POLI
[TECH〉
NIKA

Politechnika
Częstochowska

Jolanta Pozorska

Izabela Zamorska

Elementy matematyki dyskretnej

Częstochowa 2022

Politechnika Częstochowska

Jolanta Pozorska, Izabela Zamorska

Elementy matematyki dyskretnej

Podręcznik akademicki

Wydawnictwo Politechniki Częstochowskiej

Częstochowa 2022

Recenzent
dr hab. Grażyna Rygał

Redakcja
Joanna Jasińska

Redakcja techniczna
Robert Świerczewski

Projekt okładki
Dorota Boratyńska

ISBN 978-83-7193-931-0
e-ISBN 978-83-7193-932-7

Wydawnictwo Politechniki Częstochowskiej, 42-202 Częstochowa, al. Armii Krajowej 36 B
redakcja tel. 34 325 04 80, dystrybucja tel. 34 325 03 93
e-mail: wydawnictwo@pcz.pl, www.wydawnictwo.pcz.pl

Spis treści

Słowo wstępne

Matematyka dyskretna jest fascynującym działem matematyki, zlepkiem innych działów, ewoluującym od wieków. Interesowali się nią już starożytni, lecz największy rozwój matematyki dyskretnej przypada na wiek XX n.e. Cały czas się rozwija i wymaga ciągłej aktualizacji wiedzy, przez to wciąż można na nowo ją odkrywać. Znamy już sporo jej zastosowań, a ile jest jeszcze nieodkrytych? Wciąż wiele pytań zostaje otwartych, wiele twierdzeń i lematów nieudowodnionych.

Podręcznik *Elementy matematyki dyskretnej* przeznaczony jest nie tylko dla studentów kierunku *informatyka*, ale również dla wszystkich pasjonatów matematyki dyskretnej. Mamy nadzieję, że każdy znajdzie coś interesującego dla siebie. Zdajemy sobie sprawę z tego, że omawiane tematy nie zostały przedstawione w sposób wyczerpujący, przyznajemy, że był to wybór subiektywny, ale mamy nadzieję, że jednak wystarczający.

Dziękujemy Autorom zadań, które pojawiły się w podręczniku, a których nieświadomie nie zacytowałyśmy.

Na końcu chciałyśmy szczególnie podziękować Profesorowi Zbigniewowi Domańskiemu, który zapoczątkował naszą przygodę z matematyką dyskretną.

Autorki

Rozdział 1

Funkcje całkowitoliczbowe

1.1. Funkcje podłoga i sufit

Podłoga (z ang. *floor function*): $\lfloor x \rfloor$ – największa liczba całkowita mniejsza lub równa x dla dowolnego $x \in \boldsymbol{R}$. Podłoga często zwana jest częścią całkowitą, cechą lub *entier*. Oznaczana jest również jako $[x]$ lub $E(x)$.

Sufit (z ang. *ceiling function*), cecha górna: $\lceil x \rceil$ – najmniejsza liczba całkowita większa lub równa x dla dowolnego $x \in \boldsymbol{R}$.

Funkcje podłoga i sufit przyporządkowują każdej liczbie rzeczywistej podłogę lub sufit będące wartością ze zbioru liczb całkowitych. Funkcje podłoga i sufit są niemalejące.

Część ułamkowa, mantysa: $\langle x \rangle = x - \lfloor x \rfloor$, $\langle x \rangle \in [0, 1)$. Część ułamkowa jest również oznaczana przez $\{x\}$. Spełnia ona nierówności $0 \leq \langle x \rangle < 1$. Część całkowita jest funkcją okresową o okresie zasadniczym 1.

1.2. Własności funkcji całkowitoliczbowych

Z określenia liczby $\lfloor x \rfloor$ wynika, że dla każdej liczby rzeczywistej x spełnione są nierówności [1]

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \tag{1.1}$$

Podobna własność jest dla cechy górnej

$$\lceil x \rceil - 1 < x \leq \lceil x \rceil \tag{1.2}$$

Dodatkowo

$$\lfloor x \rfloor \leq x \leq \lceil x \rceil \tag{1.3}$$

Równość zachodzi tylko dla całkowitych x [2]

$$\lfloor x \rfloor = \lceil x \rceil = x \tag{1.4}$$

Dla dowolnych liczb rzeczywistych x i y takich, że $\lfloor x \rfloor = \lfloor y \rfloor$, zachodzi nierówność [3]

$$|x - y| < 1 \tag{1.5}$$

Dla każdej liczby rzeczywistej x i dla każdej liczby całkowitej n zachodzą równości [2]

$$\lfloor x+n \rfloor = \lfloor x \rfloor + n \tag{1.6}$$

$$\lceil x+n \rceil = \lceil x \rceil + n$$

$$\langle x+n \rangle = \langle x \rangle$$

Funkcje podłogi, sufitu i części całkowitej są idempotentne dla dowolnej liczby rzeczywistej x [2]

$$\big\lfloor \lfloor x \rfloor \big\rfloor = \lfloor x \rfloor \tag{1.7}$$

$$\big\lceil \lceil x \rceil \big\rceil = \lceil x \rceil$$

$$\langle \langle x \rangle \rangle = \langle x \rangle$$

I jeszcze dwie własności również spełnione dla dowolnej liczby rzeczywistej x

$$\lfloor \lceil x \rceil \rfloor = \lceil x \rceil \tag{1.8}$$

$$\lceil \lfloor x \rfloor \rceil = \lfloor x \rfloor$$

Dla dowolnych liczb rzeczywistych x i y spełnione są nierówności [1, 2]

$$\lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor \tag{1.9}$$

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$$

$$\lceil x \rceil + \lceil y \rceil - 1 \leq \lceil x+y \rceil \leq \lceil x \rceil + \lceil y \rceil$$

Dla dowolnej liczby rzeczywistej x zachodzą równości [3]

$$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor & \text{dla } x \in \boldsymbol{Z} \\ -\lfloor x \rfloor - 1 & \text{dla } x \notin \boldsymbol{Z} \end{cases} \tag{1.10}$$

Przykład 1.1

Obliczyć podłogę dla liczb ze zbioru $\{-0.5, 0.5, 1.5, e\}$.

$$\lfloor -0.5 \rfloor = -1$$

$$\lfloor 0.5 \rfloor = 0$$

$$\lfloor 1.5 \rfloor = 1$$

$$\lfloor e \rfloor = 2$$

Przykład 1.2

Obliczyć sufit dla liczb ze zbioru $\{-0.5, 0.5, 1.5, \pi\}$.

$$\lceil -0.5 \rceil = 0$$

$$\lceil 0.5 \rceil = 1$$

$\lceil 1.5 \rceil = 2$

$\lceil \pi \rceil = 4$

Przykład 1.3

Obliczyć część ułamkową dla liczb ze zbioru $\{-0.5, 0.5, 1.3\}$.

$\langle -0.5 \rangle = -0.5 - \lfloor -0.5 \rfloor = -0.5 + 1 = 0.5$

$\langle 0.5 \rangle = 0.5 - \lfloor 0.5 \rfloor = 0.5 - 0 = 0.5$

$\langle 1.3 \rangle = 1.3 - \lfloor 1.3 \rfloor = 1.3 - 1 = 0.3$

Przykład 1.4

Obliczyć:

$\left\lfloor \frac{1}{4} + \left\lfloor \frac{1}{4} \right\rfloor \right\rfloor = \left\lfloor \frac{1}{4} \right\rfloor = 0$

$\left\lfloor \frac{1}{4} + \left\lceil \frac{1}{4} \right\rceil \right\rfloor = \left\lfloor 1\frac{1}{4} \right\rfloor = 1$

$\left\lceil \frac{1}{4} + \left\lceil \frac{1}{4} \right\rceil \right\rceil = \left\lceil 1\frac{1}{4} \right\rceil = 2$

$\left\lceil \frac{1}{4} + \left\lfloor \frac{1}{4} \right\rfloor \right\rceil = \left\lceil \frac{1}{4} \right\rceil = 1$

W [4] przedstawiono wzór, za pomocą którego można ustalić liczbę liczb całkowitych w podanych przedziale rzeczywistym.

Liczba liczb całkowitych w przedziale $[a, b]$ wynosi

$$\lfloor b \rfloor - \lceil a \rceil + 1 \tag{1.11}$$

Przykład 1.5

Ile jest liczb całkowitych w przedziale $\left[-2e,\ \frac{4\pi}{3}\right]$?

$\left\lfloor \frac{4\pi}{3} \right\rfloor - \lceil -2e \rceil + 1 = 4 - (-5) + 1 = 10$

Przedział zawiera 10 liczb całkowitych.

Przykład 1.6

Wykazać okresowość funkcji $f(x) = x - \lfloor x \rfloor$. Wyznaczyć okres podstawowy [5].

Do wykazania okresowości posłuży *Wzór 1.6* $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ spełniony dla każdej liczby rzeczywistej x i każdej liczby całkowitej n.

$f(x + n) = (x + n) - \lfloor x + n \rfloor = (x + n) - (\lfloor x \rfloor + n) = x - \lfloor x \rfloor = f(x)$

Funkcja $f(x)$ jest okresowa. Okresem podstawowym jest 1.

1.3. Równania, nierówności, układy równań

Przykład 1.7

Rozwiązać równanie $\frac{2x+3}{3} = \left\lfloor \frac{7x+5}{4} \right\rfloor$.

Ze *Wzoru 1.1* wynika, że

$$\frac{2x+3}{3} \leq \frac{7x+5}{4} < \frac{2x+3}{3} + 1$$

Rozwiązując nierówność, otrzymuje się

$$-\frac{3}{13} \leq x < \frac{9}{13}$$

Po przekształceniach nierówność przyjmuje postać

$$\frac{33}{39} \leq \frac{2x+3}{3} < \frac{57}{39}$$

Do przedziału $\left[\frac{33}{39}, \frac{57}{39}\right)$ należy tylko jedna liczba całkowita 1, stąd liczba $\frac{2x+3}{3}$ może przyjmować tylko tę wartość.

$$\frac{2x+3}{3} = 1$$

Z równania wynika, że $x = 0$.

Przykład 1.8

Rozwiązać równanie $\frac{3x+1}{5} = \left\lfloor \frac{4x+3}{7} \right\rfloor$.

Ze *Wzoru 1.1* części całkowitej wynika, że

$$\frac{3x+1}{5} \leq \frac{4x+3}{7} < \frac{3x+1}{5} + 1$$

Rozwiązując nierówność, otrzymuje się

$$-27 < x \leq 8$$

Po przekształceniach nierówność przyjmuje postać

$$-16 < \frac{3x+1}{5} \leq 5$$

Do przedziału $(-16, 5]$ należy 21 liczb całkowitych, stąd liczba $\frac{3x+1}{5}$ może przyjmować wszystkie 21 wartości.

$$\frac{3x+1}{5} = -15, \frac{3x+1}{5} = -14, \frac{3x+1}{5} = -13, \frac{3x+1}{5} = -12, \ldots, \frac{3x+1}{5} = 4, \frac{3x+1}{5} = 5$$

Z równań wynika, że $x \in \left\{-\frac{76}{3}, -\frac{71}{3}, -\frac{66}{3}, -\frac{61}{3}, \ldots, \frac{19}{3}, 8\right\}$, czyli jest to 21 wyrazów ciągu liczbowego o wyrazie ogólnym $a_n = \frac{5}{3}n - \frac{81}{3}$, dla $n \in \{1, 2, 3, \ldots, 21\}$.

Więcej równań podobnych do *Przykładów 1.7* i *1.8* można znaleźć w [3, 6, 19].

Przykład 1.9

Rozwiązać równanie:

$$\lfloor 2x^4 \rfloor - \lfloor 21x^3 \rfloor + \lfloor 74x^2 \rfloor - \lfloor 105x \rfloor + 50 = 25\langle x \rangle$$

Lewa strona równania jest na pewno liczbą całkowitą. Prawa strona równania też musi być liczbą całkowitą. Z zależności $0 \leq \langle x \rangle < 1$ wynika, że jedyną liczbą całkowitą jest $\langle x \rangle = 0$.

Zadaniem jest rozwiązanie równania

$$2x^4 - 21x^3 + 74x^2 - 105x + 50 = 0$$

w zbiorze liczb całkowitych, gdyż z powyższych wniosków wynika, że x jest liczbą całkowitą.

Rozwiązanie całkowite równania musi należeć do zbioru (pominięto w nim liczby wymierne, ale niecałkowite) $x \in \{-1, 1, -2, 2, -5, 5, -10, 10, -25, 25, -50, 50\}$. Po sprawdzeniu tylko trzy liczby całkowite ze zbioru spełniają równanie. I są to $\{1, 2, 5\}$. Liczby te są jednocześnie rozwiązaniem wyjściowego równania w zbiorze liczb rzeczywistych.

Przykład 1.10

Rozwiązać równanie $-2x^2 + 11\lfloor x \rfloor - 12 = 0$ dla $x \in \boldsymbol{R}_+$ [6].

Korzystając z nierówności $\lfloor x \rfloor \leq x$, otrzymano nierówność

$$-2x^2 + 11x - 12 \geq -2x^2 + 11\lfloor x \rfloor - 12 = 0$$

Rozwiązując nierówność, otrzymano $\left[\frac{3}{2},\ 4\right]$.

Zatem $\lfloor x \rfloor \in \{1, 2, 3, 4\}$.

Po podstawieniu do równania wyjściowego kolejnych liczb z powyższego zbioru otrzymano zbiór rozwiązań $\left\{\sqrt{5}, \sqrt{\frac{21}{2}}, 4\right\}$.

Przykład 1.11

Rozwiązać układ równań:

$$\begin{cases} 5x - y + \lfloor z \rfloor = -4 \\ 2\lfloor x \rfloor + \lfloor y \rfloor + z = 3 \\ -2\lfloor x \rfloor + 2y - 3\lfloor z \rfloor = -3 \end{cases}$$

Z równania drugiego można wnioskować, że liczby $\lfloor x \rfloor$ i $\lfloor y \rfloor$ są całkowite, więc liczba z też musi być całkowita, stąd $\lfloor z \rfloor = z$. Podobnie w przypadku równania trzeciego, liczba y musi być całkowita $\lfloor y \rfloor = y$. Z pierwszego równania wynika, że liczba x jest

całkowita, w takim razie $\lfloor x \rfloor = x$. Podstawiając wszystkie powyższe zależności do wyjściowego układu, otrzymano układ

$$\begin{cases} 5x - y + z = -4 \\ 2x + y + z = 3 \\ -2x + 2y - 3z = -3 \end{cases}$$

Rozwiązaniem przekształconego układu oraz wyjściowego jest trójka liczb $(x,\ y,\ z) = (-1,\ 2,\ 3)$.

Więcej podobnych przykładów można znaleźć w [3].

1.4. Zadania różne

Liczba cyfr liczby n wyraża się wzorem

$$S(n) = \lfloor \log n \rfloor + 1 \tag{1.12}$$

gdzie $\lfloor \log n \rfloor$ jest częścią całkowitą $\log n$.

Przykład 1.12

Dane są liczby 2^{2009} i 5^{2009} w zapisie dziesiętnym. Liczby te zapisano jedna za drugą, tworząc w ten sposób pewną liczbę naturalną a. Ile cyfr ma liczba? [6].

Liczba cyfr zadanej liczby wynosi

$$S(a) = S(2^{2009}) + S(5^{2009}) = \lfloor \log 2^{2009} \rfloor + 1 + \lfloor \log 5^{2009} \rfloor + 1 = \\ = \lfloor 2009 \cdot \log 2 \rfloor + \lfloor 2009 \cdot \log 5 \rfloor + 2$$

Następnie korzystając ze *Wzoru 1.1* dla każdej części całkowitej osobno i dodając nierówności stronami, otrzymuje się

$$2009 \cdot \log 2 + 2009 \cdot \log 5 < S(a) \leq 2009 \cdot \log 2 + 2009 \cdot \log 5 + 2$$

Po przekształceniu uzyskuje się

$$2009 < S(a) \leq 2011.$$

Liczba ma 2010 cyfr.

Przykład 1.13

Udowodnić, że dla każdej liczby naturalnej n liczba $\left\lfloor \frac{n+4}{2} \right\rfloor + 3n - 2 \cdot (-1)^n$ jest podzielna przez 7 [7].

Należy rozpatrzyć dwa przypadki. Dla liczb postaci $n = 2k$ oraz $n = 2k + 1$, dla $k \in \boldsymbol{N}$.

Jeżeli $n = 2k$, to $\left\lfloor\frac{n+4}{2}\right\rfloor + 3n - 2 \cdot (-1)^n = \lfloor k + 2\rfloor + 6k - 2 = 7k$. Liczba jest podzielna przez 7, ponieważ jeden z czynników jest podzielny przez 7, a drugi czynnik jest naturalny.

Jeżeli $n = 2k + 1$, to $\left\lfloor\frac{n+4}{2}\right\rfloor + 3n - 2 \cdot (-1)^n = \lfloor k + 2{,}5\rfloor + 6k + 3 + 2 = 7k + 7$.

Liczba jest podzielna przez 7, ponieważ każdy składnik sumy jest podzielny przez 7.

Przykład 1.14

Uprościć sumę $\left\lfloor\frac{2+\sqrt{2}}{2}\right\rfloor + \left\lfloor\frac{3+\sqrt{3}}{3}\right\rfloor + \left\lfloor\frac{4+\sqrt{4}}{4}\right\rfloor + \cdots + \left\lfloor\frac{n+\sqrt{n}}{n}\right\rfloor$ [7].

Dla każdej liczby naturalnej k nie mniejszej od 2 zachodzą nierówności $1 < \frac{k+\sqrt{k}}{k} < 2$. Stąd $\left\lfloor\frac{k+\sqrt{k}}{k}\right\rfloor = 1$. Można wnioskować, że suma wynosi $n - 1$ dla $n \in \boldsymbol{N}$ i $n \geq 2$.

1.5. Ułamki łańcuchowe

Każdą liczbę niewymierną da się przedstawić w postaci nieskończonego prostego ułamka okresowego. Algorytm do przedstawienia liczby rzeczywistej w postaci prostego ułamka okresowego zaczerpnięto z [8].

Twierdzenie 1.1 (algorytm rozwinięcia liczby w ułamek łańcuchowy)

Niech $x = x_0$ będzie liczbą rzeczywistą. Wówczas x można przedstawić w postaci prostego ułamka łańcuchowego $[q_0, q_1, q_2, \ldots,\ q_n, q_{n+1}]$ za pomocą następującej procedury

$q_0 = \lfloor x_0\rfloor$, $\quad x_1 = \frac{1}{x_0 - q_0}$,

$q_1 = \lfloor x_1\rfloor$, $\quad x_2 = \frac{1}{x_1 - q_1}$,

… … … … $\quad$ … … … …

$q_n = \lfloor x_n\rfloor$, $\quad x_{n+1} = \frac{1}{x_n - q_n}$,

$q_{n+1} = \lfloor x_{n+1}\rfloor$, $\quad x_{n+2} = \frac{1}{x_{n+1} - q_{n+1}}$,

… … … … $\quad$ … … … …

gdzie liczby $q_0, q_1, q_2, \ldots$ to mianowniki częściowe, a $x_0, x_1, x_2, \ldots$ to pełne ilorazy ułamka łańcuchowego.

Przykład 1.15

Przedstawić w postaci ułamka łańcuchowego liczbę $\sqrt{5}$. Podać długość okresu ułamka łańcuchowego.

Zgodnie z *Twierdzeniem 1.1*

$q_0 = \lfloor\sqrt{5}\rfloor = 2 \qquad x = x_0 = \sqrt{5}$

$q_1 = \lfloor\sqrt{5}+2\rfloor = 4 \qquad x_1 = \frac{1}{x_0 - q_0} = \frac{1}{\sqrt{5}-2} = \sqrt{5}+2$

$q_2 = \lfloor\sqrt{5}+2\rfloor = 4 \qquad x_2 = \frac{1}{x_1 - q_1} = \frac{1}{\sqrt{5}+2-4} = \frac{1}{\sqrt{5}-2} = \sqrt{5}+2$

$q_3 = \lfloor\sqrt{5}+2\rfloor = 4 \qquad x_3 = \frac{1}{x_2 - q_2} = \frac{1}{\sqrt{5}+2-4} = \frac{1}{\sqrt{5}-2} = \sqrt{5}+2$

… …

Zatem

$$\sqrt{5} = 2 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{\ddots}}}} = [2, \overline{4}]$$

Długość okresu ułamka łańcuchowego wynosi 1.

1.6. Wzór Legendre'a

Wzór Legendre'a [9] to wzór na wykładnik ($v_p(n!)$) największej potęgi liczby pierwszej p, która dzieli $n!$ dla każdej liczby całkowitej dodatniej n

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \tag{1.13}$$

Jeśli $p^i > n$, to $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$

Czynnik p występuje w rozkładzie $n!$ dokładnie $\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ razy (lemat Legendre'a).

Przykład 1.16

Zastosować wzór Legendre'a dla $n = 10$.

