b, c, d, e
6	d	a, b, c, d
7	f	a, b, c, d, f
8	g	a, b, c, d, f, g
9	h	a, b, c, d, f, g, h
10	g	a, b, c, d, f, g
11	f	a, b, c, d, f
12	d	a, b, c, d
13	c	a, b, c
14	e	a, b, c, e
15	d	a, b, c, e, d
...	...	...

Algorytm z nawrotami zwróci drogę Hamiltona postaci a, b, c, e, d, f, g, h.

9.48. Relacja równoważności $g_1 \circ g_2$:

(1) $g_1 \circ g_1$ (zwrotna)
(2) $g_1 \circ g_2$ to $g_2 \circ g_1$ (symetryczna)
(3) $g_1 \circ g_2$ i $g_2 \circ g_3$ to $g_1 \circ g_3$ (przechodnia)

Wykażemy, że izomorfizm jest relacją równoważności.

(1) Z definicji: dowolny graf G jest izomorficzny z samym sobą, a szukana funkcja h to identyczność.

(2) Jeśli $G_1 \cong G_2$, to istnieje izomorfizm h przekształcający graf $G_1 = (V_1, E_1)$ w graf $G_2 = (V_2, E_2)$ taki, że

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{h(u), h(v)\} \in E_2.$$

Niech h^{-1} będzie funkcją odwrotną do h; oczywiście h^{-1} jest izomorfizmem. Niech x, y dowolnymi wierzchołkami grafu G_2. Jako że $G_1 \cong G_2$, wówczas istnieją wierzchołki u i v w G_1 takie, że $h(u) = x$ i $h(v) = y$. Należy wykazać, że

$$\{x, y\} \in E_2 \quad \Leftrightarrow \quad \{h^{-1}(x), h^{-1}(y)\} \in E_1.$$

Ale warunek $\{x, y\} \in E_2$ równoważny jest $\{h(u), h(v)\} \in E_2$, a to (z założenia) zachodzi wtedy i tylko wtedy, gdy $\{u, v\} \in E_1$, co równoważne jest $\{h^{-1}(x), h^{-1}(y)\} \in E_1$.

(3) Jeśli $G_1 \cong G_2$, to istnieje izomorfizm h przekształcający graf $G_1 = (V_1, E_1)$ w graf $G_2 = (V_2, E_2)$ taki, że

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{h(u), h(v)\} \in E_2.$$

Jeśli $G_2 \cong G_3$, to istnieje izomorfizm g przekształcający graf $G_2 = (V_2, E_2)$ w graf $G_3 = (V_3, E_3)$ taki, że

$$\{x, y\} \in E_2 \quad \Leftrightarrow \quad \{g(x), g(y)\} \in E_3.$$

Wówczas niech f będzie złożeniem $g \cdot h$. Oczywiście f jest izomorfizmem i pozostaje jedynie wykazać, że

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{f(u), f(v)\} \in E_3.$$

Ale z założenia zachodzi

$$\{u, v\} \in E_1 \quad \Leftrightarrow \quad \{h(u), h(v)\} \in E_2 \quad \Leftrightarrow \quad \{g(h(u)), g(h(u))\} \in E_3 \quad \Leftrightarrow \quad \{f(u), f(v)\} \in E_3,$$

co należało wykazać.

9.49. $r = \frac{2m}{n}$.

9.51. $p^{|V|}$ oraz $2 \cdot \binom{p}{2} \cdot p^{|V|-2} = (p-1) \cdot p^{|V|-1}$.

9.52. $\frac{(k+1)!}{(k+1)^{k+1}}$.

Rozwiązanie. 53 a) Niech n i m oznaczają odpowiednio liczbę wierzchołków i krawędzi grafu spójnego $G = (V, E)$. Wówczas z treści mamy, że $\frac{1}{n} \sum_{v \in V} \deg(v) > 2$. Tym samym z Faktu 9.1 otrzymujemy, że $\frac{m}{n} > 2$, a stąd $m > n$. Zatem z Twierdzenia 9.24 otrzymujemy, że w G istnieje cykl. Jednakże usunięcie dowolnej krawędzi tego cyklu nie rozspaja grafu, co więcej, otrzymana liczba krawędzi wynosi $m' = m - 1 \geq n$, a zatem znowu z Twierdzenia 9.24 wynika istnienie kolejnego cyklu. Stąd graf G posiada przynajmniej dwa różne cykle.