Rozkład na czynniki pierwsze liczby $10!$

$10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1$

Można teraz sprawdzić, czy rzeczywiście czynniki $2, 3, 5, 7$ występują w rozkładzie $10!$ odpowiednio $8, 4, 2, 1$ razy. Do tego posłuży wzór Legendre'a:

$$v_2(10!) = \sum_{i=1}^{\infty} \left\lfloor \frac{10}{2^i} \right\rfloor = \left\lfloor \frac{10}{2} \right\rfloor + \left\lfloor \frac{10}{4} \right\rfloor + \left\lfloor \frac{10}{8} \right\rfloor + \underbrace{\left\lfloor \frac{10}{2^4} \right\rfloor + \left\lfloor \frac{10}{2^5} \right\rfloor + \left\lfloor \frac{10}{2^6} \right\rfloor + \left\lfloor \frac{10}{2^7} \right\rfloor + \left\lfloor \frac{10}{2^8} \right\rfloor + \cdots}_{\text{spełniają warunek: } 2^i>10, \text{ to } \left\lfloor \frac{10}{2^i} \right\rfloor=0} =$$

$$= 5 + 2 + 1 = 8$$

$$v_3(10!) = \sum_{i=1}^{\infty} \left\lfloor \frac{10}{3^i} \right\rfloor = \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{9} \right\rfloor + \underbrace{\left\lfloor \frac{10}{3^3} \right\rfloor + \left\lfloor \frac{10}{3^4} \right\rfloor + \cdots}_{\substack{\text{spełniają warunek:} \\ 3^i>10, \text{ to } \left\lfloor \frac{10}{3^i} \right\rfloor=0}} = 3 + 1 = 4$$

$$v_5(10!) = \sum_{i=1}^{\infty} \left\lfloor \frac{10}{5^i} \right\rfloor = \left\lfloor \frac{10}{5} \right\rfloor + \underbrace{\left\lfloor \frac{10}{5^2} \right\rfloor + \cdots}_{\substack{\text{spełniają warunek:} \\ 5^i>10, \text{ to } \left\lfloor \frac{10}{5^i} \right\rfloor=0}} = 2$$

$$v_7(10!) = \sum_{i=1}^{\infty} \left\lfloor \frac{10}{7^i} \right\rfloor = \left\lfloor \frac{10}{7} \right\rfloor + \underbrace{\left\lfloor \frac{10}{7^2} \right\rfloor + \cdots}_{\substack{\text{spełniają warunek:} \\ 7^i>10, \text{ to } \left\lfloor \frac{10}{7^i} \right\rfloor=0}} = 1$$

Wzór Legendre'a oraz jego zastosowania przedstawiono również w [10].

1.7. Ciekawe stałe i wzory prowadzące do liczb pierwszych

Istnieją zależności, które dla każdej liczby naturalnej dodatniej, dla pewnych stałych, zaokrąglone w dół do liczb naturalnych, są liczbami pierwszymi.

Pierwszą taką stałą jest **stała Millsa**. W teorii liczb stała Millsa [11] jest definiowana jako najmniejsza dodatnia liczba rzeczywista A, której część całkowita jej podwójnej wykładniczej wartości jest liczbą pierwszą dla wszystkich dodatnich liczb naturalnych n.

$$\left\lfloor A^{3^n} \right\rfloor \tag{1.14}$$

Stała Millsa to $A = 1.3063\ldots$. Liczby pierwsze generowane przez stałą Millsa nazywane są liczbami Millsa. Jeśli hipoteza Riemanna jest prawdziwa, ciąg liczb pierwszych Millsa zaczyna się następująco: $2, 11, 1361, \ldots$.

Tóth udowodnił, że część całkowita we *Wzorze 1.14* może być zastąpiona funkcją sufitu, wtedy istnieje stała, dla której

$$\left\lceil B^{r^n} \right\rceil \tag{1.15}$$

jest także liczbą pierwszą dla $r > 2.106\ldots$. W przypadku $r = 3$ wartość $B = 1.2405\ldots$ = = …. Liczby pierwsze generowane ze *Wzoru 1.15* to: $2, 7, 337, \ldots$.

Bez założenia hipotezy Riemanna, Elsholtz udowodnił, że liczba

$$\left\lfloor A^{10^{10n}} \right\rfloor \tag{1.16}$$

jest pierwsza dla wszystkich liczb naturalnych dodatnich, gdzie $A \approx 1.00536773279814724017$. Podobnie liczba

$$\left\lfloor B^{3^{13n}} \right\rfloor \tag{1.17}$$

jest pierwsza dla wszystkich liczb naturalnych dodatnich, gdzie $B \approx 3.824999807343914617161555137 5$.

Jest również liczba $\omega = 1.9287800\ldots$, dla której liczby $\lfloor 2^{\omega} \rfloor, \left\lfloor 2^{2^{\omega}} \right\rfloor, \left\lfloor 2^{2^{2^{\omega}}} \right\rfloor, \ldots$ są pierwsze [12].

Z twierdzenia Wilsona, przedstawionego w [12], wynika, że

$$\pi(n) = \sum_{j=2}^{n} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor$$

gdzie $\pi(x)$ jest liczbą liczb pierwszych mniejszą lub równą x.

Żadna z zależności podanych w *Podrozdziale 1.7* nie ma praktycznego zastosowania.

1.8. Inne zastosowania

Liczba ciągów bez powtarzających się znaków

Liczbę łańcuchów (stringów), o dowolnej długości, w których żaden znak się nie powtarza [13], przedstawia wzór

$$(n)_0 + (n)_1 + \cdots + (n)_n = \lfloor en! \rfloor \tag{1.18}$$

gdzie:

n – jest liczbą liter w alfabecie angielskim (jest ich 26), $n > 0$

$(n)_k -$ silnia dolna $(n)_k = n(n-1)\ldots(n-k+1)$ oznacza liczbę łańcuchów o długości k, w których żaden charakter nie występuje dwa razy i więcej

$e -$ liczba Eulera, $e = 2.718\ldots$

Dla $n = 26$, liczba stringów jest równa $10962598503531495302220342 77$.

Operator mod

Reszta z dzielenia x przez y

$$x \pmod y = x - y \left\lfloor \frac{x}{y} \right\rfloor \tag{1.19}$$

gdzie x jest dowolną liczbą całkowitą, a y jest dodatnią liczbą całkowitą. Więcej na temat operatora modulo w [14].

Przykład 1.17

Obliczyć resztę z dzielenia:

a) $111 \pmod 7 = 111 - 7 \cdot \left\lfloor \frac{111}{7} \right\rfloor = 111 - 7 \cdot 15 = 111 - 105 = 6$

b) $-58 \pmod 3 = -58 - 3 \cdot \left\lfloor \frac{-58}{3} \right\rfloor = -58 - 3 \cdot (-20) = -58 + 60 = 2$

1.9. Zadania do rozwiązania

1. Obliczyć:
   a) $\lfloor -e \rfloor$, $\lfloor -1.4 \rfloor$, $\lfloor 0 \rfloor$, $\lfloor 2.7 \rfloor$
   b) $\lceil -\pi \rceil$, $\lceil e \rceil$, $\lceil -0.7 \rceil$, $\lceil 0 \rceil$, $\lceil -2.7 \rceil$
   c) $\left\lfloor \frac{1}{17} + \left\lfloor \frac{1}{17} \right\rfloor + \left\lfloor -\frac{1}{17} \right\rfloor \right\rfloor$, $\left\lfloor \frac{1}{18} + \left\lceil -\frac{1}{18} \right\rceil + \left\lceil \frac{1}{18} \right\rceil \right\rfloor$, $\left\lceil \frac{1}{2022} \cdot \left\lceil \frac{1}{2022} \right\rceil + \left\lceil \frac{1}{2022} \right\rceil \right\rceil$
   d) $\langle -0.25 \rangle$, $\langle 0.25 \rangle$, $\langle -2.52 \rangle$, $\langle 2.52 \rangle$
2. Funkcja o wzorze $f(x) = x - \lfloor x \rfloor$, $x \in \boldsymbol{R}$ [15]:
   a) jest okresowa,
   b) jest ograniczona,
   c) przyjmuje największą wartość.

   Wybierz poprawną odpowiedź.
3. Sporządzić wykresy funkcji:
   a) $f(x) = -\lfloor x \rfloor + 2$
   b) $f(x) = -\lfloor x - 3 \rfloor$
   c) $f(x) = \lfloor x \rfloor^2$
   d) $f(x) = \lfloor x^2 \rfloor$
   e) $f(x) = x^2 - \lfloor x^2 \rfloor$
   f) $f(x) = (x - \lfloor x \rfloor)^2$
   g) $f(x) = \frac{1}{\lfloor x \rfloor}$
   h) $f(x) = \left\lfloor \frac{1}{x} \right\rfloor$
   i) $f(x) = \langle x \rangle^2$
   j) $f(x) = \langle x^2 \rangle$
   k) $f(x) = x + \langle x \rangle + \lfloor x \rfloor + |x|$ [5]

4. Wyznaczyć wszystkie miejsca zerowe funkcji (o ile istnieją) [16]:

$$f(x) = \begin{cases} x + \lfloor x \rfloor, & \text{gdy } x \in \boldsymbol{Z} \\ x - \langle x \rangle, & \text{gdy } x \notin \boldsymbol{Z} \end{cases}$$

5. Zbadać, które z podanych niżej funkcji są okresowe. Znaleźć okres podstawowy funkcji [17]:
   a) $f(x) = \lfloor x \rfloor$
   b) $f(x) = \lfloor x \rfloor - x$
   c) $f(x) = 2x - 2\lfloor x \rfloor$
   d) $f(x) = 2x - \lfloor 2x \rfloor$
   e) $f(x) = x^2 - \lfloor x^2 \rfloor$
6. Rozwiązać równanie $\sin\left(\frac{\pi}{6} + \left\lfloor \frac{\pi}{6x} \right\rfloor\right) = \frac{1}{2}$ [18].
7. Rozwiązać równanie $\lfloor x^3 \rfloor - \lfloor 5x^2 \rfloor + \lfloor 2x \rfloor + 8 = \langle x \rangle$ [3].
8. Rozwiązać równanie $\lfloor x^3 \rfloor - \lfloor 4x^2 \rfloor + \lfloor x \rfloor + 6 = -\langle x \rangle$.
9. Rozwiązać równanie $\left\lfloor \frac{5x+6}{4} \right\rfloor = \frac{3x-1}{2}$ [6].
10. Rozwiązać równanie $1 - |x + 1| = \frac{\lfloor x \rfloor - x}{x-1}$ dla $x \in \boldsymbol{R}$ [6].
11. Rozwiązać równanie $\left\lfloor \frac{x}{2} \right\rfloor + \left\lfloor \frac{x}{3} \right\rfloor = 1995$ w zbiorze liczb $\boldsymbol{N}$ [6].
12. Rozwiązać równanie $x^3 = \lfloor x \rfloor$ w zbiorze liczb $\boldsymbol{R}$ [6].
13. Rozwiązać równanie $\lfloor 2^x \rfloor = x^2$ w zbiorze liczb $\boldsymbol{R}$ [6].
14. Rozwiązać równanie $x^2 - 6\lfloor x \rfloor - 7 = 0$ w zbiorze liczb $\boldsymbol{R}$ [6].
15. Rozwiązać układ równań $\begin{cases} \lfloor x \rfloor + y - 2\lfloor z \rfloor = 1 \\ x + y - \lfloor z \rfloor = 2 \\ 3\lfloor x \rfloor - 4\lfloor y \rfloor + z = 3 \end{cases}$ [2].
16. Naszkicować na płaszczyźnie zbiór $C = \{(x, y): \lfloor x \rfloor + \lfloor y \rfloor = 2\}$.
17. Narysować w układzie współrzędnych zbiór punktów spełniających warunek $(x - \lfloor x \rfloor)^2 + (y - \lfloor y \rfloor)^2 = 1$ [6].
18. Przedstawić liczbę w postaci ułamka łańcuchowego. Podać długość okresu ułamka łańcuchowego.
    a) $\sqrt{2}$ b) $\sqrt{3}$ c) $\sqrt{6}$ d) $\sqrt{10}$
19. Obliczyć reszty z dzielenia:
    a) $337 \pmod{11}$ b) $-251 \pmod{13}$

1.10. Wskazówki i odpowiedzi do zadań

2. a) b)

4. $x \in \boldsymbol{Z} \cup (0; 1)$

5. a) Nieokresowa

   b) Okresowa o okresie podstawowym równym 1

   c) Okresowa o okresie podstawowym równym 1

   d) Okresowa o okresie podstawowym równym $\frac{1}{2}$

   e) Nieokresowa

6. $x > \frac{\pi}{6}$

7. Równanie w liczbach całkowitych przyjmuje postać $x^3 - 5x^2 - 2x + 8 = 0$. Równanie nie ma rozwiązań całkowitych, stąd wyjściowe równanie również nie ma rozwiązań rzeczywistych.

8. $\{-1, 2, 3\}$

9. Równanie ma 6 rozwiązań.

10. $\{0, -2, -\sqrt{5}\}$

12. $\sqrt[3]{4}$

13. $\{2, \sqrt{2}, \sqrt{3}\}$

14. $\{-1, \sqrt{43}, 7\}$

15. $(2, 1, 1)$

18. a) $[1, \overline{2}]$ b) $[1, \overline{1,2}]$ c) $[2, \overline{2,4}]$ d) $[3, \overline{6}]$

19. a) 7 b) 9

1.11. Literatura

[1] https://pl.wikipedia.org/wiki/Podłoga_i_sufit

[2] https://en.wikipedia.org/wiki/Floor_and_ceiling_functions

[3] M. Węgrzyn, Ł. Drwięga, *Część całkowita i ułamkowa liczby rzeczywistej*, [w:] P. Cholewik i in., *Przed konkursem matematycznym*, Wydawnictwo Szkolne Omega, Kraków 2011.

[4] J. Grygiel, *Wprowadzenie do matematyki dyskretnej*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2007.

[5] H. Pawłowski, W. Tomalczyk, *Zadania z matematyki dla olimpijczyków gimnazjalistów i licealistów*, Oficyna Wydawnicza Tutor, Toruń 2008.

[6] J. Kowolik, T. Szwed, *Matematyka dla odważnych*, Wydawnictwo Nowik, Opole 2010.

[7] H. Pawłowski, *Matematyka 1 zakres rozszerzony*, Wydawnictwo Pedagogiczne Operon, Gdynia 2003.

[8] S.Y. Yan, *Teoria liczb w informatyce*, Wydawnictwo Naukowe PWN, Warszawa 2006.

[9] https://en.wikipedia.org/wiki/Legendre%27s_formula

[10] W. Guzicki, *Silnie i podzielność*, Seminarium OMG, Warszawa 2015.

[11] https://en.wikipedia.org/wiki/Mills%27_constant

[12] P. Ribenboim, *The New Book of Prime Number Records*, Springer, New York 1996.

[13] oeis.org

[14] K.A. Ross, Ch.R.B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[15] E. Świda, K. Kłaczkow, A. Winsztal, *Zdaj maturę Matematyka*, Oficyna Edukacyjna * Krzysztof Pazdro, Warszawa 2004.

[16] P. Pyrdoł, *Matematyka 1. Zakres podstawowy i rozszerzony. Zbiór zadań. Linia 2 standardowa*, Wydawnictwo Pedagogiczne Operon, Gdynia 2003.

[17] B. Gdowski, E. Pluciński, *Zadania i testy z matematyki dla uczniów szkół średnich*, Wydawnictwa Naukowo-Techniczne, Warszawa 1999.

[18] H. Pawłowski, *Matematyka 1. Zbiór zadań*, Wydawnictwo Pedagogiczne Operon, Gdynia 2003.

[19] G. Szkibiel, Cz. Wowk, *Zadania z arytmetyki szkolnej i teorii liczb,* Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin 1999.

Rozdział 2

Indukcja matematyczna i rekurencja

2.1. Twierdzenie o indukcji matematycznej

W matematyce wiele własności, twierdzeń dotyczy liczb naturalnych. Dowodzenie tych twierdzeń opiera się na dedukcji (jak i cała matematyka). Wychodząc od zasady minimum, mówiącej, że każdy niepusty podzbiór zbioru liczb naturalnych ma element najmniejszy, wykazuje się prawdziwość twierdzeń przy pomocy indukcji matematycznej.

Pierwszym opublikowanym dowodem indukcyjnym był (w drugiej połowie XVI wieku) dowód stwierdzenia, że suma kwadratów n kolejnych dodatnich liczb nieparzystych jest równa kwadratowi ich liczby. Przedstawił go włoski matematyk Francesco Maurolico (*„Arithmeticorum libri duo"*).

Na czym polega dowód indukcyjny?
Składa się on z dwóch, równie istotnych, etapów.
Pierwszy z nich: sprawdzenie (S) prawdziwości twierdzenia dla początkowych wartości, na ogół jest bardzo prosty, ale niezbędny dla kompletności rozumowania. Kolejnym etapem jest założenie prawdziwości twierdzenia dla pewnej ustalonej, ale dowolnej, liczby naturalnej (założenie indukcyjne (ZI)) i wykazanie, że dla kolejnej wartości argumentu twierdzenie również jest prawdziwe (dowód (D) tezy indukcyjnej (TI)).
W poprawnie przeprowadzonym dowodzie indukcyjnym nie może zabraknąć żadnego z tych etapów.

Twierdzenie 2.1. (o indukcji matematycznej)

Niech $T(n)$ będzie twierdzeniem dotyczącym liczb naturalnych oraz $n_0 \in \boldsymbol{N}$
(S) prawdziwe jest twierdzenie $T(n_0)$
(ZI) prawdziwe jest twierdzenie $T(k)$ dla $k \geq n_0$
(TI) prawdziwe jest twierdzenie $T(k+1)$ dla $k+1 \geq n_0$

W związku z tym, że liczba k jest dowolną liczbą naturalną i twierdzenie dla k oraz $k+1$ jest prawdziwe, wnioskuje się, że jest prawdziwe dla dowolnej liczby naturalnej $n \geq n_0$

$$\left[T(n_0) \wedge \forall_{k \geq n_0}\ T(k) \implies T(k+1)\right] \implies \forall_{n \geq n_0}\ T(n) \tag{2.1}$$

Tematy indukcji matematycznej i rekurencji, w tym ciągów Fibonacciego i Lucasa, zostały zaprezentowane ogólnie lub bardziej szczegółowo w wielu pozycjach literatury oraz zasobach Internetu (np. [1-9]). Przedstawione przykłady wykazanych własności, a także zadania pozostawione Czytelnikowi do samodzielnej pracy zostały zaczerpnięte między innymi z następujących źródeł: [2, 3, 6-23].

Przykład 2.1

Udowodnić, że dla każdej liczby naturalnej dodatniej n zachodzi równość:

$$1 \cdot 1 + 2 \cdot 3 + 3 \cdot 7 + \cdots + n \cdot (2^n - 1) = (n-1) \cdot 2^{n+1} + 2 - \frac{n(n+1)}{2}$$

(S):

$n = 1 \qquad L = 1 \cdot 1 = 1, \quad P = 0 \cdot 2^2 + 2 - \frac{1 \cdot 2}{2} = 1, \quad L = P$

$n = 2 \qquad L = 1 \cdot 1 + 2 \cdot 3 = 7, \quad P = 1 \cdot 2^3 + 2 - \frac{2 \cdot 3}{2} = 7, \quad L = P$

(ZI): $\forall_{k \in \boldsymbol{N}_+}$

$$1 \cdot 1 + 2 \cdot 3 + 3 \cdot 7 + \cdots + k \cdot \left(2^k - 1\right) = (k-1) \cdot 2^{k+1} + 2 - \frac{k(k+1)}{2}$$

(TI): $\forall_{k+1 \in \boldsymbol{N}_+}$

$$1 \cdot 1 + 2 \cdot 3 + 3 \cdot 7 + \cdots + k \cdot \left(2^k - 1\right) + (k+1) \cdot \left(2^{k+1} - 1\right) = k \cdot 2^{k+2} + 2 - \frac{(k+1)(k+2)}{2}$$

(D):

$$\underbrace{1 \cdot 1 + 2 \cdot 3 + 3 \cdot 7 + \cdots + k \cdot \left(2^k - 1\right)}_{\text{(ZI)}} + (k+1) \cdot \left(2^{k+1} - 1\right)$$

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

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

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

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

□

Przykład 2.2

Wykazać, że dla każdej liczby naturalnej dodatniej n i dowolnej liczby rzeczywistej x zachodzi równość:

$$1 - \frac{x}{1!} + \frac{x(x-1)}{2!} + \cdots + (-1)^n \frac{x(x-1)\cdots(x-n+1)}{n!} = (-1)^n \frac{(x-1)\cdots(x-n)}{n!}$$

(S):

$n = 1 \qquad L = 1 - \frac{x}{1!} = 1 - x, \quad P = -\frac{(x-1)}{1!} = 1 - x, \quad L = P$

$n = 2 \qquad L = 1 - \frac{x}{1!} + \frac{x(x-1)}{2!} = 1 - \frac{x}{1} + \frac{x(x-1)}{2}$

$= \frac{-2(x-1)+x(x-1)}{2} = \frac{(x-1)(x-2)}{2!}, \; P = \frac{(x-1)(x-2)}{2!}, \quad L = P$

(ZI): $\forall_{k \in \boldsymbol{N}_+} \; 1 - \frac{x}{1!} + \frac{x(x-1)}{2!} + \cdots + (-1)^k \frac{x(x-1)\cdots(x-k+1)}{k!} = (-1)^k \frac{(x-1)\cdots(x-k)}{k!}$

(TI): $\forall_{k+1 \in \boldsymbol{N}_+}$

$$1 - \frac{x}{1!} + \frac{x(x-1)}{2!} + \cdots + (-1)^k \frac{x(x-1)\cdots(x-k+1)}{k!} + (-1)^{k+1} \frac{x(x-1)\cdots(x-k+1)(x-k)}{(k+1)!}$$

$$= (-1)^{k+1} \frac{(x-1)\cdots(x-k-1)}{(k+1)!}$$

(D):

$$\underbrace{1 - \frac{x}{1!} + \frac{x(x-1)}{2!} + \cdots + (-1)^k \frac{x(x-1)\cdots(x-k+1)}{k!}}_{\text{(ZI)}} + (-1)^{k+1} \frac{x(x-1)\cdots(x-k+1)(x-k)}{(k+1)!}$$

$$= (-1)^k \frac{(x-1)\cdots(x-k)}{k!} + (-1)^{k+1} \frac{x(x-1)\cdots(x-k+1)(x-k)}{(k+1)!}$$

$$= \frac{(-1)^k}{(k+1)!}[(x-1)\cdots(x-k)(k+1) - x(x-1)\cdots(x-k+1)(x-k)]$$

$$= \frac{(-1)^k}{(k+1)!}(x-1)\cdots(x-k)[k+1-x]$$

$$= \frac{(-1)^{k+1}}{(k+1)!}(x-1)\cdots(x-k)(x-k-1)$$

□

Przykład 2.3

Udowodnić, że dla każdej liczby $n \in \boldsymbol{N}_+$ prawdziwa jest nierówność:

$$\frac{\log n!}{n} < \frac{\log(n+1)!}{n+1}$$

Nierówność tę, korzystając z własności logarytmów, można zapisać w innej postaci:

$\frac{\log n!}{n} < \frac{\log(n+1)!}{n+1}$

$(n+1) \cdot \log n! < n \cdot \log(n+1)!$

$n \cdot \log n! + \log n! < n \cdot \log n! + n \cdot \log(n+1)$

$\log n! < \log(n+1)^n$

$n! < (n+1)^n$

(S):

$n = 1 \qquad L = 1! = 1, \quad P = 2^1 = 2, \quad L < P$

$n = 2 \qquad L = 2! = 2, \quad P = 3^2 = 9, \quad L < P$

(ZI): $\forall_{k \in \boldsymbol{N}_+} \quad k! < (k+1)^k$

(TI): $\forall_{k+1 \in \boldsymbol{N}_+} \; (k+1)! < (k+1)^{k+1}$

(D):

$$(k+1)! = \underbrace{k! \cdot (k+1)}_{\text{(ZI)}} < (k+1)^k \cdot (k+1) = (k+1)^{k+1}$$

□

Przykład 2.4

Udowodnić, że dla każdej liczby $n \in \boldsymbol{N}_+$ zachodzi nierówność:

$$\frac{4^n}{2\sqrt{n}} \leq \binom{2n}{n}$$

Prawą stronę nierówności można zapisać w postaci: $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$

(S):

$n = 1 \qquad L = \frac{4}{2} = 2, \quad P = \frac{(2)!}{(1!)^2} = 2, \quad L = P$

$n = 2 \qquad L = \frac{4^2}{2\sqrt{2}} = 4\sqrt{2} = \sqrt{32}, \quad P = \frac{(4)!}{(2!)^2} = 6 = \sqrt{36}, \quad L < P$

(ZI): $\forall_{k \in \boldsymbol{N}_+} \quad \frac{4^k}{2\sqrt{k}} \leq \frac{(2k)!}{(k!)^2}$

(TI): $\forall_{k+1 \in \boldsymbol{N}_+} \quad \frac{4^{k+1}}{2\sqrt{k+1}} \leq \frac{(2k+2)!}{[(k+1)!]^2}$

(D):

$$\frac{4^{k+1}}{2\sqrt{k+1}} = \frac{4^k}{2\sqrt{k}} \cdot \frac{4\sqrt{k}}{\sqrt{k+1}} = \frac{4^k}{2\sqrt{k}} \cdot \frac{4\sqrt{k}}{\sqrt{k+1}} \cdot \frac{\sqrt{k+1}}{\sqrt{k+1}} = \underbrace{\frac{4^k}{2\sqrt{k}}}_{\text{(ZI)}} \cdot \frac{4\sqrt{k} \cdot \sqrt{k+1}}{k+1} \leq \frac{(2k)!}{(k!)^2} \cdot \frac{2\sqrt{4k^2+4k} \cdot (k+1)}{(k+1)^2}$$

$$\leq \frac{(2k)!}{(k!)^2} \cdot \frac{\sqrt{4k^2+4k+1} \cdot (2k+2)}{(k+1)^2} = \frac{(2k)! \cdot (2k+1) \cdot (2k+2)}{[(k+1)!]^2} = \frac{(2k+2)!}{[(k+1)!]^2}$$

□

Przykład 2.5

Wykazać, że dla każdej liczby $n \in \boldsymbol{N}_+, n \geq 2, k \geq 1, n > k$ zachodzi związek:

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

(S):

$n = 2, k = 1 \qquad L = \binom{2}{1} = 2, \quad P = \binom{1}{0} + \binom{1}{1} = 1 + 1 = 2, \quad L = P$

$n = 3\,, k = 1 \qquad L = \binom{3}{1} = 3, \quad P = \binom{2}{0} + \binom{2}{1} = 1 + 2 = 3, \quad L = P$

$n = 3\,, k = 2 \qquad L = \binom{3}{2} = 3, \quad P = \binom{2}{1} + \binom{2}{2} = 2 + 1 = 3, \quad L = P$

(ZI): $\forall_{t\epsilon \boldsymbol{N}_+\ t\geq 2, k\geq 1, t>k} \quad \binom{t}{k} = \binom{t-1}{k-1} + \binom{t-1}{k}$

(TI): $\forall_{t+1\epsilon \boldsymbol{N}_+\ t\geq 2, k\geq 1, t>k} \quad \binom{t+1}{k} = \binom{t}{k-1} + \binom{t}{k}$

(D):

$L = \binom{t+1}{k} = \frac{(t+1)!}{k!(t+1-k)!} = \frac{(t+1)!}{k![t-(k-1)]!}$

$P = \binom{t}{k-1} + \binom{t}{k} = \frac{t!}{(k-1)!(t+1-k)!} + \frac{t!}{k!(t-k)!}$

$= \frac{t!}{k![t-(k-1)]!} \cdot k + \frac{t!}{k![t-(k-1)]!} \cdot [t-(k-1)] = \frac{t!}{k![t-(k-1)]!} \cdot [k + t - (k-1)]$

$= \frac{t!}{k![t-(k-1)]!} \cdot (t+1) = \frac{(t+1)!}{k![t-(k-1)]!}\,, \; L = P$

□

Przykład 2.6

Korzystając z własności wykazanej w *Przykładzie 2.5*, udowodnić, że dla każdej liczby $n\epsilon \boldsymbol{N}_+$ prawdą jest, że:

$$1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$$

(S):

$n = 1 \qquad L = 1 + 1 = 2, \quad P = 2^1 = 2, \quad L = P$

$n = 2 \qquad L = 1 + 2 + 1 = 4, \quad P = 2^2 = 4, \quad L = P$

(ZI): $\forall_{k\epsilon \boldsymbol{N}_+} \quad 1 + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \binom{k}{k} = 2^k$

(TI): $\forall_{k+1\epsilon \boldsymbol{N}_+} \quad 1 + \binom{k+1}{1} + \binom{k+1}{2} + \cdots + \binom{k+1}{k} + \binom{k+1}{k+1} = 2^{k+1}$

(D):

$$1 + \underbrace{\binom{k+1}{1}}_{\binom{k}{0}+\binom{k}{1}} + \binom{k+1}{2} + \cdots + \underbrace{\binom{k+1}{k}}_{\binom{k}{k-1}+\binom{k}{k}} + \underbrace{\binom{k+1}{k+1}}_{1}$$

$$= 1 + \binom{k}{0} + \binom{k}{1} + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \binom{k}{k} + 1$$

$$= 1 + 1 + \binom{k}{1} + \binom{k}{1} + \binom{k}{2} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \binom{k}{k-1} + 1 + 1$$

$$= 2 \cdot \underbrace{\left[1 + \binom{k}{1} + \binom{k}{2} + \cdots + \binom{k}{k-1} + \underbrace{1}_{\binom{k}{k}}\right]}_{(ZI)} = 2 \cdot 2^k = 2^{k+1}$$

□

Przykład 2.7

Wykazać, że liczba $17^{80} - 17^{16}$ jest podzielna przez 20.

Korzystając ze wzoru skróconego mnożenia, możemy zapisać:

$17^{80} - 17^{16} = (17^{40} + 17^8)(17^{40} - 17^8)$

Liczba 17 i każda jej naturalna potęga są nieparzyste, natomiast każdy z czynników powyższego iloczynu (suma i różnica liczb nieparzystych) są parzyste. Stąd iloczyn ten jest podzielny przez 4.

Aby wykazać podzielność przez 20, należy jeszcze wykazać, że liczba ta jest podzielna przez 5.

Przyjmując $x = 17^8$, otrzymuje się: $x^{10} - x^2 = (x^5 + x)(x^5 - x)$

Wykazując, że istnieje taka liczna naturalna w, dla której $(n^5 + n)(n^5 - n) = 5w$, gdzie n jest dowolną liczbą naturalną, wykaże się również podzielność dla $n = x$.

(S):

$n = 0$ $\quad (0^5 + 0)(0^5 - 0) = 0 = 5 \cdot 0$

$n = 1$ $\quad (1^5 + 1)(1^5 - 1) = 2 \cdot 0 = 0 = 5 \cdot 0$

$n = 2$ $\quad (2^5 + 2)(2^5 - 2) = 34 \cdot 30 = 5 \cdot 204$

Można zauważyć, że podzielność przez 5 daje drugi czynnik iloczynu, a mianowicie: $n^5 - n$. Należy to wykazać.

(ZI): $\forall_{k \in \boldsymbol{N}} \ \exists_{t \in \boldsymbol{N}} \quad k^5 - k = 5t$

(TI): $\forall_{k+1 \in \boldsymbol{N}_+} \ \exists_{s \in \boldsymbol{N}} \quad (k+1)^5 - (k+1) = 5s$

(D):

$$(k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1$$

$$= \underbrace{k^5 - k}_{(ZI)} + \underbrace{5k^4 + 10k^3 + 10k^2 + 5k}_{5(k^4 + 2k^3 + 2k^2 + k)} = 5\underbrace{(t + k^4 + 2k^3 + 2k^2 + k)}_{s} = 5s$$

Tak więc $w = 5t(n^5 + n)$, gdzie n jest dowolną a t pewną liczbą naturalną zależną od wartości n (np. t wynosi 0 dla $n = 0$ i $n = 1$, t wynosi 6 dla $n = 2$, t wynosi 48 dla $n = 3$, t wynosi 204 dla $n = 4$ itd.).

□

Przykład 2.8

Wykazać wzór Newtona: $\forall_{n,k\in\boldsymbol{N}} \quad (x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$

(S):

$n=0 \qquad L=(x+y)^0=1, \quad P=\binom{0}{0}x^0y^0=1$

$n=1 \qquad L=(x+y)^1=x+y, \quad P=\binom{1}{0}x^1y^0+\binom{1}{1}x^0y^1=x+y$

$n=2 \qquad L=(x+y)^2=x^2+2xy+y^2$

$P=\binom{2}{0}x^2y^0+\binom{2}{1}x^1y^1+\binom{2}{2}x^0y^2=x^2+2xy+y^2$

(ZI): $\forall_{t,k\in\boldsymbol{N},\ t\geq k} \quad (x+y)^t=\sum_{k=0}^{t}\binom{t}{k}x^{t-k}y^k$

(TI): $\forall_{t+1,k\in\boldsymbol{N},\ t\geq k} \quad (x+y)^{t+1}=\sum_{k=0}^{t+1}\binom{t+1}{k}x^{t+1-k}y^k$

(D):

$$(x+y)^{t+1}=\underbrace{(x+y)^t}_{\text{(ZI)}}\cdot(x+y)=(x+y)\cdot\sum_{k=0}^{t}\binom{t}{k}x^{t-k}y^k$$

$$=\sum_{k=0}^{t}\binom{t}{k}x^{t+1-k}y^k+\sum_{k=0}^{t}\binom{t}{k}x^{t-k}y^{k+1}$$

$$=\binom{t}{0}x^{t+1}+\underbrace{\binom{t}{1}x^ty+\cdots\binom{t}{t}xy^t}_{\sum_{k=1}^{t}\binom{t}{k}x^{t+1-k}y^k}+\underbrace{\binom{t}{0}x^ty+\binom{t}{1}x^{t-1}y^2+\cdots}_{\sum_{k=0}^{t-1}\binom{t}{k}x^{t-k}y^{k+1}}+\binom{t}{t}y^{t+1}$$

$$=\binom{t}{0}x^{t+1}+\sum_{k=1}^{t}\binom{t}{k}x^{t+1-k}y^k+\sum_{k=0}^{t-1}\binom{t}{k}x^{t-k}y^{k+1}+\binom{t}{t}y^{t+1}$$

Ponieważ:

$$\sum_{k=0}^{t-1}\binom{t}{k}x^{t-k}y^{k+1}=\binom{t}{0}x^ty+\binom{t}{1}x^{t-1}y^2+\cdots+\binom{t}{t-2}x^2y^{t-1}+\binom{t}{t-1}xy^t$$

$$=\sum_{k=1}^{t}\binom{t}{k-1}x^{t+1-k}y^k$$

Otrzymuje się więc:

$$\binom{t}{0}x^{t+1}+\sum_{k=1}^{t}\binom{t}{k}x^{t+1-k}y^k+\sum_{k=1}^{t}\binom{t}{k-1}x^{t+1-k}y^k+\binom{t}{t}y^{t+1}$$

$$=\binom{t}{0}x^{t+1}+\sum_{k=1}^{t}\left[\binom{t}{k}+\binom{t}{k-1}\right]x^{t+1-k}y^k+\binom{t}{t}y^{t+1}$$

Wiedząc również, że:

$\binom{t}{0}=\binom{t+1}{0}$, $\binom{t}{t}=\binom{t+1}{t+1}$ oraz (*Przykład 2.5*) $\binom{t}{k}+\binom{t}{k-1}=\binom{t+1}{k}$

ostatecznie uzyskuje się:

$$\binom{t+1}{0}x^{t+1}+\sum_{k=1}^{t}\binom{t+1}{k}x^{t+1-k}y^{k}+\binom{t+1}{t+1}y^{t+1}=\sum_{k=0}^{t+1}\binom{t+1}{k}x^{t+1-k}y^{k}$$

□

Przykład 2.9

Udowodnić podzielność: $\forall_{n\epsilon N_+}\ 11|6^{2n-2}+3^{n+1}+3^{n-1}$

(S):

$n=1$ $\qquad 6^0+3^2+3^0=11$

$n=2$ $\qquad 6^2+3^3+3^1=66=11\cdot 6$

(ZI): $\forall_{k\epsilon N_+}\ \exists_{t\epsilon N}\quad 6^{2k-2}+3^{k+1}+3^{k-1}=11\cdot t$

(TI): $\forall_{k+1\epsilon N_+}\ \exists_{s\epsilon N}\quad 6^{2k}+3^{k+2}+3^{k}=11\cdot s$

(D):

$$6^{2k}+3^{k+2}+3^{k}=6^{2k-2}\cdot 36+3^{k+1}\cdot 3+3^{k}\cdot 3$$
$$=3\cdot\underbrace{\left(6^{2k-2}+3^{k+1}+3^{k}\right)}_{\text{(ZI)}}+33\cdot 6^{2k-2}=3\cdot 11\cdot t+3\cdot 11\cdot 6^{2k-2}$$
$$=11\cdot\underbrace{\left(3\cdot t+3\cdot 6^{2k-2}\right)}_{s}=11\cdot s$$

□

Przykład 2.10

Udowodnić podzielność: $\forall_{n\epsilon N_+}\ 14\left|\ \frac{5\cdot 3^{4n-1}+3\cdot 5^{2n}}{15}\right.$

(S):

$n=1$ $\qquad \frac{5\cdot 3^3+3\cdot 5^2}{15}=\frac{210}{15}=14$

$n=2$ $\qquad \frac{5\cdot 3^7+3\cdot 5^4}{15}=\frac{12810}{15}=854=14\cdot 61$

(ZI): $\quad \forall_{k\epsilon N_+}\ \exists_{t\epsilon N}\quad \frac{5\cdot 3^{4k-1}+3\cdot 5^{2k}}{15}=14\cdot t$

(TI): $\quad \forall_{k+1\epsilon N_+}\ \exists_{s\epsilon N}\quad \frac{5\cdot 3^{4k+3}+3\cdot 5^{2k+2}}{15}=14\cdot s$

(D):

$$\frac{5\cdot 3^{4k+3}+3\cdot 5^{2k+2}}{15}=\frac{5\cdot 3^{4k-1}\cdot 3^4+3\cdot 5^{2k}\cdot 5^2}{15}=\frac{81\cdot 5\cdot 3^{4k-1}+25\cdot 3\cdot 5^{2k}}{15}$$

$$= \frac{(14\cdot 5+11)\cdot 5\cdot 3^{4k-1}+(14+11)\cdot 3\cdot 5^{2k}}{15} = 14\cdot\frac{15\cdot\left(5\cdot 3^{4k-2}+5^{2k-1}\right)}{15} + 11\cdot\underbrace{\frac{5\cdot 3^{4k-1}+3\cdot 5^{2k}}{15}}_{(ZI)}$$

$$= 14\cdot\underbrace{\left(5\cdot 3^{4k-2}+5^{2k-1}+11t\right)}_{s} = 14s$$

□

Przykład 2.11

Udowodnić, że dla dowolnej liczby naturalnej $n \in \boldsymbol{N}_+$ spełniona jest równość:

$$\sin x + \sin 2x + \cdots + \sin nx = \frac{\sin\frac{nx}{2}\cdot\sin\frac{(n+1)x}{2}}{\sin\frac{x}{2}}$$

(S):

$n = 1$ $\quad L = \sin x, \quad P = \frac{\sin\frac{x}{2}\cdot\sin x}{\sin\frac{x}{2}} = \sin x \quad L = P$

$n = 2$ $\quad L = \sin x + \sin 2x = 2\cdot\sin\frac{3x}{2}\cdot\cos\left(-\frac{x}{2}\right) = 2\cdot\sin\frac{3x}{2}\cdot\cos\frac{x}{2}$

$$P = \frac{\sin x\cdot\sin\frac{3x}{2}}{\sin\frac{x}{2}} = \frac{2\cdot\sin\frac{x}{2}\cdot\cos\frac{x}{2}\cdot\sin\frac{3x}{2}}{\sin\frac{x}{2}} = 2\cdot\sin\frac{3x}{2}\cdot\cos\frac{x}{2} \qquad L = P$$

(ZI): $\forall_{k\in\boldsymbol{N}_+}$ $\quad \sin x + \sin 2x + \cdots + \sin kx = \frac{\sin\frac{kx}{2}\cdot\sin\frac{(k+1)x}{2}}{\sin\frac{x}{2}}$

(TI): $\forall_{k+1\in\boldsymbol{N}_+}$ $\quad \sin x + \sin 2x + \cdots + \sin(k+1)x = \frac{\sin\frac{(k+1)x}{2}\cdot\sin\frac{(k+2)x}{2}}{\sin\frac{x}{2}}$

(D):

$$L = \underbrace{\sin x + \sin 2x + \cdots + \sin kx}_{(ZI)} + \sin(k+1)x = \frac{\sin\frac{kx}{2}\cdot\sin\frac{(k+1)x}{2}}{\sin\frac{x}{2}} + \sin(k+1)x$$

$$= \frac{\sin\frac{(k+1)x}{2}\cdot\left[\sin\frac{kx}{2}+2\cdot\cos\frac{(k+1)x}{2}\cdot\sin\frac{x}{2}\right]}{\sin\frac{x}{2}}$$

$$P = \frac{\sin\frac{(k+1)x}{2}\cdot\sin\frac{(k+2)x}{2}}{\sin\frac{x}{2}} = \frac{\sin\frac{(k+1)x}{2}\cdot\sin\left(\frac{kx}{2}+x\right)}{\sin\frac{x}{2}} = \frac{\sin\frac{(k+1)x}{2}\cdot\left[\sin\frac{kx}{2}\cdot\cos x+\sin x\cdot\cos\frac{kx}{2}\right]}{\sin\frac{x}{2}}$$

$$= \frac{\sin\frac{(k+1)x}{2}\cdot\left[\sin\frac{kx}{2}\cdot\left(1-2\cdot\sin^2\frac{x}{2}\right)+2\cdot\sin\frac{x}{2}\cdot\cos\frac{x}{2}\cdot\cos x\frac{kx}{2}\right]}{\sin\frac{x}{2}}$$

$$= \frac{\sin\frac{(k+1)x}{2}\cdot\left[\sin\frac{kx}{2}+2\cdot\sin\frac{x}{2}\cdot\left(\cos\frac{x}{2}\cdot\cos\frac{kx}{2}-\sin\frac{x}{2}\cdot\sin\frac{kx}{2}\right)\right]}{\sin\frac{x}{2}} = \frac{\sin\frac{(k+1)x}{2}\cdot\left[\sin\frac{kx}{2}+2\cdot\sin\frac{x}{2}\cdot\cos\frac{(k+1)x}{2}\right]}{\sin\frac{x}{2}}$$

$L = P$

W powyższym dowodzie wykorzystane zostały następujące wzory i własności trygonometryczne:

$\sin 2\alpha = 2\sin\alpha \cdot \cos\alpha, \quad \cos 2\alpha = 1 - 2 \cdot \sin^2\alpha$

$\sin(\alpha + \beta) = \sin\alpha \cdot \cos\beta + \cos\alpha \cdot \sin\beta$

$\cos(\alpha + \beta) = \cos\alpha \cdot \cos\beta - \sin\alpha \cdot \sin\beta$

□

2.2. Rekurencja

Wzór rekurencyjny (indukcyjny) jest jednym ze sposobów opisu ciągu liczbowego (x_n) o wyrazach $x_1, x_2, \dots, x_n$ w ten sposób, że znając wartości pewnej skończonej liczby pierwszych wyrazów ciągu, wszystkie kolejne definiuje się za ich pomocą, np.:

$$\begin{cases} x_1 = -1, x_2 = -1, x_3 = 5 \\ x_{n+3} = 3\,x_{n+1} - x_{n+2} + 2x_n^2 \quad \text{dla } n \geq 1 \end{cases}$$

Przykład 2.12

Niech dany będzie ciąg zadany następująco: $x_1 = 1, x_2 = -2, x_n = \frac{2x_{n-2}}{x_{n-1}}, \ n > 3$

Kolejnymi wyrazami ciągu są:
$x_1 = 1, \ x_2 = -2, \ x_3 = \frac{2x_1}{x_2} = \frac{2}{-2} = -1, \ x_4 = \frac{-4}{-1} = 4,$
$x_5 = \frac{-2}{4} = \frac{-1}{2}, \ x_6 = \frac{8}{\frac{-1}{2}} = -16 \dots$

Przykład 2.13

Wyznaczyć definicje rekurencyjne następujących ciągów:

a) $(-2, \ 12, \ -72, \ 432, \ -2592, \ \dots)$

Ciąg ten można zapisać również w postaci:

$\left(-\frac{1}{3} \cdot 6, \ \frac{1}{3} \cdot 36, \ -\frac{1}{3} \cdot 216, \ \frac{1}{3} \cdot 1296, \ -\frac{1}{3} \cdot 7776, \dots\right)$

$= \left(\frac{(-6)^1}{3}, \ \frac{(-6)^2}{3}, \ \frac{(-6)^3}{3}, \ \frac{(-6)^4}{3}, \ \frac{(-6)^5}{3}, \dots\right)$

a rekurencyjnie przedstawić za pomocą wzoru:

$x_1 = -2, \ x_{n+1} = -6 \cdot \ x_n, \ \ n \in \boldsymbol{N}_+$

b) $\left(x, x^2, x^4, x^8, x^{16}, \dots\right)$, gdzie $x \neq 0$, czyli inaczej: $(x, x^2, (x^2)^2, ((x^2)^2)^2, \dots)$.