W przypadku b) rozumowanie analogiczne do powyższego prowadzi do wniosku, że nie będzie będzie istniał żaden cykl, gdyż otrzymamy $m \leq n - 1$, czyli graf G jest drzewem (jest spójny z założenia). Natomiast w przypadku c) graf G posiada jeden cykl.

9.54. Załóżmy, że graf G spełniający warunek $m > \binom{n-1}{2}$ jest niespójny. Rozważmy jego składową spójność o minimalnej liczbie wierzchołków k. Wówczas graf G ma co najwyżej

$$\frac{k(k-1)}{2} + \frac{(n-k)(n-k-1)}{2}$$

krawędzi: odpowiada to optymistycznej sytuacji, gdy są tylko dwie składowe spójności, każda będąca grafem pełnym. Tym samym otrzymujemy, że

$$\frac{k(k-1)}{2} + \frac{(n-k)(n-k-1)}{2} \geq m > \binom{n-1}{2},$$

$$k(k-1) + (n-k)(n-k-1) > (n-1)(n-2),$$

$$k^2 - k + n^2 - kn - n - nk + k^2 + k > n^2 - 3n + 2,$$

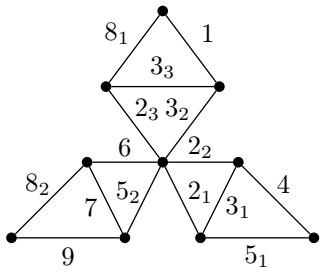
$$k^2 - 1 > n(k-1).$$

Zauważmy jednak, że skoro są przynajmniej dwie składowe spójności, to $n \geq k + 1$, co prowadzi do

$$k^2 - 1 > n(k-1) \geq k^2 - 1,$$

czyli do sprzeczności.

9.55.



Posortowany ciąg krawędzi: $1, 2_1, 2_2, 2_3, 3_1, 3_2, 3_3, 4, 5_1, 5_2, 6, 7, 8_1, 8_1, 9$.
Dla ułatwienia ilustracji działania algorytmu utożsamiamy wagi krawędzi z samymi krawędziami. Przebieg algorytmu jest następujący.

rozpatrywana krawędź	cykl?	krawędzie drzewa
1	$-$	1
2_1	$-$	$1, 2_1$
2_2	$-$	$1, 2_1, 2_2$
2_3	$-$	$1, 2_1, 2_2, 2_3$
3_1	$+$	$1, 2_1, 2_2, 2_3$
3_2	$-$	$1, 2_1, 2_2, 2_3, 3_2$
3_3	$+$	$1, 2_1, 2_2, 2_3, 3_2$
4	$-$	$1, 2_1, 2_2, 2_3, 3_2, 4$
5_1	$+$	$1, 2_1, 2_2, 2_3, 3_2, 4$
5_2	$-$	$1, 2_1, 2_2, 2_3, 3_2, 4, 5_2$
6	$-$	$1, 2_1, 2_2, 2_3, 3_2, 4, 5_2, 6$
7	$+$	$1, 2_1, 2_2, 2_3, 3_2, 4, 5_2, 6$
8_1	$+$	$1, 2_1, 2_2, 2_3, 3_2, 4, 5_2, 6$
8_2	$-$	$1, 2_1, 2_2, 2_3, 3_2, 4, 5_2, 6, 8$
9	$+$	$1, 2_1, 2_2, 2_3, 3_2, 4, 5_2, 6, 8$

9.57. Zauważmy, że rozwiązanie problemu równoważne jest minimalnemu drzewu spinającemu w ważonym grafie pełnym $G = (V, E, w)$, w którym wierzchołki odpowiadają miastom, a wagi krawędzi odległościom pomiędzy tymi miastami. Aby wyznaczyć to drzewo korzystamy z algorytmu Kruskala — koszt otrzymanego rozwiązania/drzewa wynosi 17000000 PLN.

9.60.

a)

Iteracja	u	V	$D[a]$	$D[b]$	$D[c]$	$D[d]$	$D[e]$	$D[f]$
0		$\{b, c, d, e, f\}$	0	$\underline{1}$	∞	∞	4	6
1	b	$\{c, d, e, f\}$	0	1	$\underline{2}$	∞	4	6
2	c	$\{d, e, f\}$	0	1	2	4	$\underline{3}$	6
3	e	$\{d, f\}$	0	1	2	$\underline{4}$	3	4
4	d	$\{f\}$	0	1	2	4	3	$\underline{4}$
5	f	$\emptyset$	0	1	2	4	3	4

A zatem najkrótsza ścieżka z a do f ma długość $D[f] = 4$. Wyznaczenie tej ścieżki:

$$\begin{aligned} 4 \;=\; D[f] \;&=\; D[e]+1 = (D[c]+1)+1 = ((D[b]+1)+1)+1 = \\ &=\; (((D[a]+1)+1)+1)+1 = (((0+1)+1)+1)+1 = 4. \end{aligned}$$

Tym samym ścieżka ta wiedzie przez wierzchołki a, b, c, e, f.

b)

	u	V	$D[a]$	$D[b]$	$D[c]$	$D[d]$	$D[e]$	$D[f]$	$D[g]$	$D[h]$	$D[i]$	$D[j]$
0		$\{b,c,d,e,f,g,h,i,j\}$	0	2	∞	∞	∞	∞	∞	∞	∞	$\underline{1}$
1	j	$\{b,c,d,e,f,g,h,i\}$	0	$\underline{2}$	4	∞	2	∞	4	3	2	1
2	b	$\{c,d,e,f,g,h,i\}$	0	2	3	∞	$\underline{2}$	∞	4	3	2	1
3	e	$\{c,d,f,g,h,i\}$	0	2	3	4	2	5	4	3	$\underline{2}$	1
4	i	$\{c,d,f,g,h\}$	0	2	$\underline{3}$	4	2	5	4	3	2	1
5	c	$\{d,f,g,h\}$	0	2	3	4	2	5	4	$\underline{3}$	2	1
6	h	$\{d,f,g\}$	0	2	3	4	2	5	4	$\underline{3}$	2	1
7	d	$\{f,g\}$	0	2	3	$\underline{4}$	2	5	4	3	2	1
8	g	$\{g\}$	0	2	3	$\underline{4}$	2	5	4	3	2	1
9	f	$\emptyset$	0	2	3	4	2	$\underline{5}$	4	3	2	1

A zatem najkrótsza ścieżka z a do f ma długość $D[f] = 5$. Wyznaczenie tej ścieżki:

$$\begin{aligned} 5 \;=\; D[f] \;&=\; D[e]+3 = (D[j]+1)+3 = ((D[a]+1)+1)+3 = \\ &=\; (((0+1)+1)+1)+1 = 5. \end{aligned}$$

Tym samym ścieżka ta wiedzie przez wierzchołki a, j, e, f.

9.62.

1. `0000` $\longrightarrow$ `0001`
2. `0000` $\longrightarrow$ `0010`
   `0001` $\longrightarrow$ `0011`
3. `0000` $\longrightarrow$ `0100`
   `0001` $\longrightarrow$ `0101`
   `0010` $\longrightarrow$ `0110`
   `0011` $\longrightarrow$ `0111`
4. `0000` $\longrightarrow$ `1000`
   `0001` $\longrightarrow$ `1001`
   `0010` $\longrightarrow$ `1010`
   `0011` $\longrightarrow$ `1011`
   `0100` $\longrightarrow$ `1100`
   `0101` $\longrightarrow$ `1101`
   `0110` $\longrightarrow$ `1110`
   `0111` $\longrightarrow$ `1111`

9.64.