Rekurencyjna definicja tego ciągu jest następująca:

$x_1 = x, \ x_{n+1} = \ {x_n}^2, \ \ n \in \boldsymbol{N}_+$

Przykład 2.14

Wyznaczyć wzór rekurencyjny ciągu (x_n) określonego wzorem ogólnym $x_n = \frac{n+3}{n+1}$.

Pierwszym wyrazem ciągu (x_n) jest $x_1 = 2$.

Ze wzoru ogólnego należy wyznaczyć n. W prezentowanym przykładzie $n = \frac{3-x_n}{x_n-1}$.

Wyraz ciągu o numerze $n+1$ jest postaci $x_{n+1} = \frac{n+4}{n+2}$ dla $n \geq 1$.

Uwzględniając n w x_{n+1}, otrzymuje się:

$$x_{n+1} = \frac{\frac{3-x_n}{x_n-1}+4}{\frac{3-x_n}{x_n-1}+2} = \frac{3x_n-1}{x_n+1}$$

Wzór rekurencyjny rozpatrywanego ciągu to: $\begin{cases} x_1 = 2 \\ x_{n+1} = \frac{3x_n-1}{x_n+1} \end{cases} \quad n \geq 1$

Ciąg Fibonacciego i ciąg Lucasa

Najsłynniejszymi przykładami ciągów rekurencyjnych są ciągi Fibonacciego i Lucasa.

Za odkrywcę ciągu Fibonacciego powszechnie uważa się włoskiego matematyka Leonarda z Pizy („Fibonacci" było jego przydomkiem), który na początku XIII wieku zastosował go do rozwiązania teoretycznego (nierealistycznego) zadania dotyczącego rozmnażania się królików. Według założeń tego abstrakcyjnego problemu co cztery tygodnie każda para królików wita na świecie parę nowo narodzonych króliczą t, ponadto króliki nie umierają i rozmnażają się systematycznie i bez końca.

Oznaczając przez F_n liczbę par królików po n miesiącach, można **ciąg Fibonacciego** (F_n) zdefiniować następująco:

$F_0 = 0, F_1 = F_2 = 1,$
$F_n = F_{n-2} + F_{n-1}\,, n > 2$

Początkowe wyrazy ciągu Fibonacciego (**liczby Fibonacciego**) to:
$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, \ldots$

Można również podać definicję ciągu Fibonacciego bez warunku $F_0 = 0$, zaczynając od 1.

Granica ilorazu dwóch kolejnych liczb Fibonacciego dąży do tzw. **złotej liczby** (**złoty podział**): $\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \phi = \frac{1+\sqrt{5}}{2} \approx 1{,}618$

n-ty wyraz ciągu Fibonacciego można określić za pomocą wzoru Bineta:

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Dowód indukcyjny tego wzoru można znaleźć w wielu pozycjach literatury.

Prezentowany ciąg oraz złoty podział przypisane zostały Leonardowi z Pizy, jednak zastosowania ich pojawiają się już od czasów starożytnych. Liczby Fibonacciego spotkamy w przyrodzie, architekturze, sztuce, muzyce, kosmosie, modzie, projektach graficznych, a nawet na giełdzie.
Złoty podział uznawany jest za proporcję idealną. Człowiek postrzega dźwięki, kształty zbudowane w oparciu o nią za bardziej harmonijne i estetyczne.

Jednym z badaczy ciągu Fibonacciego był XIX-wieczny francuski matematyk François Édouard Anatole Lucas. Wyznaczył on m.in. wzór na n-ty wyraz ciągu F_n, jest także autorem testu pozwalającego na badanie pierwszości liczb, tzw. testu Lucasa-Lehmera oraz gry „Wieże Hanoi".
Przede wszystkim jest jednak znany z wyznaczonego przez siebie ciągu nazwanego **ciągiem Lucasa**, który tworzy się, podobnie jak ciąg Fibonacciego, sumując parami kolejne liczby, jednak przy innych warunkach początkowych:

$L_0 = 2, L_1 = 1,$
$L_n = L_{n-2} + L_{n-1}\,, n \geq 2$

Początkowe wartości ciągu Lucasa, to:
$2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, \ldots$

Okazuje się, że ciąg ten ma dokładnie taką samą własność jak ciąg Fibonacciego, a mianowicie $\lim\limits_{n\to\infty} \frac{L_{n+1}}{L_n} = \phi$, czyli złoty podział możliwy jest do uzyskania również za pomocą innych ciągów.

Ponadto można zauważyć, że przybliżenia do jedności kolejnych potęg ϕ^{n-1} dają liczby ciągu Lucasa, tzn.:

$$\phi^0 = 1, \phi^1 \approx 2, \phi^2 \approx 3, \phi^3 \approx 4, \phi^4 \approx 7, \phi^5 \approx 11, \ldots, \phi^8 \approx 47, \ldots$$

Podstawowymi zastosowaniami ciągu Lucasa są wyszukiwanie liczb pierwszych oraz algorytmy szyfrowania.

Przykład 2.15

Niech: $\begin{cases} x_1 = 1 \\ x_{n+1} = \frac{2n+1}{n^2+n} - x_n \end{cases}$ $n \geq 1$. Wyznaczyć kilka pierwszych wyrazów ciągu (x_n), na ich podstawie wyznaczyć wzór ogólny tego ciągu i udowodnić go indukcyjnie. Następnie sprawdzić, które wyrazy ciągu spełniają warunek:

$x_n^2 + 3x_n \leq 4$

Kolejne wyrazy ciągu to:

$x_1 = 1$

$x_2 = \frac{2\cdot 1+1}{1^2+1} - x_1 = \frac{3}{2} - 1 = \frac{1}{2}$

$x_3 = \frac{2\cdot 2+1}{2^2+2} - x_2 = \frac{5}{6} - \frac{1}{2} = \frac{1}{3}$

$x_4 = \frac{2\cdot 3+1}{3^2+3} - x_3 = \frac{7}{12} - \frac{1}{3} = \frac{1}{4}$, …

Można przewidzieć, że wzorem ogólnym tego ciągu będzie: $x_n = \frac{1}{n}$ dla $n \geq 1$.

Należy teraz to udowodnić. Ponieważ wzór zgaduje się na podstawie początkowych wartości ciągu, to w dowodzie indukcyjnym można pominąć pierwszy etap, czyli sprawdzenie.

Założenie i teza indukcyjna będą następujące:

(ZI): $\forall_{k\in \boldsymbol{N}_+} \quad x_k = \frac{1}{k}$

(TI): $\forall_{k+1\in \boldsymbol{N}_+} \quad x_{k+1} = \frac{1}{k+1}$

(D): $x_{k+1} = \frac{2k+1}{k^2+k} - x_k = \frac{2k+1}{k(k+1)} - \frac{1}{k} = \frac{2k+1-(k+1)}{k(k+1)} = \frac{k}{k(k+1)} = \frac{1}{k+1}$

□

Warunek dla tego ciągu możemy przekształcić, wstawiając postać ogólną ciągu:

$x_n^2 + 3x_n \leq 4$

$\frac{1}{n^2} + 3\frac{1}{n} - 4 \leq 0$

$4n^2 - 3n - 1 \geq 0$, gdzie $n\in \boldsymbol{N}_+$

Więc otrzymuje się ostatecznie $n \geq 1$, czyli wszystkie wyrazy ciągu spełniają zadany warunek.

Przykład 2.16

Udowodnić wzór: $\sum_{i=0}^{n} F_i = F_{n+2} - 1$, gdzie F_i to wyrazy ciągu Fibonacciego.

(S):

$n = 1$

$L = F_0 + F_1 = 1,\ P = F_3 - 1 = 2 - 1 = 1 \quad L = P$

$n = 2$

$L = F_0 + F_1 + F_2 = 2,\ P = F_4 - 1 = 3 - 1 = 2 \quad L = P$

(ZI): $\forall_{k\in \boldsymbol{N}} \quad \sum_{i=0}^{k} F_i = F_{k+2} - 1$

(TI): $\forall_{k+1\in \boldsymbol{N}} \quad \sum_{i=0}^{k+1} F_i = F_{k+3} - 1$

(D): $\sum_{i=0}^{k+1} F_i = F_{k+2} - 1 + F_{k+1} = F_{k+3} - 1$

□

Przykład 2.17

Udowodnić wzór na n-ty wyraz ciągu Fibonacciego: $F_n = 0{,}2 \cdot (L_{n-1} + L_{n+1})$, gdzie L_n to wyrazy ciągu Lucasa.

(S):

$n = 1$

$F_1 = 0{,}2 \cdot (L_0 + L_2) = 0{,}2 \cdot (L_0 + L_0 + L_1) = 0{,}2 \cdot 5 = 1$

$n = 2$

$F_2 = 0{,}2 \cdot (L_1 + L_3) = 0{,}2 \cdot (2L_1 + L_2) = 0{,}2 \cdot 5 = 1$

(ZI): $\forall_{k \in \boldsymbol{N}_+} \quad F_k = 0{,}2 \cdot (L_{k-1} + L_{k+1})$

(TI): $\forall_{k+1 \in \boldsymbol{N}_+} \quad F_{k+1} = 0{,}2 \cdot (L_k + L_{k+2})$

(D): $F_{k+1} = F_{k-1} + F_k = 0{,}2 \cdot (L_{k-2} + L_k + L_{k-1} + L_{k+1}) = 0{,}2 \cdot (L_k + L_{k+2})$

□

2.3. Zadania do rozwiązania

Zapisać (ZI) oraz (TI) w dowodzie własności:

1. $\forall_{n \in \boldsymbol{N}_+} \quad 1 \cdot 3 \cdot (1!)^2 + 2 \cdot 4 \cdot (2!)^2 + \cdots + n \cdot (n+2) \cdot (n!)^2 = [(n+1)!]^2 - 1$
2. $\forall_{x \geq 0} \ \forall_{n \in \boldsymbol{N}} \quad (1+x)^n \geq 1 + nx + \frac{n(n-1)}{2} x^2$
3. $\forall_{n,k \in \boldsymbol{N}} \quad \sum_{k=0}^{n} \frac{1}{3^k} = \frac{3^{n+1}-1}{2 \cdot 3^n}$
4. $\forall_{n \in \boldsymbol{N}} \quad 13 \mid 10^{3n+1} + 3 \cdot (-1)^n$
5. $\forall_{x,y>0} \ \forall_{n \in \boldsymbol{N}} \quad (x+y)^n < 2^n (x^n + y^k)$

Wykazać, korzystając z zasady indukcji matematycznej, że prawdziwe są następujące zależności:

6. $\forall_{n \in \boldsymbol{N}_+} \quad \left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{9}\right) \cdots \left(1 - \frac{1}{n^2}\right) = \frac{n+1}{2n}$
7. $\forall_{n \in \boldsymbol{N}_+} \quad 1 \cdot 4 + 2 \cdot 7 + 3 \cdot 10 + \cdots + (n+1) \cdot (3n+4) = (n+1) \cdot (n+2)^2$
8. $\forall_{n \in \boldsymbol{N}} \quad 1 + 7 \cdot (1!)^3 + 26 \cdot (2!)^3 + \cdots + ((n+1)^3 - 1) \cdot (n!)^3 = \left((n+1)!\right)^3$
9. $\forall_{n \in \boldsymbol{N}_+} \quad 2^3 + 4^3 + \cdots + (2n)^3 = 2n^2 (n+1)^2$
10. $\forall_{n \in \boldsymbol{N}_+} \quad 1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \cdot \frac{n(n+1)}{2}$

11. $\forall_{n\in\boldsymbol{N}_+}\quad \frac{1^2}{1\cdot 3}+\frac{2^2}{3\cdot 5}+\cdots+\frac{n^2}{(2n-1)(2n+1)}=\frac{n(n+1)}{2(2n+1)}$

12. $\forall_{n\in\boldsymbol{N}_+}\quad \frac{1}{\sqrt{2}(\sqrt{2}+1)}+\frac{1}{(\sqrt{2}+1)(\sqrt{2}+2)}+\cdots+\frac{1}{(\sqrt{2}+n-1)(\sqrt{2}+n)}=\frac{n}{\sqrt{2}(\sqrt{2}+n)}$

13. $\forall_{n\in\boldsymbol{N}_+}\forall_{x\in\boldsymbol{N}}\quad 1+x+x^2+\cdots+x^n=\frac{(x+n)!}{x^n}-x!$

14. $\forall_{n\in\boldsymbol{N}}\,\forall_{x\neq 1}\quad \frac{1\cdot x!}{x}+\frac{2\cdot(x+1)!}{x^2}+\cdots+\frac{n\cdot(x+n-1)!}{x^n}=\frac{x^{n+1}-1}{x^n-1}$

15. $\forall_{n\in\boldsymbol{N}_+,n>3}\quad n!>2^n$

16. $\forall_{n\in\boldsymbol{N}_+,n>2}\quad n!<\left(\sqrt{2}\right)^{n(n-1)}$

17. $\forall_{n,k\in\boldsymbol{N}}\quad \binom{n}{k}\cdot\binom{n}{n-k}=\binom{n}{k}^2$

18. $\forall_{n,k\in\boldsymbol{N}}\quad \binom{n}{0}^2+\binom{n}{1}^2+\cdots+\binom{n}{n-1}^2+\binom{n}{n}^2=\binom{2n}{n}$

19. $\forall_{n\in\boldsymbol{N}}\quad 25|4\cdot 6^n+5n-4$

20. $\forall_{n\in\boldsymbol{N}}\quad 17|3\cdot 5^{2n+1}+2^{3n+1}$

21. $\forall_{n\in\boldsymbol{N}}\quad 38\left|\frac{2}{5}\cdot 5^{2n}\cdot 2^n+\frac{3}{2}\cdot 12^n\right.$

22. $\forall_{n\in\boldsymbol{N}}\quad 11|2^{6n+1}+3^{2n+2}$

23. Znaleźć wzór rekurencyjny ciągu:
    a) $1, 27, 125, 343, 729, 1331, 2197, \ldots$
    b) $5, 17, 37, 65, 101, 145, 197, \ldots$
    c) $3, 4, 4, 5, 5, 6, 6, 7, 7, \ldots$

24. Obliczyć pięć początkowych wyrazów ciągu określonego wzorem rekurencyjnym oraz:
    a) $\begin{cases}a_1=\sqrt{3}\\ a_{n+1}=\sqrt{3+a_n^2}\end{cases}\quad n\geq 1.$ Wyznaczyć wzór ogólny tego ciągu.
    b) $\begin{cases}a_1=-2\\ a_{n+1}=a_n+\frac{1}{n}\cdot\sin^2\frac{(2n-1)\pi}{2}\end{cases}\quad n\geq 1.$ Zbadać, czy ciąg jest monotoniczny.
    c) $\begin{cases}a_1=-1\\ a_{n+1}=a_n^2\cdot 2^n-1\end{cases}\quad n\geq 1.$ Sprawdzić, czy jest to ciąg geometryczny.

25. Niech dany będzie ciąg (x_n) określony rekurencyjnie. Wyznaczyć wyrazy o numerach 2-6 tego ciągu, podać jego wyraz ogólny, a następnie udowodnić indukcyjnie prawdziwość wyznaczonego wzoru. Sprawdzić, który wyraz ciągu (x_n) spełnia zadany warunek W:

a) $x_1 = 1, x_{n+1} = (n+1)^2 x_n, \quad n \geq 1;$ W: $\sqrt{x_n} \leq 30$

b) $x_1 = x_2 = 1, x_{n+2} = 2\,x_{n+1} + 3x_n \quad n \geq 1;$ W: $x_n = 365$

c) $x_1 = x_2 = 2, \quad x_{n+2} = 2x_{n+1} - x_n, \quad n \geq 1;$ W: $\left|x_n + \frac{6}{n}\right| = \log_2 x_n^6$

d) $x_1 = 0, x_{n+1} = 7n + x_n, \quad n \geq 1;$ W: $\frac{x_{n+1}}{x_n} = 1{,}5$

e) $x_1 = 3\ , x_{n+1} = 2x_n - 1, \quad n \geq 1;$ W: x_n jest liczbą pierwszą mniejszą od 50

26. Zapisać wzór rekurencyjny ciągu geometrycznego określonego wzorem ogólnym $x_n = -4 \cdot \left(\frac{5}{7}\right)^n$.

27. Ciąg (x_n) określony jest następująco: $\begin{cases} x_1 = 1, x_2 = 1, x_3 = -1 \\ x_n = x_{n-3} \cdot x_{n-1} \end{cases} \quad n \geq 4$. Wyznaczyć $x_{2023} + 2x_{1900}$.

28. Wykazać prawdziwość wzorów, korzystając z rekurencyjnej definicji ciągu Fibonacciego i ciągu Lucasa:

a) $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$

b) $F_0 - F_1 + F_2 - F_3 + \cdots - F_{2n-1} + F_{2n} = F_{2n-1} - 1$

c) $F_0^2 + F_1^2 + F_2^2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$

d) $L_1 + L_3 + L_5 + \cdots + L_{2n+1} = L_{2n+2} - 2$

e) $L_n = F_{n-1} \cdot F_{n+1}$

2.4. Wskazówki i odpowiedzi do zadań

5. Wskazówka: Porównać z *Przykładem 2.8.*

15. Wskazówka: $k + 1 > 2$

18. Wskazówka: Porównać z *Przykładami 2.4-2.6.*

23. b) $(2n)^2 + 1$ c) $\left\lfloor \frac{n}{2} \right\rfloor + 3$

24. b) Ciąg jest rosnący. c) Ciąg nie jest geometryczny.

25. b) $x_7 = 365$

27. -3

2.5. Literatura

[1] W. Broniowski, *Matematyka dyskretna. Wykłady dla studentów informatyki*, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2015.

[2] R. Kalina, T. Szymański, F. Linke, M. Woźniak, *Matematyka dla klasy II liceum i technikum*, Wydawnictwo Sens, Warszawa 2003.

[3] K. Kłaczkow, M. Kurczab, E. Świda, *Matematyka. Klasa I*, Oficyna Wydawnicza Krzysztof Pazdro, Warszawa 2002.

[4] W. Leksiński, I. Nabiałek, W. Żakowski, *Matematyka: definicje, twierdzenia, przykłady, zadania*, Wydawnictwa Naukowo-Techniczne, Warszawa 1992.

[5] L. Lovász, K. Vesztergombi, *Discrete Mathematics*, Lecture Notes, Yale University, 1999.

[6] J. Pozorska, I. Zamorska, *Wybrane zagadnienia z matematyki dyskretnej. Część 1*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2021.

[7] K.A. Ross, C.R.B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[8] http://pl.wikipedia.org/

[9] http://wazniak.mimuw.edu.pl

[10] A. Cewe, H. Nahorska, *Matura. Zbiór zadań*, Wydawnictwo Podkowa, Gdańsk 1999.

[11] A. Cewe, Cz. Grajek, H. Nahorska, *Matura – zbiór zadań (profil matematyczno-fizyczny). Część II*, Wydawnictwo Podkowa, Gdańsk 1996.

[12] E. Bańkowska, A. Cewe, D. Stankiewicz, *Egzamin wstępny na wyższe uczelnie. Zbiór zadań*, Wydawnictwo Podkowa, Gdańsk 1999.

[13] V. Bryant, *Aspekty kombinatoryki*, Wydawnictwa Naukowo-Techniczne, Warszawa 2007.

[14] H. Furmańczyk, K. Horodecki, P. Żyliński, *Matematyka dyskretna dla studentów kierunku Informatyka*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2010.

[15] B. Gdowski, E. Pluciński, *Zbiór zadań z matematyki dla kandydatów na wyższe uczelnie*, Wydawnictwa Naukowo-Techniczne, Warszawa 1973.

[16] B. Gdowski, E. Pluciński, *Zadania i testy z matematyki dla uczniów szkół średnich*, Wydawnictwa Naukowo-Techniczne, Warszawa 1994.

[17] J. Jaworski, Z. Palka, J. Szymański, *Matematyka dyskretna dla informatyków*, Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 2007.

[18] M. Kurczab, E. Kurczab, E. Świda, *Matematyka. Próbne arkusze maturalne,* Oficyna Wydawnicza Krzysztof Pazdro, Warszawa 2016.

[19] W. Leksiński, B. Macukow, W. Żakowski, *Matematyka w zadaniach dla kandydatów na wyższe uczelnie techniczne*, Wydawnictwa Naukowo-Techniczne, Warszawa 1987.

[20] Z. Palka, A. Ruciński, *Wykłady z kombinatoryki*, Wydawnictwo Naukowe PWN, Warszawa 1998.

[21] H. Pawłowski, *Matematyka 1 i 2*. *Zbiór zadań*, Wydawnictwo Pedagogiczne Operon, Gdynia 2003.

[22] P. Pytroł, *Matematyka*, *Zbiór zadań*, Wydawnictwo Pedagogiczne Operon, Gdynia 2003.

[23] https://www.odkrywamyzakryte.com/dziwne-liczby-lucasa/

Rozdział 3

Relacje. Relacja kongruencji

3.1. Relacje

Niech dane będą niepuste zbiory X, Y o elementach postaci, odpowiednio, x, y.
Iloczynem (produktem) **kartezjańskim** zbiorów X, Y nazywa się wszystkie pary (x, y) takie, że: $(x, y) \in X \times Y \Leftrightarrow x \in X \ \wedge y \in Y$.

x jest poprzednikiem pary, y jest następnikiem, a kolejność tych elementów jest istotna.

Dowolny podzbiór $R \subseteq X \times Y$ nosi nazwę **relacji binarnej** (dwuargumentowej).

Podzbiór iloczynu $X^2 = X \times X$ nazywa się **relacją w zbiorze X**.

Stosuje się następujące oznaczenia dla elementów będących ze sobą w relacji: $(x, y) \in R$ lub xRy. W literaturze można również znaleźć oznaczenie $R(x, y)$ [1-4].

Dziedziną relacji R nazywa się zbiór: $D(R) = \{x \in X: \exists y \in Y \ \ (x, y) \in R\}$.

Przeciwdziedziną relacji R nazywa się zbiór:
$D^{-1}(R) = \{y \in Y: \exists x \in X \ \ (x, y) \in R\}$.

Relacją odwrotną do relacji R jest podzbiór R^{-1} iloczynu $Y \times X$ spełniający warunek: $(y, x) \in R^{-1} \Leftrightarrow (x, y) \in R$.

Dopełnieniem relacji jest zbiór: $R' = (X \times Y) \backslash R$.

Jeśli zbiory X, Y są zbiorami skończonymi, to relację można (prócz podania jej warunku, np.: $(x, y) \in R \Leftrightarrow \frac{x}{y} = 2$ czy: $(x, y) \in R$, gdy y jest najmniejszym nieparzystym dzielnikiem $3x + 2y$) przedstawić:

- podając wszystkie pary należące do tej relacji;
- rysując graf tej relacji (nieskierowany, gdy relacja jest symetryczna, lub skierowany, gdy relacja tej własności nie ma);
- zapisując tablicę relacji wymiaru $|X| \times |Y|$. Jeśli xRy, to w tablicy, w miejscu odpowiadającym wierszowi x i kolumnie y wstawia się x lub 1. W przeciwnym razie, odpowiednio, zostawia się puste miejsce lub wpisuje 0.

Wybrane własności relacji:

Relacja R w zbiorze X jest:

zwrotna, gdy: $\forall x \in X \quad (x,x) \in R$

przeciwzwrotna, gdy: $\forall x \in X \quad (x,x) \notin R$

symetryczna, gdy: $\forall x,y \in X \quad (x,y) \in R \implies (y,x) \in R$

asymetryczna, gdy: $\forall x,y \in X \quad (x,y) \in R \implies \sim(y,x) \in R$

antysymetryczna, gdy: $\forall x,y \in X \quad (x,y) \in R \wedge (y,x) \in R \iff x = y$

przechodnia, gdy: $\forall x,y,z \in X \quad (x,y) \in R \wedge (y,z) \in R \implies (x,z) \in R$

euklidesowa, gdy: $\forall x,y,z \in X \quad (x,y) \in R \wedge (x,z) \in R \implies (y,z) \in R$

liniowa, gdy: $\forall x,y \in X \quad (x,y) \in R \vee (y,x) \in R$

spójna, gdy: $\forall x,y \in X \quad (x,y) \in R \vee (y,x) \in R \vee x = y$

Relacja, która jest zwrotna, symetryczna i przechodnia, nosi nazwę **relacji równoważności**.

Relacja, która jest zwrotna, antysymetryczna i przechodnia, nazywa się **relacją porządkującą** (porządkiem). Dodając do tego własność liniowości relacji, otrzymuje się **relację liniowo uporządkowaną** (łańcuch). O zbiorze X mówi się wówczas, że jest uporządkowany przez relację R.

W zbiorze uporządkowanym przez relację można wyróżnić elementy maksymalne i największe oraz minimalne i najmniejsze.

Niech X będzie zbiorem uporządkowanym przez relację R, wówczas:

$y \in X$ jest **elementem maksymalnym** w X, jeśli $\forall x \in X \quad (y,x) \in R \implies x = y$

$y \in X$ jest **elementem największym** w X, jeśli $\forall x \in X \quad (x,y) \in R$

$y \in X$ jest **elementem minimalnym** w X, jeśli $\forall x \in X \quad (x,y) \in R \implies x = y$

$y \in X$ jest **elementem najmniejszym** w X, jeśli $\forall x \in X \quad (y,x) \in R$

Przykład 3.1

Niech $\boldsymbol{P}, \boldsymbol{N}, \boldsymbol{Z}, \boldsymbol{Q}$ będą odpowiednio zbiorami liczb pierwszych, naturalnych, całkowitych i wymiernych oraz niech $X = \{\boldsymbol{P}, \boldsymbol{N}, \boldsymbol{Z}, \boldsymbol{Q}\}$. Relację R w zbiorze X zdefiniowano następująco: $(x,y) \in R \iff x$ jest podzbiorem y.

$D(R) = D^{-1}(R) = X$

Pary należące do tej relacji to:

$R = \{(\boldsymbol{P},\boldsymbol{P}),(\boldsymbol{P},\boldsymbol{N}),(\boldsymbol{P},\boldsymbol{Z}),(\boldsymbol{P},\boldsymbol{Q}),(\boldsymbol{N},\boldsymbol{N}),(\boldsymbol{N},\boldsymbol{Z}),(\boldsymbol{N},\boldsymbol{Q}),(\boldsymbol{Z},\boldsymbol{Z}),(\boldsymbol{Z},\boldsymbol{Q}),(\boldsymbol{Q},\boldsymbol{Q})\}$

Relację odwrotną tworzą pary:

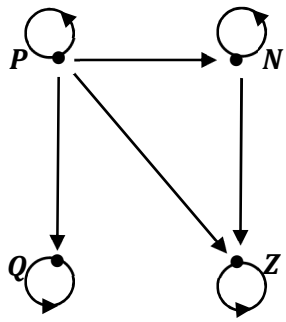
$R^{-1} = \{(\boldsymbol{P},\boldsymbol{P}),(\boldsymbol{N},\boldsymbol{P}),(\boldsymbol{Z},\boldsymbol{P}),(\boldsymbol{Q},\boldsymbol{P}),(\boldsymbol{N},\boldsymbol{N}),(\boldsymbol{Z},\boldsymbol{N}),(\boldsymbol{Q},\boldsymbol{N}),(\boldsymbol{Z},\boldsymbol{Z}),(\boldsymbol{Q},\boldsymbol{Z}),(\boldsymbol{Q},\boldsymbol{Q})\}$

a dopełnieniem relacji jest zbiór:

$R' = \{(\boldsymbol{N},\boldsymbol{P}),(\boldsymbol{Z},\boldsymbol{P}),(\boldsymbol{Z},\boldsymbol{N}),(\boldsymbol{Q},\boldsymbol{P}),(\boldsymbol{Q},\boldsymbol{N}),(\boldsymbol{Q},\boldsymbol{Z})\}$

Tablica i graf tej relacji:

	$\boldsymbol{P}$	$\boldsymbol{N}$	$\boldsymbol{Z}$	$\boldsymbol{Q}$
$\boldsymbol{P}$	x	x	x	x
$\boldsymbol{N}$		x	x	x
$\boldsymbol{Z}$			x	x
$\boldsymbol{Q}$				x



Graf jest grafem skierowanym (strzałka wskazuje następnik pary).

Przy sprawdzaniu, jakie relacja ma własności, szczególną uwagę należy zwrócić na kwantyfikator ∀ („dla każdego…")!

Omawiana relacja jest zwrotna (bo każdy zbiór jest swoim podzbiorem), antysymetryczna (symetria zachodzi tylko dla par $(\boldsymbol{P},\boldsymbol{P}),(\boldsymbol{N},\boldsymbol{N}),(\boldsymbol{Z},\boldsymbol{Z}),(\boldsymbol{Q},\boldsymbol{Q})$), przechodnia, liniowa oraz spójna (te własności wynikają z własności zawierania się zbiorów).
Jest to więc relacja liniowo uporządkowana, w której elementem maksymalnym i elementem największym jest zbiór $\boldsymbol{Q}$, natomiast elementem minimalnym i jednocześnie najmniejszym jest zbiór $\boldsymbol{P}$.
Nie jest to relacja przeciwzwrotna ani asymetryczna (np. $(\boldsymbol{P},\boldsymbol{P}) \in R$), nie jest też symetryczna (np. $(\boldsymbol{N},\boldsymbol{Z}) \in R$, ale $(\boldsymbol{Z},\boldsymbol{N}) \notin R$), nie jest także relacją euklidesową ($(\boldsymbol{P},\boldsymbol{Z}) \in R$ i $(\boldsymbol{P},\boldsymbol{N}) \in R$, ale $(\boldsymbol{Z},\boldsymbol{N}) \notin R$).

Przykład 3.2

Relacja dana jest za pomocą tablicy:

	○	□	Δ	%	!
○	x	x			x
□					
Δ	x		x		x
%	x				
!		x		x	

$D(R) = \{\circ,\ \Delta,\ \%,\ !\}$

$D^{-1}(R) = \{\circ, \square, \Delta, \%, !\}$

Pary należące do tej relacji to:

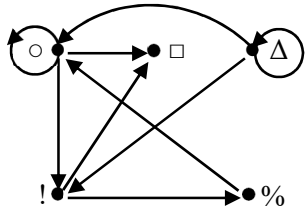
$R = \{(\circ,\circ), (\circ, \square), (\circ, !), (\Delta,\circ), (\Delta, \Delta), (\Delta, !), (\%,\circ), (!, \square), (!, \%)\}$

Relacja odwrotna i dopełnienie są następujące:

$R^{-1} = \{(\circ,\circ), (\square,\circ\ ), (!,\circ\ ), (\circ, \Delta\ ), (\Delta, \Delta), (!, \Delta\ ), (\circ, \%\ ), (\square, !), (\%, !)\}$

$R' = \{(\circ, \Delta), (\circ, \%), (\square,\circ), (\square, \square), (\square, \Delta), (\square, \%), (\square, !), (\Delta, \square),$
$(\Delta, \%), (\%, \square), (\%, \Delta), (\%, \%), (\%, !\ ), (!,\circ), (!, \Delta), (!, !)\}$

Graf tej relacji:



Relacja ta:

Nie jest zwrotna (np. $(!, \square) \notin R$).

Nie jest przeciwzwrotna ani asymetryczna (np. $(\circ,\circ) \in R$).

Nie jest symetryczna (np. $(\Delta,\circ) \in R$, ale $(\circ, \Delta) \notin R$).

Nie jest przechodnia (np. $(\circ, !) \in R$ oraz $(!, \%) \in R$, ale $(\circ, \%) \notin R$).

Nie jest euklidesowa (np. $(\circ, \square) \in R$ oraz $(\circ, !) \in R$, ale $(\square, !\ ) \notin R$).

Nie jest również liniowa ani spójna (np. $(\square, \Delta\ ) \notin R$, ani $(\Delta, \square\ ) \notin R$, ani $\Delta = \square$).

Jest za to antysymetryczna (symetria zachodzi tylko dla par $(\circ,\circ)$ oraz (Δ, Δ)).

Przykład 3.3

Dane są pary elementów będących ze sobą w relacji:

$R = \{(1,2), (2,1), (2,3), (2,4), (2,5), (2,6), (3,2), (3,3), (4,2), (5,2), (6,2)\}$

Podać dziedzinę, przeciwdziedzinę oraz dopełnienie relacji. Przedstawić tablicę, narysować graf oraz zbadać własności tej relacji.

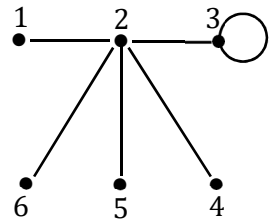
$D(R) = D^{-1}(R) = \{1,2,3,4,5,6\}$

$R^{-1} = \{(1,1), (1,3), (1,4), (1,5), (1,6), (2,2), (3,1), (3,4), (3,5), (3,6), (4,1),$
$(3,3), (3,5), (3,6), (4,1), (4,3), (4,4), (4,5), (4,6), (5,1), (5,3), (5,4), (5,5),$
$(5,6), (6,1), (6,3), (6,4), (6,5), (6,6)\}$

$D^{-1}(R) = R^{-1} \backslash \{(3,3)\}$

Tablica i graf tej relacji są następujące:

	1	2	3	4	5	6
1		x				
2	x		x	x	x	x
3		x	x			
4		x				
5		x				
6		x				



Jak widać, tablica tej relacji jest symetryczna względem głównej przekątnej, więc relacja również jest symetryczna. Wobec tego graf relacji jest grafem nieskierowanym, tzn. każda krawędź oznacza, że relacja zachodzi w obie strony.
Jakie inne własności ma przedstawiona relacja?
Nie jest to relacja zwrotna (np. $(2,2) \notin R$) ani przeciwzwrotna ($(3,3) \in R$). Nie jest również relacją przechodnią (np. $(3,2) \in R \ \wedge (2,4) \in R$, ale $(3,4) \notin R$) ani euklidesową (np. $(2,3) \in R$ oraz $(2,4) \in R$, ale $(3,4) \notin R$), ani liniową czy spójną (np. $(1,5) \notin R$ i $(5,1) \notin R$ i $5 \neq 1$).
Ponadto relacja ta nie spełnia również własności asymetrii oraz antysymetrii (np. $(2,4) \in R$ i $(4,2) \in R$, ale $2 \neq 4$).

3.2. Relacja kongruencji

Arytmetyka modularna (inaczej arytmetyka reszt) to system liczb całkowitych, w którym liczby „zawijają się" po osiągnięciu pewnej wartości nazywanej modułem, często określanej terminem *modulo* (skracane *mod*) [5]. Swoje początki zawdzięcza Carlowi Friedrichowi Gaussowi, który przedstawił arytmetykę reszt w swoim dziele z 1801 r. *Badania arytmetyczne*. Arytmetyka modularna pojawia się tam, gdzie pojawia się powtarzalność i cykliczność. Ma liczne zastosowania, m.in. zasada działania szyfru RSA opiera się na arytmetyce modularnej.

Definicja 3.1

Niech m będzie liczbą naturalną większą od 1. Liczba całkowita a przystaje do liczby całkowitej b modulo m, jeśli liczba $a - b$ jest podzielna przez liczbę m. Zależność można zapisać jako $a \equiv b (\mathrm{mod}\ m)$ i jest to kongruencja.

Lemat

Warunek $a \equiv b (\mathrm{mod}\ m)$ jest spełniony wtedy i tylko wtedy, gdy liczby a i b dają równe reszty z dzielenia przez m.

Z powyższej definicji i lematu wynikają własności kongruencji:

1. dla każdej liczby całkowitej a, $a \equiv a(\mathrm{mod}\, m)$;
2. jeśli $a \equiv b(\mathrm{mod}\, m)$, to $b \equiv a(\mathrm{mod}\, m)$;
3. jeśli $a \equiv b(\mathrm{mod}\, m)$ oraz $b \equiv c(\mathrm{mod}\, m)$, to $a \equiv c(\mathrm{mod}\, m)$.

Zaletą kongruencji jest to, że można je traktować tak jak równania.

Twierdzenie 3.1

Niech a, b, c, d będą liczbami całkowitymi, a m i k liczbami całkowitymi dodatnimi, przy czym $m > 1$. Wówczas jeśli $a \equiv b(\mathrm{mod}\, m)$, to

$a + c \equiv b + c(\mathrm{mod}\, m)$;

$ac \equiv bc(\mathrm{mod}\, m)$ oraz $ac \equiv bc(\mathrm{mod}\, mc)$;

$a^k \equiv b^k(\mathrm{mod}\, m)$.

Jeśli natomiast $a \equiv b(\mathrm{mod}\, m)$ oraz $c \equiv d(\mathrm{mod}\, m)$, to

$a + c \equiv b + c(\mathrm{mod}\, m)$;

$ac \equiv bc(\mathrm{mod}\, m)$.

Twierdzenie 3.2

Założono, że $a \equiv b(\mathrm{mod}\, m)$, oraz przyjęto, że liczby a i b są podzielne przez liczbę całkowitą dodatnią d.

Jeśli liczba m jest podzielna przez d, to $\frac{a}{d} \equiv \frac{b}{d}\left(\mathrm{mod}\, \frac{m}{d}\right)$.

Jeśli liczby m i d są względnie pierwsze, to $\frac{a}{d} \equiv \frac{b}{d}(\mathrm{mod}\, m)$.

Dowody *Lematu*, *Twierdzenia 3.1* i *Twierdzenia 3.2* można m.in. znaleźć w [6].

Definicja 3.2 [7]

Jeśli $x \equiv a(\mathrm{mod}\, m)$, to liczba a nazywana jest resztą z x modulo m. **Klasą reszt modulo m** reprezentowaną przez a nazywa się zbiór wszystkich liczb całkowitych przystających do a modulo m i oznacza się przez $[a]_n$.

Definicja 3.3 [7]

Zbiór wszystkich klas reszt modulo m oznacza się przez Z_m.

Przykład 3.4

Wyznaczyć cztery klasy reszt modulo 4.

Istnieją cztery klasy reszt modulo 4:

$[0]_4 = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$

$[1]_4 = \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}$

$[2]_4 = \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}$

$[3]_4 = \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}$

Przykład 3.5

Czy liczba $5^{1454} + 6^{2709}$ jest podzielna przez 11? [6].

W rozwiązaniu zadania można skorzystać z kongruencji.

$5 \equiv 5 (\mathrm{mod}\ 11)$

$5^2 \equiv 5^2 (\mathrm{mod}\ 11) \equiv 3 (\mathrm{mod}\ 11)$

$5^{10} \equiv 3^5 (\mathrm{mod}\ 11) \equiv 243 (\mathrm{mod}\ 11) \equiv 1 (\mathrm{mod}\ 11).$

Korzystając z okresowości, własności potęg i powyższych kongruencji, otrzymuje się

$5^{1454} \equiv (5^{10})^{145} \cdot (5^2)^2 \equiv 1 \cdot 9 \equiv 9 (\mathrm{mod}\ 11).$

$6 \equiv 6 (\mathrm{mod}\ 11)$

$6^2 \equiv 6^2 (\mathrm{mod}\ 11) \equiv 3 (\mathrm{mod}\ 11)$

$6^{10} \equiv 3^5 (\mathrm{mod}\ 11) \equiv 243 (\mathrm{mod}\ 11) \equiv 1 (\mathrm{mod}\ 11).$

I ponownie korzystając z okresowości, własności potęg i powyższych kongruencji, uzyskuje się

$6^{2709} \equiv (6^{10})^{270} \cdot (6^2)^4 \cdot 6 \equiv 1 \cdot 4 \cdot 6 \equiv 3 (\mathrm{mod}\ 11).$

Podstawiając otrzymane reszty do liczby

$5^{1454} + 6^{2709} \equiv 9 + 3 (\mathrm{mod}\ 11)\ \equiv 1 (\mathrm{mod}\ 11).$

Liczba $5^{1454} + 6^{2709}$ nie jest podzielna przez 11, ponieważ reszta z dzielenia tej liczby przez 11 wynosi 1.