1. 1000 ⟶ 0000
   1001 ⟶ 0001
   1010 ⟶ 0010
   1011 ⟶ 0011
   1100 ⟶ 0100
   1101 ⟶ 0101
   1110 ⟶ 0110
   1111 ⟶ 0111

2. 0100 ⟶ 0000
   0101 ⟶ 0001
   0110 ⟶ 0010
   0111 ⟶ 0011

3. 0010 ⟶ 0000
   0011 ⟶ 0001

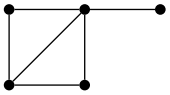
4. 0001 ⟶ 0000

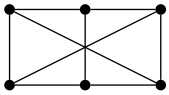
9.65.

a) TAK
b) NIE
c) TAK
d) NIE
e) TAK
f) NIE
g) TAK
h) TAK
i) NIE
j) TAK
k) NIE
l) NIE
m) NIE

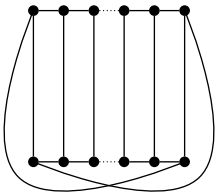
Wskazówki dla Prowadzących

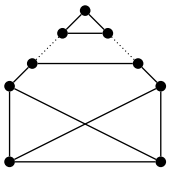
9.2.

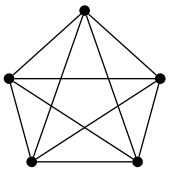
a) 

b) 

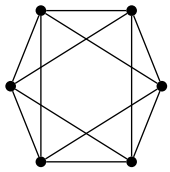
9.3.

a) 

b) 

c) 

$n = 5$ (nieparzyste)



$n = 6$ (parzyste)

9.10.

a) $n = k$ oraz $n \geq k + 2$.

Przypadek $n = k$: po prostu k izolowanych wierzchołków.
Przypadek $n = k+1$ niemożliwy, bo ten „dodatkowy" jeden wierzchołek też byłby izolowany — sprzeczność z liczbą izolowanych wierzchołków równą k.
Przypadek $n \geq k + 2$: k izolowanych wierzchołków i np. graf pełny $K_{n-k\geq 2}$ na pozostałych.

b) k parzyste: $n \geq k$;
$k = 1$: $n \geq 4$ oraz $k \geq 3$ nieparzyste: $n \geq k + 1$.

Przypadek k parzyste: po prostu $k/2$ izolowanych krawędzi, a pozostałe wierzchołki izolowane.
Przypadek k nieparzyste: $n = k$ niemożliwe, bo wtedy suma stopni nieparzysta.
Przypadek $k = 1$ oraz $n = 2, 3$: niemożliwe — – sprzeczność z liczbą wiszących wierzchołków.
Przypadek $k = 1$ oraz $n \geq 4$: liść podpięty do wierzchołka grafu pełnego $K_{n-1\geq 3}$.
Przypadek $k = 3$ oraz $n \geq k + 1$: k liści podpiętych do jednego wierzchołka, pozostałe wierzchołki izolowane.

9.11.

a) $n = k$: $\min = \max = 0$.

$n \geq k + 2$:

- $\min = \lceil \frac{n-k}{2} \rceil$.
  W zależności od parzystości $n-k$, mamy albo $\frac{n-k}{2} = \lceil \frac{n-k}{2} \rceil$ krawędzi izolowanych, albo $\frac{n-k-3}{2}$ krawędzie izolowane, a pozostałe 3 wierzchołki tworzą 3-wierzchołkową ścieżkę, co daje $\frac{n-k-3}{2} + 2 = \lceil \frac{n-k}{2} \rceil$.

- $\max = \frac{(n-k)(n-k-1)}{2}$.
  k izolowanych wierzchołków i graf pełny $K_{n-k\geq 2}$ na pozostałych.

b) k parzyste, $n \geq k$:

- $\min = \frac{k}{2}$: bo $\frac{k}{2}$ izolowanych krawędzi, pozostałe wierzchołki izolowane.
- $n = k$: $\max = \frac{k}{2}$ — bo możliwe tylko $\frac{k}{2}$ izolowanych krawędzi.

  $n \geq k+1$: $\max = k + \frac{(n-k)(n-k-1)}{2}$.
  Jeśli $n = k+1$, to gwiazda o k liściach i k krawędziach.
  Jeśli $n \geq k+2$, to dzielimy liście na dwie dowolne grupy i podpinamy je do dwóch różnych wierzchołków pełnego grafu na $n-k$ wierzchołkach, otrzymując liczbą krawędzi $k + \frac{(n-k)(n-k-1)}{2}$.