Przykład 3.6

Wyznaczyć dwie ostatnie cyfry zapisu dziesiętnego liczby $99^{99} + 49^{49}$ [8].

Dwie ostanie cyfry można otrzymać, dzieląc liczbę przez 100.

$99 \equiv 99 (\mathrm{mod}\ 100)$

$99^2 \equiv 99^2 (\mathrm{mod}\ 100) \equiv 9801 (\mathrm{mod}\ 100) \equiv 1 (\mathrm{mod}\ 100)$

Wykorzystując powyższe kongruencje, można wyznaczyć dwie ostatnie cyfry pierwszej potęgi

$99^{99} \equiv (99^2)^{49} \cdot 99 \equiv 1 \cdot 99 \equiv 99 (\mathrm{mod}\ 100)$

Analogicznie dla drugiej potęgi

$49 \equiv 49 (\mathrm{mod}\ 100)$

$49^2 \equiv 49^2 (\mathrm{mod}\ 100) \equiv 2401 (\mathrm{mod}\ 100) \equiv 1 (\mathrm{mod}\ 100)$

$49^{49} \equiv (49^2)^{24} \cdot 49 \equiv 1 \cdot 49 \equiv 49 (\mathrm{mod}\ 100)$

Suma powyższych dwóch szukanych kongruencji wynosi

$99^{99} + 49^{49} \equiv 99 + 49 (\mathrm{mod}\ 100) \equiv 48 (\mathrm{mod}\ 100)$

Dwie ostatnie cyfry zapisu dziesiętnego liczby to 48.

Przykład 3.7

Uzasadnić, że liczba $943^{87} - 243^{87}$ jest podzielna przez 4 [9].

$943 \equiv 3 (\mathrm{mod}\ 4)$

$943^2 \equiv 3^2 \equiv 1 (\mathrm{mod}\ 4)$

$943^{87} \equiv (943^2)^{43} \cdot 943 \equiv 3 (\mathrm{mod}\ 4)$

$243 \equiv 3 (\mathrm{mod}\ 4)$

$243^2 \equiv 3^2 \equiv 1 (\mathrm{mod}\ 4)$

$243^{87} \equiv (243^2)^{43} \cdot 243 \equiv 3 (\mathrm{mod}\ 4)$

Potęgi z dzielenia przez 4 otrzymują te same reszty. Różnica tych potęg jest podzielna przez 4. Więcej tego typu zadań w [1].

Przykład 3.8

Udowodnić, że liczba $2^{5^1} + 2^{5^2} + 2^{5^3} + \cdots + 2^{5^{2021}} + 2^{5^{2022}}$ przy dzieleniu przez 100 daje resztę 4 [8].

Liczba $2^{5^1} \equiv 32 (\mathrm{mod}\ 100)$.

Należy pokazać, że prawdziwa jest kongruencja $2^{5^k} \equiv 32 (\mathrm{mod}\ 100)$ dla każdego naturalnego k. Do udowodnienia ww. kongruencji najlepiej zastosować indukcję matematyczną.

(S):

$k = 1$: $2^{5^1} \equiv 32 (\mathrm{mod}\ 100)$

Kongruencja spełniona.

(ZI): $\forall_{k\in \boldsymbol{N}_+} 2^{5^k} \equiv 32(\mathrm{mod}\ 100)$

(TI): $\forall_{k+1\in \boldsymbol{N}_+} 2^{5^{k+1}} \equiv 32(\mathrm{mod}\ 100)$

Dowód

$$2^{5^{k+1}} \equiv \left(\underbrace{2^{5^k}}_{\text{z założenia}} \right)^5 \equiv 32^5 \equiv 32(\mathrm{mod}\ 100).$$

□

Stąd liczba $2^{5^1} + 2^{5^2} + 2^{5^3} + \cdots + 2^{5^{2021}} + 2^{5^{2022}} \equiv 2022 \cdot 32 \equiv 22 \cdot 32 \equiv$ $\equiv 4(\mathrm{mod}\ 100)$. Liczba $2^{5^1} + 2^{5^2} + 2^{5^3} + \cdots + 2^{5^{2021}} + 2^{5^{2022}}$ przy dzieleniu przez 100 daje resztę 4.

□

Przykład 3.9

Wykazać, że dla każdej liczby naturalnej n liczba $5^{2n+1} + 2^{n+4} + 2^{n+1}$ jest podzielna przez 23 [8].

Liczbę można przedstawić jako sumę dwóch liczb 5^{2n+1} i $2^{n+4} + 2^{n+1}$. W przypadku pierwszej liczby otrzymano kongruencję

$$5^{2n+1} \equiv 25^n \cdot 5 \equiv 2^n \cdot 5(\mathrm{mod}\ 23)$$

Drugą liczbę zapisano

$$2^{n+4} + 2^{n+1} \equiv 2^n \cdot 18(\mathrm{mod}\ 23)$$

Zatem liczba

$5^{2n+1} + 2^{n+4} + 2^{n+1} \equiv 2^n \cdot 5 + 2^n \cdot 18 \equiv 2^n \cdot 23 \equiv 0(\mathrm{mod}\ 23)$

Liczba $5^{2n+1} + 2^{n+4} + 2^{n+1}$ jest podzielna przez 23.

Przykład 3.10

Wyznacz wszystkie takie pary (a, b) dodatnich liczb całkowitych, że liczba $a + b$ jest liczbą pierwszą oraz liczba $a^3 + b^3$ jest podzielna przez 3 [10].

W pozycji literaturowej [10] zaprezentowano kilka rozwiązań tego zadania. W tym przykładzie będzie pokazane tylko to, które bezpośrednio nawiązuje do kongruencji.

Rozwiązanie zadania należy rozpocząć od wykazania, że liczby a i a^3 dają takie same reszty z dzielenia przez 3. W tym celu zastosowano własności kongruencji.

Każda liczba całkowita a spełnia jedną z zależności:

$a \equiv 0(\mathrm{mod}\ 3), \qquad a \equiv 1(\mathrm{mod}\ 3), \qquad a \equiv 2(\mathrm{mod}\ 3).$

Po podniesieniu obustronnym powyższych kongruencji do potęgi 3, otrzymuje się:

$a^3 \equiv 0(\mathrm{mod}\ 3), \qquad a^3 \equiv 1(\mathrm{mod}\ 3), \qquad a^3 \equiv 2(\mathrm{mod}\ 3).$

Stąd $a^3 \equiv a(\mathrm{mod}\ 3)$, co należało wykazać. To oznacza, że liczby a i a^3dają takie same reszty z dzielenia przez 3. Tę samą własność mają liczby b i b^3. Liczby $a + b$ i $a^3 + b^3$ dają takie same reszty z dzielenia przez 3. Z faktu, że liczba $a^3 + b^3$ jest podzielna przez 3, można wnioskować, że liczba $a + b$ również. Wiadomo dodatkowo z treści zadania, że liczba $a + b$ jest pierwsza. Łącząc te dwa fakty, zauważyć można, że możliwa jest tylko jedna wartość sumy $a + b$, $a + b = 3$. Dwie pary liczb spełniają te warunki: $(1, 2)$ i $(2, 1)$. Sprawdzenie potwierdza, że obie pary spełniają warunki zadania.

Przykład 3.11

Znajdź wszystkie takie liczby pierwsze p, dla których liczba $p^2 + 2$ także jest pierwsza [11].

W zadaniu wykorzystano spostrzeżenie, że jedyną liczbą pierwszą podzielną przez liczbę pierwszą p jest p.

Liczba p jest nie mniejsza od 2. Jeśli liczba p dzieli się przez 3, to musi być równa 3, gdyż jest to liczba pierwsza. Wtedy $p^2 + 2 = 11$ również jest liczbą pierwszą. Teraz kolej na sprawdzenie, co w przypadku, gdy liczba p nie dzieli się przez 3. Wtedy możliwe są dwa przypadki $p \equiv 1\ (\mathrm{mod}\ 3)$ lub $p \equiv 2\ (\mathrm{mod}\ 3)$. W obu przypadkach otrzymuje się $p^2 \equiv 1\ (\mathrm{mod}\ 3)$, a co za tym idzie $p^2 + 2 \equiv 0\ (\mathrm{mod}\ 3)$. Liczba $p^2 + 2$ jest podzielna przez 3. Liczba $p^2 + 2$ musi być złożona, ponieważ jest większa od 3. Jedyną liczbą p spełniającą warunki zadania jest $p = 3$.

Przykład 3.12

Wyznaczyć wszystkie liczby naturalne $n \geq 1$, dla których liczba $\frac{1^n + 2^{n+1} + 3^{n+2}}{1+2+3}$ jest liczbą naturalną [6].

Należy pokazać, że licznik jest liczbą podzielną przez 6 dla każdej liczby naturalnej $n \geq 1$. Najlepiej rozpatrzyć każdą potęgę z licznika osobno.

Potęga $1^n \equiv 1(\mathrm{mod}\ 6)$.

Potęga $2^2 \equiv 1(\mathrm{mod}\ 6)$.

Po podniesieniu kongruencji stronami do potęgi k-tej (liczba całkowita nieujemna) otrzymano

$2^{2k} \equiv 1(\mathrm{mod}\ 3)$.

Następnie należy pomnożyć dwukrotnie przez 2

$2^{2k+1} \equiv 2(\mathrm{mod}\ 6)$

$2^{2k+2} \equiv 4(\mathrm{mod}\ 6).$

Po podstawieniu do dwóch powyższych kongruencji odpowiednio $n = 2k$ i $n = 2k + 1$ potęga przyjmuje postać

$$2^{n+1} \equiv \begin{cases} 2\ (\mathrm{mod}\ 6), & \text{jeśli } n \text{ jest liczbą parzystą} \\ 4\ (\mathrm{mod}\ 6), & \text{jeśli } n \text{ jest liczbą nieparzystą} \end{cases}$$

Następnie w podobny sposób trzeba znaleźć reszty dla potęg 3.

$3 \equiv 1(\mathrm{mod}\ 2)$

$3^{n+1} \equiv 1(\mathrm{mod}\ 2)$

$3^{n+2} \equiv 3(\mathrm{mod}\ 6)$

Podsumowując: jeśli n jest liczbą parzystą, to liczba

$1^n + 2^{n+1} + 3^{n+2} \equiv 1 + 2 + 3 = 0(\mathrm{mod}\ 6)$

Liczba $1^n + 2^{n+1} + 3^{n+2}$ jest podzielna przez 6.

Jeśli n jest liczbą nieparzystą, to

$1^n + 2^{n+1} + 3^{n+2} \equiv 1 + 4 + 3 = 2(\mathrm{mod}\ 6)$

W tym przypadku liczba $1^n + 2^{n+1} + 3^{n+2}$ nie jest podzielna przez 6.

Przykład 3.13

Wykazać, że liczba naturalna n jest podzielna przez 3 wtedy i tylko wtedy, gdy suma cyfr liczby n jest podzielna przez 3.

Liczba n jest postaci

$$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$$

gdzie $k \in \boldsymbol{N}$, $a_k, a_{k-1}, \ldots, a_1, a_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ i $a_k \neq 0$

Można zauważyć, że jeśli $10 \equiv 1(\mathrm{mod}\ 3)$, to wtedy $10^b \equiv 1(\mathrm{mod}\ 3)$ dla dowolnego $b \in \boldsymbol{N}$.

Wykorzystując powyższe fakty, otrzymano

$a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0(\mathrm{mod}\ 3)$

Stąd liczba naturalna n jest podzielna przez 3 wtedy i tylko wtedy, gdy suma jej cyfr jest podzielna przez 3. Analogicznie wykazano podzielność przez 9 w [8].

Przykład 3.14

Niech x_1 i x_2 będą pierwiastkami równania $x^2 - 6x + 1 = 0$. Wykazać, że dla każdej liczby naturalnej dodatniej n suma $x_1^n + x_2^n$ jest liczbą całkowitą niepodzielną przez 5 [12].

Można oznaczyć $x_1^n + x_2^n = a_n$, dla $n \in \boldsymbol{N}$.

Na początku obliczono siedem pierwszych wyrazów ciągu (będą potrzebne w dalszej części)

$a_1 = x_1 + x_2 = 6$

$a_2 = x_1^2 + x_2^2 = 34$

$a_3 = x_1^3 + x_2^3 = 198$

$a_4 = x_1^4 + x_2^4 = 1154$

$a_5 = x_1^5 + x_2^5 = 6726$

$a_6 = x_1^6 + x_2^6 = 39202$

$a_7 = x_1^7 + x_2^7 = 228486$

Następnie pomnożono rozpatrywane równanie kwadratowe przez x_1^n i x_2^n i otrzymano

$x_1^{n+2} - 6x_1^{n+1} + x_1^n = 0$

$x_2^{n+2} - 6x_2^{n+1} + x_2^n = 0$

Po dodaniu równań stronami otrzymano wzór rekurencyjny dla $n \in \boldsymbol{N}$

$a_{n+2} = 6a_{n+1} - a_n$

Z powyższego wzoru oraz z obliczonych a_1, a_2, a_3, a_4, a_5, a_6, a_7 wynika, że wszystkie wyrazy ciągu a_n są liczbami całkowitymi.

Rozwiązując kongruencję $\mathrm{mod}\ 5$ dla $a_{n+2} = 6a_{n+1} - a_n$, otrzymano

$a_{n+2} = a_{n+1} - a_n (\mathrm{mod}\ 5)$

Z reszt $1, 4, 3, 4, 1, 2, 1$ odpowiednio dla a_1, a_2, a_3, a_4, a_5, a_6, a_7 w $\mathrm{mod}\ 5$ i z ich okresowości wynika kongruencja

$a_{n+6} = a_n (\mathrm{mod}\ 5)$.

To oznacza, że żaden wyraz ciągu a_n nie jest podzielny przez 5, a co za tym idzie suma $x_1^n + x_2^n$ też nie jest podzielna.

3.3. Odwracalność kongruencji

Definicja 3.4

Odwrotnością elementu a modulo m, oznaczany przez a^{-1}, nazywa się taki element, że $aa^{-1} \equiv 1(\mathrm{mod}\ m)$ [13].

Przykład 3.15

Znaleźć odwrotność liczby 2 modulo 5.

Do znalezienia odwrotności a założono, że a i odwrotność a należą do zbioru $\{1, 2, 3, 4\}$. Odwrotnością liczby 2 modulo 5 jest liczba 3, ponieważ $2 \cdot 3 \equiv 1(\mathrm{mod}\ 5)$.

Twierdzenie 3.3 (kryterium odwracalności w arytmetyce zegarowej) [13]

Dodatnia liczba naturalna a jest odwracalna modulo m wtedy i tylko wtedy, gdy a oraz m są względnie pierwsze. W szczególności dla liczby pierwszej p każdy niezerowy element Z_p jest odwracalny.

Liczby względnie pierwsze to takie, dla których $NWD(a, m) = 1$. Natomiast Z_p oznacza zbiór reszt modulo liczba pierwsza p, $\{0, 1, 2, \dots, p-1\}$.

Przykład 3.16

Wyznaczyć $19^{-1}(\mathrm{mod}\ 62)$, stosując odwrotny algorytm Euklidesa.

Odwrotny algorytm Euklidesa zastosowano do liczb 19 i 62.

$62 = 3 \cdot 19 + 5$

$19 = 3 \cdot 5 + 4$

$5 = 1 \cdot 4 + 1$

Następnie

$$1 = 5 - 1 \cdot 4 = 5 - (19 - 3 \cdot 5) = 4 \cdot 5 - 19 = 4(62 - 3 \cdot 19) - 19$$
$$= 4 \cdot 62 - 12 \cdot 19 - 19 = \underbrace{4 \cdot 62}_{248} - \underbrace{13 \cdot 19}_{247}$$

zatem

$19 \cdot (-13) \equiv 1\ (\mathrm{mod}\ 62)$, czyli $19^{-1} \equiv -13 \equiv 49\ (\mathrm{mod}\ 62)$

3.4. Wybrane twierdzenia dotyczące kongruencji

Twierdzenie 3.4 (Wilsona)

Dla każdej liczby pierwszej p liczba $(p-1)!+1$ jest podzielna przez p.

Powyższe *Twierdzenie 3.4* można zapisać $(p-1)!+1 \equiv 0 \pmod{p}$. Można je stosować jako kryterium pierwszości. Niestety obliczenia silni są dość kłopotliwe i nie pomoże nam nawet wzór Stirlinga, który daje tylko wartość przybliżoną silni. Twierdzenie Wilsona może pomóc w rozstrzygnięciu, czy liczba jest pierwsza, czy złożona.

Przykład 3.17

Rozstrzygnąć, czy liczba $10!+1$ jest liczbą pierwszą, czy liczbą złożoną.

W tym celu należy wykorzystać twierdzenie Wilsona.

Należy pokazać, że liczba $10!+1=(11-1)!+1 \equiv 0(\mathrm{mod}\ 11)$.

$$10!+1 \equiv 36288001 \equiv 0 \pmod{11}$$

Można też zapisać $10!$ jako iloczyn liczb od 1 do 10, odpowiednio zapisanych parami

$$10! = [(1\cdot 10)]\cdot[(2\cdot 6)\cdot(3\cdot 4)\cdot(5\cdot 9)\cdot(7\cdot 8)] \equiv [-1]\cdot[1\cdot 1\cdot 1\cdot 1] \equiv -1(\mathrm{mod}\ 11)$$

Liczba $10!+1$ jest liczbą pierwszą.

Przykład 3.18

Znaleźć resztę z dzielenia liczby $102!$ przez 103.

Liczba 103 jest liczbą pierwszą.

W tym przypadku najlepiej skorzystać z kongruencji

$(p-1)! \equiv p-1 \equiv -1(\mathrm{mod}\ p)$.

Po zastosowaniu powyższej kongruencji otrzymano

$(102)! \equiv 102 \equiv -1(\mathrm{mod}\ 103) \equiv 102(\mathrm{mod}\ 103)$.

Reszta wynosi 102.

Twierdzenie 3.5 (małe twierdzenie Fermata)

Jeśli liczba pierwsza p nie dzieli liczby a, to $a^{p-1} \equiv 1(\mathrm{mod}\ p)$.

Twierdzenie to jest jednym z ważniejszych w teorii liczb sformułowanym przez Pierre'a de Fermata i jest podstawą dla testu pierwszości Fermata.

Przykład 3.19

Każda liczba naturalna a niepodzielna przez 31 spełnia kongruencję $a^{31} \equiv a(\mathrm{mod}\ 31)$. Kongruencja wynika z małego twierdzenia Fermata, które daje kongruencję $a^{30} \equiv 1(\mathrm{mod}\ 31)$. Pomnożenie stronami otrzymanej kongruencji przez a generuje kongruencję wyjściową.

Przykład 3.20

Znaleźć resztę z dzielenia 3^{9000} przez 19, korzystając z małego twierdzenia Fermata.

Liczby 3 i 19 są względnie pierwsze i pierwsze. Z małego twierdzenia Fermata wynika, że $3^{18} \equiv 1(\mathrm{mod}\ 19)$. Liczba $3^{9000} \equiv 3^{18} \equiv 1(\mathrm{mod}\ 19)$. Szukana reszta wynosi 1.

Z małym twierdzeniem Fermata mają związek **liczby Carmichaela**. Liczby Carmichaela to takie liczby naturalne złożone, dla których teza małego twierdzenia Fermata jest prawdziwa.

Liczba naturalna n jest liczbą Carmichaela wtedy i tylko wtedy, gdy:

a) Jest liczbą złożoną.

b) Dla każdej liczby naturalnej a z przedziału $1 < a < n$ względnie pierwszej z n, liczba $a^{n-1} - 1$ jest podzielna przez n.

Każda liczba Carmichaela jest liczbą pseudopierwszą, a nie na odwrót. Liczby Carmichaela charakteryzuje to, że:

a) Są nieparzyste.

b) Przy rozkładzie na czynniki pierwsze żaden czynnik nie występuje w potędze wyższej niż pierwsza.

c) Każda jest iloczynem przynajmniej trzech liczb pierwszych.

Najmniejszą liczbą Carmichaela jest $561 = 3 \cdot 11 \cdot 17$.

W [14] Jack Chernick podał wzór dla liczb Carmicheala o trzech czynnikach pierwszych.

Podstawiając kolejne liczby naturalne za n, wyznacza się liczbę $(6n + 1)(12n + 1)(18n + 1)$. Jeśli wszystkie trzy czynniki liczby są liczbami pierwszymi, to liczba $(6n + 1)(12n + 1)(18n + 1)$ jest liczbą Carmichaela.

Przykład 3.21

Sprawdzić, czy liczby postaci $(6n + 1)(12n + 1)(18n + 1)$ są liczbami Carmichaela dla $n \in \{1, 2\}$.

Dla $n = 1$ jest to $1729 = 7 \cdot 13 \cdot 19$ i jest to liczba Carmichaela.

Dla $n = 2$ jest to $12\,025 = 13 \cdot 25 \cdot 37$ i nie jest to liczba Carmichaela, ponieważ liczba 25 jest liczbą złożoną.

Przykład 3.22

Z małego twierdzenia Fermata wynika, że dla dowolnej liczby naturalnej a względnie pierwszej z 1105 zachodzą kongruencje:

$a^4 \equiv 1(\mathrm{mod}\ 5), \qquad a^{12} \equiv 1(\mathrm{mod}\ 13), \qquad a^{16} \equiv 1(\mathrm{mod}\ 17).$

Wywnioskować, że dla dowolnej liczby naturalnej a względnie pierwszej z 1105 zachodzi $a^{1104} \equiv 1(\mathrm{mod}\ 1105)$.

Liczba 1105 jest liczbą Carmichaela i ma trzy czynniki pierwsze $5 \cdot 13 \cdot 17$.

Podnosząc zadane kongruencje do odpowiednich potęg, otrzymuje się

$a^4 \equiv 1(\mathrm{mod}\ 5) \Rightarrow a^{1104} = (a^4)^{276} \equiv 1(\mathrm{mod}\ 5)$

$a^{12} \equiv 1(\mathrm{mod}\ 13) \Rightarrow a^{1104} = (a^{12})^{92} \equiv 1(\mathrm{mod}\ 13)$

$a^{16} \equiv 1(\mathrm{mod}\ 17) \Rightarrow a^{1104} = (a^{16})^{69} \equiv 1(\mathrm{mod}\ 17)$

a więc $a^{1104} \equiv 1\big(\mathrm{mod}\ (5 \cdot 13 \cdot 17)\big)$ dla wszystkich liczb całkowitych a względnie pierwszych z: $5, 13, 17, 1105$.

Rzędem elementu a modulo p nazywa się najmniejszą liczbę k o własności $a^k \equiv 1(\mathrm{mod}\ p)$, gdzie liczba naturalna a jest niepodzielna przez liczbę pierwszą p, k to dodatnia liczba naturalna taka, że $k \leq p - 1$. Rząd elementu a modulo p oznacza się przez $\mathrm{ord}_p a$.

Przykład 3.23

Wyznaczyć rząd elementu 3 modulo 5.

$3^1 = 3 = 0 \cdot 5 + 3 \equiv 3(\mathrm{mod}\ 5)$

$3^2 = 9 = 1 \cdot 5 + 4 \equiv 4(\mathrm{mod}\ 5)$

$3^3 = 27 = 5 \cdot 5 + 2 \equiv 2(\mathrm{mod}\ 5)$

$3^4 = 81 = 16 \cdot 5 + 1 \equiv 1(\mathrm{mod}\ 5)$

Najmniejszą dodatnią liczbą całkowitą k taką, że $3^k \equiv 1(\mathrm{mod}\ 5)$ jest 4, czyli $\mathrm{ord}_5 3 = 4$.

Element rzędu $p - 1$ nazywa się **pierwiastkiem pierwotnym modulo p**. Pierwiastki pierwotne to takie liczby mające w cyklu wszystkie liczby od 1 do $p - 1$, które są względnie pierwsze.

Przykład 3.24

Czy 3 jest pierwiastkiem pierwotnym modulo 5?

Tak, ponieważ 3 ma w cyklu wszystkie liczby od 1 do 4.

Przykład 3.25

Dla liczby pierwszej $p = 5$ zbadać kolejne liczby od 1 do 4 i ich potęgi, zacząć od pierwszej, a skończyć, gdy cykl zacznie się powtarzać. Wyznaczyć pierwiastki pierwotne modulo 5. Określić rząd elementu a modulo 5.

Dla $a = 1$, $1 \equiv 1 (\mathrm{mod}\ 5)$ $\quad \mathrm{ord}_5 1 = 1$

Dla $a = 2$, $2^1 \equiv 2 (\mathrm{mod}\ 5)$

$2^2 \equiv 4 (\mathrm{mod}\ 5)$

$2^3 \equiv 3 (\mathrm{mod}\ 5)$

$2^4 \equiv 1 (\mathrm{mod}\ 5)$ $\quad \mathrm{ord}_5 2 = 4$

Dla $a = 3$, $3^1 \equiv 3 (\mathrm{mod}\ 5)$

$3^2 \equiv 4 (\mathrm{mod}\ 5)$

$3^3 \equiv 2 (\mathrm{mod}\ 5)$

$3^4 \equiv 1 (\mathrm{mod}\ 5)$ $\quad \mathrm{ord}_5 3 = 4$

Dla $a = 4$, $4^1 \equiv 4 (\mathrm{mod}\ 5)$

$4^2 \equiv 1 (\mathrm{mod}\ 5)$ $\quad \mathrm{ord}_5 4 = 2$

Ostatecznie dla $p = 5$ pierwiastkami pierwotnymi są $a = 2$ i $a = 3$.

Twierdzenie 3.6 (chińskie twierdzenie o resztach) [15]

Jeśli $a_1, a_2, \dots, a_n$ są liczbami całkowitymi parami względnie pierwszymi oraz $b_1, b_2, \dots, b_n$ liczbami całkowitymi, to istnieje taka liczba x, że

$x \equiv b_1 (\mathrm{mod}\ a_1)$

$x \equiv b_2 (\mathrm{mod}\ a_2)$

$\vdots$

$x \equiv b_n (\mathrm{mod}\ a_n)$

oraz $x \leq a_1 \cdot a_2 \cdot a_3 \cdot \dots \cdot a_n$

Przykład 3.26

Rozwiązać układ kongruencji:

$$\begin{cases} x \equiv 1(\mathrm{mod}\ 7) \\ x \equiv 5(\mathrm{mod}\ 12) \end{cases}$$

Rozwiązaniem kongruencji $x \equiv 1(\mathrm{mod}\ 7)$ jest liczba $1 + 7c$, gdzie c jest dowolną liczbą całkowitą. Następnie używając tzw. metody generowania kolejnych wielokrotności, poszukuje się najmniejszego c, dla którego x postaci $x = 1 + 7c$ spełnia drugą kongruencję. Najmniejsze takie c to 4. Z dwóch pierwszych kongruencji otrzymuje się kongruencję $x \equiv 29(\mathrm{mod}\ 84)$. Czyli najmniejsze rozwiązanie układu kongruencji to 29, a rozwiązanie ogólne to $29 + 84d$, gdzie d jest dowolną liczbą całkowitą.

Przykład 3.27

Rozwiązać układ kongruencji:

$$\begin{cases} x \equiv 2(\mathrm{mod}\ 3) \\ x \equiv 1(\mathrm{mod}\ 4) \\ x \equiv 3(\mathrm{mod}\ 11) \end{cases}$$

Podobnie jak w *Przykładzie 3.26* dobrze jest wyznaczyć ogólne rozwiązanie pierwszej kongruencji, będzie to liczba postaci $2 + 3c$, gdzie c jest dowolną liczbą całkowitą. Podstawiając za c kolejne liczby całkowite i jednocześnie sprawdzając, która liczba postaci $2 + 3c$ spełnia kongruencję $x \equiv 1(\mathrm{mod}\ 4)$, otrzymuje się dla $c = 1$ liczbę 5. Zatem dwie pierwsze kongruencje zapisuje się jako kogruencję $x \equiv 5(\mathrm{mod}\ 12)$. Tym razem rozwiązaniem jest liczba postaci $x \equiv 5 + 12d$, gdzie d jest dowolną liczbą całkowitą. Postępując w taki sam sposób jak w przypadku drugiej kongruencji, wyznacza się liczbę spełniającą trzecią kongruencję. Dla $d = 9$ szukana liczba to 113. Rozwiązanie ogólne to $113 + 132e$, gdzie e jest dowolną liczbą całkowitą.

Twierdzenie 3.7 (prawo skracania) [13]

Jeżeli a jest względnie pierwsze z m, to zachodzi prawo skracania

$$ab \equiv ac(\mathrm{mod}\ m) \ \Rightarrow\ b \equiv c(\mathrm{mod}\ m)$$

Przykład 3.28

Rozwiązać kongruencję $8x \equiv 4\ (\mathrm{mod}\ 21)$ z niewiadomą x.

Na początku w celu uproszczenia kongruencji stosuje sią prawo skracania. Można je zastosować, gdyż liczba 2 jest względnie pierwsza z 21.

Po skróceniu otrzymuje się kongruencję $2x \equiv 1(\mathrm{mod}\ 21)$.

Korzystając z algorytmu Euklidesa, otrzymuje się

$21 \equiv 10 \cdot 2 + 1$

$1 \equiv 21 - 10 \cdot 2$

Równania (wyjściowe i przekształcone) spełnia kongruencja $x \equiv 11(\mathrm{mod}\ 21)$. Najmniejszym rozwiązaniem kongruencji jest liczba 11, a rozwiązaniem ogólnym są liczby postaci $11 + 21d$, gdzie d jest dowolną liczbą całkowitą.

Przykład 3.29

Rozwiązać kongruencję $27x \equiv 6(\mathrm{mod}\ 67)$ z niewiadomą x.

Na początku w celu uproszczenia kongruencji stosuje sią prawo skracania. Można je zastosować, gdyż liczba 3 jest względnie pierwsza z 67.
Po skróceniu otrzymuje się kongruencję $9x \equiv 2(\mathrm{mod}\ 67)$. Aby rozwiązać tę kongruencję, rozwiązujemy kongruencję $9y \equiv 1(\mathrm{mod}\ 67)$, korzystając z algorytmu Euklidesa.

$67 \equiv 7 \cdot 9 + 4$

$9 \equiv 2 \cdot 4 + 1$

$1 \equiv 9 - 2 \cdot 4 = 9 - 2(67 - 7 \cdot 9) = 9 - 2 \cdot 67 + 14 \cdot 9 = 15 \cdot 9 - 2 \cdot 67$

Rozwiązaniami kongruencji $9y \equiv 1(\mathrm{mod}\ 67)$ są liczby $y \equiv 15(\mathrm{mod}\ 67)$. A zatem rozwiązaniem kongruencji zadanej są liczby $x \equiv 30(\mathrm{mod}\ 67)$. Najmniejszym rozwiązaniem kongruencji jest liczba 30, a rozwiązaniem ogólnym są liczby postaci $30 + 67d$, gdzie d jest dowolną liczbą całkowitą.
Więcej kongruencji i układów kongruencji w [2, 16].

Przykład 3.30

Rozwiązać równanie $x^2 - 4x - 5 = 0\ (\mathrm{mod}\ 17)$.

Powyższe równanie jest równoważne równaniu

$(x + 1)(x - 5) = 0\ (\mathrm{mod}\ 17)$

Rozwiązania równania to $x = 16\ (\mathrm{mod}\ 17)$ oraz $x = 5\ (\mathrm{mod}\ 17)$. Więcej zadań w [16].
Liczbę y nazywa się **pierwiastkiem kwadratowym** liczby x w pierścieniu $\mathbb{Z}_m$, jeśli

$x = y^2(\mathrm{mod}\ m)$

Przykład 3.31

Ile pierwiastków kwadratowych ma liczba 2 w $\mathbb{Z}_7$? Wyznaczyć je.

W $\mathbb{Z}_7$ pierwiastki kwadratowe, o ile istnieją, należą do zbioru $\{0, 1, 2, 3, 4, 5, 6\}$. Liczba 2 ma dwa pierwiastki kwadratowe 3 oraz 4, ponieważ $3^2(\mathrm{mod}\ 7) = 4^2(\mathrm{mod}\ 7) = 2$. Więcej zadań w [16].

3.5. Wybrane testy pierwszości

Jest wiele testów pierwszości. Najbardziej popularne testy to: sito Eratostenesa, test Lucasa–Lehmera i test Rabina–Millera. Są to najbardziej znane i nieskomplikowane testy. W tym rozdziale zostaną opisane dwa ostatnie z wymienionych.

Test Lucasa–Lehmera

Test Lucasa–Lehmera jest to test pierwszości, za pomocą którego można wykrywać liczby pierwsze Mersenne'a.

Wykazuje się, że dla nieparzystych $p > 1$ liczba $2^p - 1$ jest liczbą pierwszą wtedy i tylko wtedy, gdy $2^p - 1$ dzieli $S(p-1)$, gdzie funkcja $S(k)$ jest określona rekurencyjnie

$$\begin{cases} S(1) = 4 \\ S(k+1) = (S(k))^2 - 2 \end{cases}$$

Przykład 3.32

Zbadać, czy liczba $2^7 - 1$ jest liczbą pierwszą.

Liczba $p = 7$ spełnia warunki testu Lucasa–Lehmera. Jest większa od 1 i nieparzysta.

$2^7 - 1 = 127$

$S(1) \equiv 4 (\mathrm{mod}\ 127)$

$S(2) \equiv 4^2 - 2 \equiv 14 (\mathrm{mod}\ 127)$

$S(3) \equiv 14^2 - 2 \equiv 194 \equiv 67 (\mathrm{mod}\ 127)$

$S(4) \equiv 67^2 - 2 \equiv 4487 \equiv 42 (\mathrm{mod}\ 127)$

$S(5) \equiv 42^2 - 2 \equiv 1762 \equiv 111 (\mathrm{mod}\ 127)$

$S(6) \equiv 111^2 - 2 \equiv 12319 \equiv 0 (\mathrm{mod}\ 127)$

Zatem 127 dzieli $S(6)$, więc liczba $2^7 - 1$ jest liczbą pierwszą.

Przykład 3.33

Wykazać, że liczba $2^{11} - 1$ nie jest pierwsza.

Ponownie liczba $p = 11$ spełnia warunki testu Lucasa–Lehmera. Jest większa od 1 i nieparzysta.

$2^{11} - 1 = 2047$

$S(1) \equiv 4 (\mathrm{mod}\ 2047)$

$S(2) \equiv 4^2 - 2 \equiv 14 (\mathrm{mod}\ 2047)$

$S(3) \equiv 14^2 - 2 \equiv 194 (\mathrm{mod}\ 2047)$

$S(4) \equiv 194^2 - 2 \equiv 37\,634 \equiv 788 (\mathrm{mod}\ 2047)$

$S(5) \equiv 788^2 - 2 \equiv 620\,942 \equiv 701 (\mathrm{mod}\ 2047)$

$S(6) \equiv 701^2 - 2 \equiv 491\,399 \equiv 119 (\mathrm{mod}\ 2047)$

$S(7) \equiv 119^2 - 2 \equiv 14\,159 \equiv 1877 (\mathrm{mod}\ 2047)$

$S(8) \equiv 1877^2 - 2 \equiv 3\,523\,127 \equiv 240 (\mathrm{mod}\ 2047)$

$S(9) \equiv 240^2 - 2 \equiv 57\,598 \equiv 282 (\mathrm{mod}\ 2047)$

$S(10) \equiv 282^2 - 2 \equiv 79\,522 \equiv 1736 (\mathrm{mod}\ 2047)$

A zatem liczba $2^{11} - 1$ nie jest liczbą pierwszą, gdyż nie dzieli $S(10)$.

Test Rabina–Millera

Test ten nie jest doskonały. Ma w sobie pewien element losowości, dlatego śmiało można go zakwalifikować do testów probabilistycznych. Nie daje on pewności, że liczba rzeczywiście jest pierwsza, ale pozwala odróżnić liczby pierwsze od złożonych. Jego działanie opiera się na czterech krokach [15]:

1) wybór k, które jest liczbą naturalną spełniającą warunki $k \geq 2$ małych liczb $a < N$ i względnie pierwszych z N;
2) zapisanie $N - 1$ w postaci $2^s d$, gdzie d jest liczbą nieparzystą;
3) sprawdzenie, czy zachodzi jeden z warunków $a^d \equiv 1 (\mathrm{mod}\ N)$ lub $a^{2^r d} \equiv -1 (\mathrm{mod}\ N)$ dla $0 \leq r < s$;
4) jeśli dla pewnego a nie zachodzi jeden z podanych powyżej warunków, to należy uznać N za złożone. Jeśli natomiast dla pewnego a zachodzi jeden z podanych warunków, to uważa się N za pierwsze.

Prawdopodobieństwo błędu wynosi $\left(\frac{1}{4}\right)^k$.

Więcej na temat testów pierwszości w [7, 13, 15].

Przykład 3.34

Zastosować test Rabina–Millera do liczby 89.

Na początku zapisuje się liczbę w postaci $N - 1 = 2^3 \cdot 11$

Najlepiej zacząć od $a = 2$.

$2^{11} \equiv 1 (\mathrm{mod}\ 89)$

Dla $a = 2$ spełniony jest pierwszy warunek.

Teraz kolej na $a = 3$

$3^{11} \equiv 37 (\mathrm{mod}\ 89)$

$3^{22} \equiv 34 (\mathrm{mod}\ 89)$

$3^{44} \equiv 88 \equiv -1 (\mathrm{mod}\ 89)$

Dla $a = 3$ spełniony jest drugi warunek.

Dla zwiększenia prawdopodobieństwa bada się jeszcze $a = 4$.

$4^{11} \equiv (2^2)^{11} \equiv (2^{11})^2 \equiv 1 (\mathrm{mod}\ 89)$

Spełniony warunek pierwszy.

Prawdopodobieństwo, że liczba 89 jest pierwsza, wynosi $1 - \left(\frac{1}{4}\right)^3 = \frac{63}{64} \approx 98\%$, tak też jest w istocie.

3.6. Wykrywanie i korygowanie błędów

W tym podrozdziale zaprezentowane zostanie ciekawe zastosowanie teorii kongruencji do wykrywania i korygowania błędów.

Metody polegają na szukaniu błędów za pomocą sprawdzania cyfr i porównywania ich z liczbami identyfikującymi. W taki sposób nadawane są i sprawdzane m.in. numery PESEL, REGON, NIP, kody kreskowe UPC (z ang. *Universal Product Code*) czy numery ISBN (z ang. *International Standard Book Number*) na wydawanych książkach i wiele innych.

Numery ISBN

Od 2007 r. obowiązują 13-cyfrowe numery ISBN. Wcześniej obowiązywały numery 10-cyfrowe. Wykrywanie i korygowanie błędów w numerach 10-cyfrowych opisano w [7]. W tej części rozdziału nie będzie opisu, jak stworzyć 13-cyfrowe numery ISBN, tylko jak sprawdzić, czy numer wyznaczono prawidłowo [17, 18]. Najważniejsza będzie ostatnia cyfra, tzw. cyfra kontrolna.

Dla identyfikatora ISBN-13 wagi $1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3$ mnoży się przez kolejne cyfry ciągu cyfr $x_1, x_2, \ldots, x_{12}$ numeru ISBN. Sumę iloczynów dzieli się przez 10 (modulo 10). Resztę odejmujemy od 10 i otrzymany wynik ponownie dzielimy przez 10. Uzyskana cyfra powinna być zgodna z ostatnią cyfrą kodu EAN-13.

Przykład 3.35

Czy numer ISBN $978\text{-}83\text{-}01\text{-}14380\text{-}0$ nadany książce K.A. Ross, Ch.R.B. Wright, *Matematyka dyskretna* jest prawidłowy?

Zaczyna się od obliczenia sumy

$$1 \cdot 9 + 3 \cdot 7 + 1 \cdot 8 + 3 \cdot 8 + 1 \cdot 3 + 3 \cdot 0 + 1 \cdot 1 + 3 \cdot 1 + 1 \cdot 4 + 3 \cdot 3 + 1 \cdot 8 + 3 \cdot 0 = 9 + 21 + 8 + 24 + 3 + 1 + 3 + 4 + 9 + 8 = 90$$

Wynik dzieli się przez 10

$$90 \bmod 10 \equiv 0$$

Otrzymany wynik odejmuje się od 10 i ponownie dzieli przez 10

$$10 - 0 = 10$$

$$10 \bmod 10 \equiv 0$$

Cyfra kontrolna to 0, zatem numer jest prawidłowy.

Przykład 3.36

Jaka powinna być cyfra kontrolna x, aby numer ISBN $978\text{-}83\text{-}01\text{-}14764\text{-}x$ był prawidłowy?

Zadanie zostanie rozwiązane w analogiczny sposób jak w *Przykładzie 3.32*.

$$1 \cdot 9 + 3 \cdot 7 + 1 \cdot 8 + 3 \cdot 8 + 1 \cdot 3 + 3 \cdot 0 + 1 \cdot 1 + 3 \cdot 1 + 1 \cdot 4 + 3 \cdot 7 + 1 \cdot 6 + 3 \cdot 4 = 9 + 21 + 8 + 24 + 3 + 1 + 3 + 4 + 21 + 6 + 12 = 112$$

$$112 \bmod 10 \equiv 2$$

$$10 - 2 = 8$$

$$8 \bmod 10 \equiv 8$$

Cyfra kontrolna wynosi 8.