  W obu przypadkach $m = k + \frac{(n-k)(n-k-1)}{2}$

$k = 1$, $n \geq 4$:

- $\min = 4$: trójkąt K_3 z dołączonym liściem, pozostałe wierzchołki izolowane.
- $\max = 1 + \frac{(n-k)(n-k-1)}{2}$: graf pełny $K_{n-1\geq 3}$ z dołączonym liściem.

$k \geq 3$ nieparzyste, $n \geq k+1$:

- $\min = \lceil \frac{k}{2} \rceil + 1$.
  Podpinamy 3 liście do pojedynczego wierzchołka, pozostałe $k-3$ liście parujemy, a reszta $n-k$ wierzchołków jest izolowanych. Otrzymujemy $3 + \frac{k-3}{2} = \lceil \frac{k}{2} \rceil + 1$ krawędzi.

- $\max = k + \frac{(n-k)(n-k-1)}{2}$. (Analogicznie jak w przypadku parzystego k.)
  Jeśli $n = k+1$, to gwiazda o k liściach i k krawędziach.
  Jeśli $n \geq k+2$, to dzielimy liście na dwie dowolne grupy i podpinamy je do dwóch różnych wierzchołków pełnego grafu na $n-k$ wierzchołkach, otrzymując liczbą krawędzi $k + \frac{(n-k)(n-k-1)}{2}$.

  W obu przypadkach $m = k + \frac{(n-k)(n-k-1)}{2}$

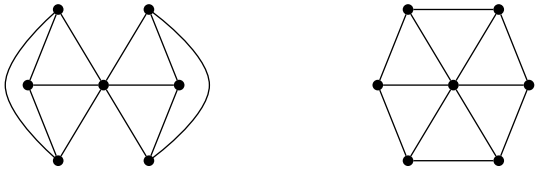
9.13.

a) Cykl C_5.
b) Cykl C_5 z jedną cięciwą/przekątną.
c) Graf pełny K_4 z dołączonym liściem.

9.15.

a) b)

9.22.



9.25. Np. długie ścieżki z dołączonym w „zasadniczo różnym" miejscu dodatkowym liściem — w obu przypadkach ciąg stopni $(3, 2, 2, \ldots, 2, 1, 1, 1)$, a drzewa nie są izomorficzne.

9.47. Np. graf pełny K_{n-1}, gdzie wierzchołki mają etykiety $1, 2, \ldots, n-1$, z dołączonym n-tym wierzchołkiem o etykiecie n do wierzchołka o etykiecie 1 oraz 2. Czas działania: musimy na pewno przeglądnąć wszystkie permutacje zbioru $\{2, \ldots, n-1\}$ zanim algorytm rozpatrzy kolejność $1, n, \ldots$ i chwilę potem znajdzie drogę Hamiltona.

Literatura

1. N. Briggs
   Discrete Mathematics
   Oxford University Press (2003)

2. R. Diestel
   Graph theory
   Springer (2000)

3. T. Gerstenkorn, T. Śródka
   Kombinatoryka i rachunek prawdopodobieństwa: teoria, ćwiczenia i zbiór zadań
   Państwowe Wydawnictwo Naukowe (1967)

4. N. Hartsfield, G. Ringel
   Pearls in graph theory: a comprehensive introduction
   Dover Publications (2003)

5. E. Kowalik
   Kombinatoryka
   Wydawnictwa Naukowo-Techniczne (1993)

6. L. Lovasz, J. Pelikan, K. Vesztergombi
   Discrete mathematics: elementary and beyond
   Springer (2003)

7. J. Matousek, J. Nesetril
   Invitation to Discrete Mathematics
   Clarendon Press (1998)

8. A. Szepietowski
   Matematyka dyskretna
   Wydawnictwo Uniwersytetu Gdańskiego (2004)

9. N. A. Vilenkin
   Kombinatoryka
   Państwowe Wydawnictwo Naukowe (1972)

10. R. J. Wilson
    Wprowadzenie do teorii grafów
    Wydawnictwo Naukowe PWN (2008).

11. M. Żynel
    Materiały do zajęć — Matematyka dyskretna
    Uniwersytet w Białymstoku (2009)