3.7. Zadania do rozwiązania

1. Niech $x, y \in X = \{1, 2, 3, 4, 5, 6, 7\}$. Wyznaczyć pary należące do relacji w zbiorze X, narysować tablicę i graf relacji. Sprawdzić, które z poznanych własności relacja spełnia. Czy jest to relacja równoważności?
   a) $(x, y) \in R \Leftrightarrow \min(x, y) = 4 \ \vee \ \max(x, y) = 3$
   b) $(x, y) \in R \Leftrightarrow 4 | \ x \cdot y$
   c) $(x, y) \in R \Leftrightarrow 3xy + x$ jest liczbą nieparzystą
   d) $(x, y) \in R \Leftrightarrow \ (x - y)^2 + 1$ jest liczbą pierwszą
   e) $(x, y) \in R \Leftrightarrow \frac{|x^2 - y^2|}{x \cdot y} > 1$

2. Mając dane pary należące do relacji, narysować tablicę i graf oraz sprawdzić własności relacji. Podać dziedzinę, przeciwdziedzinę oraz dopełnienie relacji.

   a) $R = \{(1,1),(2,2),(2,3),(2,4),(2,6),(3,4),(4,4),(6,6),(7,1),(7,5),(7,6)\}$, gdzie $X = \{1,2,3,4,5,6,7\}$

   b) $R = \{(1,2),(1,3),(1,5),(1,6),(2,1),(2,4),(2,7),(3,1),(3,7),(4,1),(4,7),(5,2),(5,6),(6,3),(6,5),(7,4)\}$, gdzie $X = \{1,2,3,4,5,6,7\}$

   c) $R = \{(1,2),(1,4),(1,5),(2,5),(3,1),(4,1),(5,3),(5,4)\}$, gdzie $X = \{1,2,3,4,5\}$

   d) $R = \{(1,1),(2,2),(2,3),(3,3),(4,4),(5,4),(5,5)\}$, gdzie $X = \{1,2,3,4,5\}$

   e) $R = \{(1,1),(1,6),(3,1),(4,2),(5,1),(5,3),(6,2),(6,4),(6,6)\}$, gdzie $X = \{1,2,3,4,5,6\}$

3. Dane są tablice relacji. Zbadać, jakie własności spełniają te relacje. Czy są to relacje równoważności, porządku, liniowego porządku?

a)

	1	2	3	4	5
1		x			
2	x			x	x
3					x
4		x			
5		x	x		

b)

	A	B	C	D	E
A	x	x			x
B					
C	x		x		x
D	x				
E		x		x	

c)

	!	●	?	□	%
!	x	x			
●			x		
?			x	x	
□		x			x
%					x

d)

	1	2	3	4	5	6
1	x				x	
2		x				x
3			x			
4				x		
5	x				x	
6		x				x

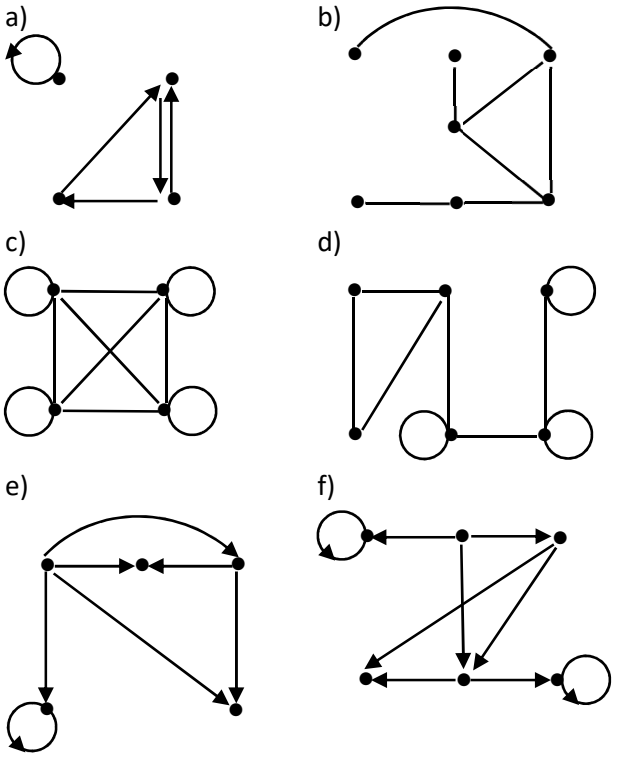
e)

	A	B	C	D	E	F
A		x	x	x	x	x
B			x	x	x	x
C				x	x	x
D					x	x
E						x
F						

f)

	1	2	3	4	5	6	7
1	x		x		x		x
2		x				x	
3	x						x
4				x			
5	x						x
6		x				x	
7	x		x		x		x

4. Na podstawie rysunków grafów przedstawić tablice relacji zobrazowanych tymi grafami oraz zbadać własności relacji.



5. Niech $X = \{1, 2, 3, \dots, 10\}$. Sprawdzić, czy relacja określona następująco:

   $(x, y) \in R \Leftrightarrow |x - y| \leq 1 \vee |x - y| \geq 8$ jest relacją równoważności.

6. Wyznaczyć cyfrę jedności zapisu dziesiętnego liczby $4^{444} + 7^{777}$.

7. Wyznaczyć dwie ostatnie cyfry zapisu dziesiętnego liczby $13^{256} - 23^{16}$.

8. Wyznaczyć resztę z dzielenia liczby $11^{301} + 31^{101}$ przez 7.

9. Czy liczba $5^{111} + 6^{234}$ jest podzielna przez 11? Odpowiedź uzasadnić.

10. Dane są liczby całkowite a, b, c, takie że $a + b + c = 0$. Udowodnić, że liczba $a^3 + b^3 + c^3$ jest podzielna przez 6 [6].

11. Jakie reszty z dzielenia przez 7 mogą dawać liczby postaci $2^{2^n} + 1$, gdzie n jest liczbą całkowitą nieujemną? [6].

12. Pewna liczba całkowita dodatnia zaczyna się cyfrą 1. Jeśli cyfrę tę przestawimy na koniec, to liczba zwiększy się trzykrotnie. Jaka jest najmniejsza liczba o tej własności? [19].

13. Wykazać, że liczba $n^n + (n+1)^{n+1}$ jest złożona dla nieskończenie wielu liczb naturalnych n [20, zadanie nr 19].

14. Wykazać, że jeśli n jest dodatnią liczbą całkowitą, to liczba $2(n^2+1)-n$ nie jest kwadratem liczby całkowitej [21].

15. Dana jest liczba całkowita dodatnia n oraz takie liczby całkowite a, b, c, d, e, f, że $a+b=c+d=e+f=n$. Wykazać, że liczba $ace+bdf$ jest podzielna przez n [6].

16. Udowodnić małe twierdzenie Fermata, że dla każdej liczby całkowitej n oraz każdej liczby pierwszej p liczba $n^p - n$ jest podzielna przez p.

17. Wykazać, że dla każdej liczby naturalnej n liczba $2^{5n+3} + 5^n \cdot 3^{n+2}$ jest podzielna przez 17 [8].

18. Czy istnieje liczba naturalna n, dla której liczba $9 \cdot 2^{2^n} + 1$ jest liczbą pierwszą? [8].

19. Wyznaczyć wszystkie takie liczby naturalne n, że liczba $1 + 2^n + 3^n + 4^n$ jest podzielna przez 5 [8].

20. Dany jest ciąg liczbowy (a_n) określony wzorem $a_n = 1^{4n} + 2^{4n} + 3^{4n}$, gdzie $n \in \boldsymbol{N}$. Wyznacz zbiór reszt z dzielenia wyrazów ciągu (a_n) przez 5 [22].

21. Znaleźć najmniejszą liczbę dodatnią, wielokrotność 7, która przy dzieleniu przez $2, 3, 4, 5, 6$ daje resztę 1 [12].

22. Rozstrzygnij, dla jakich nieujemnych liczb całkowitych n, liczba $A_n = 2021^n + 2022^n + 2023^n$ jest podzielna przez 3 [22].

23. Znaleźć:

    a) $13^{-1} (\mathrm{mod}\ 63)$

    b) $43^{-1} (\mathrm{mod}\ 111)$

    c) $89^{-1} (\mathrm{mod}\ 200)$

24. Znaleźć resztę z dzielenia:

    a) $78!$ przez 79

    b) $166!$ przez 167

25. Znaleźć resztę z dzielenia 2^{7000} przez 29, korzystając z małego twierdzenia Fermata.

26. Z małego twierdzenia Fermata wynika, że dla dowolnej liczby naturalnej a względnie pierwszej z 6601 zachodzą kongruencje:

    $a^6 \equiv 1 (\mathrm{mod}\ 7), \quad a^{22} \equiv 1 (\mathrm{mod}\ 23), \quad a^{40} \equiv 1 (\mathrm{mod}\ 41).$

Wywnioskować, że dla dowolnej liczby naturalnej a względnie pierwszej z 6601 zachodzi $a^{6600} \equiv 1 (\mathrm{mod}\ 6601)$.

27. Udowodnić, że:

    a) $\mathrm{ord}_7 2 = 3$

    b) $\mathrm{ord}_7 3 = 6$

    c) $\mathrm{ord}_7 4 = 3$

28. Dla liczby pierwszej p wyznaczyć pierwiastki pierwotne modulo p:

    a) $p = 7$

    b) $p = 11$

29. Rozwiązać układ kongruencji. Podać najmniejszą liczbę całkowitą dodatnią spełniającą układ.

    a) $\begin{cases} x \equiv 1 (\mathrm{mod}\ 5) \\ x \equiv 3 (\mathrm{mod}\ 12) \end{cases}$

    b) $\begin{cases} x \equiv 5 (\mathrm{mod}\ 7) \\ x \equiv 1 (\mathrm{mod}\ 15) \end{cases}$

    c) $\begin{cases} x \equiv 1 (\mathrm{mod}\ 9) \\ x \equiv 2 (\mathrm{mod}\ 11) \\ x \equiv 3 (\mathrm{mod}\ 13) \end{cases}$

    d) $\begin{cases} x \equiv 4 (\mathrm{mod}\ 14) \\ x \equiv 5 (\mathrm{mod}\ 19) \\ x \equiv 20 (\mathrm{mod}\ 23) \end{cases}$

30. Rozwiązać kongruencję z niewiadomą x. Podać najmniejszą liczbę całkowitą dodatnią spełniającą kongruencję.

    a) $3x \equiv 1 (\mathrm{mod}\ 19)$

    b) $3x \equiv 2 (\mathrm{mod}\ 17)$

    c) $5x \equiv 2 (\mathrm{mod}\ 13)$

    d) $8x \equiv 6 (\mathrm{mod}\ 83)$

31. Zbadać, czy liczba jest liczbą pierwszą?

    a) $2^5 - 1$

    b) $2^9 - 1$

    c) $2^{13} - 1$

32. Zastosować test Rabina–Millera do liczby:

    a) 137 b) 233 c) 149

33. Rozwiązać równania:

    a) $x^2 - x - 2 = 0 \pmod{11}$

    b) $x^2 + 3x = 0 \pmod{13}$

    c) $x^2 = 9 \pmod{19}$

34. Ile pierwiastków kwadratowych ma liczba x w $\mathbb{Z}_m$? Wyznaczyć je.

    a) $x = 1, m = 7$ b) $x = 5, m = 9$ c) $x = 7, m = 9$

35. Czy numer ISBN $978\text{-}83\text{-}7193\text{-}852\text{-}8$ nadany książce J. Pozorska, I. Zamorska, *Wybrane zagadnienia z matematyki dyskretnej. Część 1* jest prawidłowy?

36. Jaka jest cyfra kontrolna fikcyjnego numeru ISBN (ISBN-13), jeśli 12 pierwszych cyfr to $978\text{-}1\text{-}1380\text{-}6347\text{-}x$?

3.8. Wskazówki i odpowiedzi do zadań

1. a) Relacja jest symetryczna i spójna.

   d) Relacja jest przeciwzwrotna i symetryczna.

   e) Relacja jest przeciwzwrotna i symetryczna.

2. b) Relacja jest przeciwzwrotna. $D(R) = D^{-1}(R) = \{1, 2, 3, 4, 5, 6, 7\}$

   d) Relacja jest zwrotna, antysymetryczna i przechodnia, czyli jest relacją porządkującą. $D(R) = D^{-1}(R) = \{1, 2, 3, 4, 5\}$

   e) Relacja jest asymetryczna i antysymetryczna. $D(R) = \{1, 3, 4, 5, 6\}$, $D^{-1}(R) = \{1, 2, 3, 4, 6\}$

3. a) Nie jest to relacja równoważności ani porządku, więc również nie liniowego porządku.

   b) Relacja ma jedynie własność antysymetrii.

   e) Relacja jest przeciwzwrotna, asymetryczna, antysymetryczna, przechodnia, euklidesowa i spójna.

4. b) Relacja jest przeciwzwrotna i symetryczna.

   c) Relacja jest zwrotna, symetryczna, przechodnia, euklidesowa, spójna i liniowa. Jest relacją równoważności.

   f) Relacja ma jedynie własność antysymetrii.

6. 3

7. 80

8. 2

9. Nie

10. Udowodnić, że dla każdej liczby n $n^3 \equiv n(\mathrm{mod}\ 6)$, korzystając z faktu, że iloczyn $n^3 - n$ jest iloczynem trzech kolejnych liczb całkowitych.

11. Liczby postaci $2^{2^n} + 1$ to liczby Fermata. Możliwe są jedynie reszty 3 oraz 5. W pierwszej kolejności należy zbadać reszty z dzielenia przez 3 liczby 2^n.

12. 142857

14. Wykorzystać fakt, że jeżeli kwadrat liczby całkowitej jest podzielny przez pewną liczbę pierwszą p, to jest też podzielny przez liczbę p^2.

15. Jest podzielna, ponieważ $a \equiv -b(\mathrm{mod}\ n)$, $c \equiv -d(\mathrm{mod}\ n)$, $e \equiv -f(\mathrm{mod}\ n)$.

16. Każda liczba całkowita dodatnia (w tym przypadku pierwsza) daje z dzielenia przez p jedną z reszt: $0, 1, \dots, p-1$. Dla każdej liczby całkowitej n spełniona jest jedna z kongruencji $n \equiv 0(\mathrm{mod}\ p)$, $n \equiv 1(\mathrm{mod}\ p)$,..., $n \equiv p-1(\mathrm{mod}\ p)$.

18. Dla $n = 0$ liczba 19, a dla $n = 1$ liczba 37.

19. Dla wszystkich liczb naturalnych niepodzielnych przez 4.

22. Dla $n = 0$ lub n jest nieparzystą liczbą naturalną.

23. a) $13^{-1} \equiv 34(\mathrm{mod}\ 63)$

    b) $43^{-1} \equiv 31(\mathrm{mod}\ 111)$

    c) $89^{-1} \equiv 9(\mathrm{mod}\ 200)$

24. a) 78

    b) 166

25. 1

28. a) $a = 3$ i $a = 5$

29. a) 51, liczby postaci $51 + 60\ t$, gdzie t jest dowolną liczbą całkowitą.

    b) 61, liczby postaci $61 + 105\ t$, gdzie t jest dowolną liczbą całkowitą.

    c) 640, liczby postaci $640 + 1287\ t$, gdzie t jest dowolną liczbą całkowitą.

    d) 480, liczby postaci $480 + 6118\ t$, gdzie t jest dowolną liczbą całkowitą.

30. a) Rozwiązaniem kongruencji jest $x \equiv 13(\mathrm{mod}\ 19)$. Najmniejszą liczbą całkowitą spełniającą kongruencję jest 13.

b) Rozwiązaniem kongruencji jest $x \equiv 12(\mathrm{mod}\ 17)$. Najmniejszą liczbą całkowitą spełniającą kongruencję jest 12.

c) Rozwiązaniem kongruencji jest $x \equiv 3(\mathrm{mod}\ 13)$. Najmniejszą liczbą całkowitą spełniającą kongruencję jest 3.

d) Rozwiązaniem kongruencji jest $x \equiv 63(\mathrm{mod}\ 83)$. Najmniejszą liczbą całkowitą spełniającą kongruencję jest 63.

31. a) Tak b) Nie c) Tak

33. a) $x = 10(\mathrm{mod}\ 11)$ oraz $x = 2(\mathrm{mod}\ 11)$

b) $x = 0(\mathrm{mod}\ 13)$ oraz $x = 10(\mathrm{mod}\ 13)$

c) $x = 3(\mathrm{mod}\ 19)$ oraz $x = 16(\mathrm{mod}\ 19)$

34. a) 1 oraz 6 b) Brak c) 4 oraz 5

35. Tak

36. 1

3.9. Literatura

[1] J. Pozorska, I. Zamorska, *Wybrane zagadnienia z matematyki dyskretnej. Część 1*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2021.

[2] K.A. Ross, Ch.R.B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[3] S. Przybyło, A. Szlachtowski, *Algebra i wielowymiarowa geometria analityczna w zadaniach*, Wydawnictwa Naukowo-Techniczne, Warszawa 1994.

[4] https://pl.wikipedia.org

[5] https://pl.wikipedia.org/wiki/Arytmetyka_modularna

[6] J. Dymel, M. Niedźwiedź, *Kongruencje*, [w:] W. Pompe (red. wydania), *I Olimpiada Matematyczna Gimnazjalistów 2005/2006*, Stowarzyszenie na rzecz Edukacji Matematycznej, Wydawnictwo Szkolne OMEGA, Kraków 2009.

[7] S.Y. Yan, *Teoria liczb w informatyce*, Wydawnictwo Naukowe PWN, Warszawa 2006.

[8] P. Cholewik, *Kongruencje*, [w:] P. Cholewik i in., *Przed konkursem matematycznym*, Wydawnictwo Szkolne Omega, Kraków 2011.

[9] A. Męcel, *Więcej o cechach*, zdalne seminarium OMJ dla nauczycieli matematyki, 15-16.05.2020.

[10] W. Pompe (red. wydania), *IV Olimpiada Matematyczna Gimnazjalistów 2008/2009, Stowarzyszenie na rzecz Edukacji Matematycznej*, Wydawnictwo Szkolne OMEGA, Kraków 2012.

[11] Ł. Bożyk, *Kwadraty, liczby pierwsze i reszta*, „Kwadrat. Gazetka Olimpiady Matematycznej Juniorów”, nr 7, grudzień 2012.

[12] J. Kowolik, T. Szwed, *Matematyka dla odważnych*, Wydawnictwo Nowik, Opole 2010.

[13] M. Zakrzewski, *Markowe wykłady z matematyki*, Oficyna Wydawnicza GiS, Wrocław 2014.

[14] J. Chernick, *On Fermat's Simple Theorem*, „Bulletin of the American Mathematical Society", 1939, Vol. 45, s. 269-274.

[15] W. Mizerski (praca zbiorowa pod redakcją), *Tablice matematyczne*, Wydawnictwo Adamantan, Warszawa 2001.

[16] H. Furmańczyk, K. Horodecki, P. Żyliński, *Matematyka dyskretna dla studentów Informatyki*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2010.

[17] algorytm.org/numery-identyfikacyjne

[18] bn.org.pl

[19] B. Zawalski, *Teoria liczb*, „Kwadrat. Gazetka Olimpiady Matematycznej Juniorów", nr 23, wrzesień 2019.

[20] Baltic Way Mathematical Contests – Estonian Math Competitions 2012, https://www.math.olympiaadid.ut.ee/

[21] Czesko-Polsko-Słowackie Zawody Matematyczne Juniorów 2012, https://omj.edu.pl/cpsj

[22] skm.katowice.pl

Rozdział 4

Wybrane zagadnienia teorii grafów

4.1. Grafy rządzą światem?

Niniejszy rozdział został opracowany na podstawie [1-13], a także niepublikowanych wykładów prof. Zbigniewa Domańskiego.

Pojęcie **grafu** jest jednym z kluczowych pojęć matematyki dyskretnej. **Teoria grafów** łączy pojęcia matematyczne i rozwiązania informatyczne. Graf pozwala w prosty, schematyczny sposób opisać połączenia lub powiązania relacji z pewnymi jej własnościami, przedstawić graficznie pewną sytuację.

Grafy są ważnymi narzędziami matematycznymi nie tylko w informatyce (gdzie spotkać je można np. przy analizie relacji na portalach internetowych, ale także w zagadnieniach dotyczących przechowywania informacji, kodowania i wielu, wielu innych). Jako graf przedstawia się drzewa genealogiczne, struktury organizacyjne w firmach, sieci połączeń drogowych (mapa drogowa to nic innego jak graf), plany ewakuacji z budynków, rysunki obwodów elektrycznych. W biologii i neurobiologii grafy mogą zobrazować sieci połączeń neuronów. Dzięki zastosowaniu grafów oraz algorytmów informatycznych (m.in. dzięki polskim naukowcom) wykazano, że współczesna chemia to w głównej mierze ok. 340 związków i ok. 500 reakcji chemicznych pozwalających na odtworzenie ok. 80% związków chemicznych wykorzystywanych w przemyśle. Daje to możliwość obniżenia cen i kosztów produkcji owych związków. Teoria grafów ma również zastosowanie na rynkach finansowych, w bezpieczeństwie publicznym, a nawet wywiadzie wojskowym [1, 2].

A zaczęło się tak niewinnie…
Z XVIII-wiecznym problemem mostów w Królewcu spotkał się już chyba każdy z Czytelników. Krótko przypominając: mieszkańcy Królewca lubili spacerować po mostach znajdujących się na rzece Pregoła, która rozwidla się i w centrum miasta tworzy dwie wyspy. W owym czasie znajdowało się tam siedem mostów: jedną z wysp łączyły z każdym z brzegów po dwa mosty, drugą wyspę po jednym moście, był także most pomiędzy wyspami. Padło pytanie: czy możliwa jest taka trasa spacerowa która przechodzi przez każdy most dokładnie jeden raz, żadnego z nich nie omija i pozwala wrócić do punktu wyjścia? Problem wyjaśnił w 1735 r. wielki szwajcarski matematyk Leonhard Euler, mówiąc, że nie istnieje rozwiązanie tego problemu. W opublikowanej w 1736 r. pracy Euler sformował pierwsze twierdzenie dotyczące grafów.

Publikacja Eulera stała się zalążkiem nowego, ważnego i wciąż rozwijającego się działu matematyki: teorii grafów. Samo wprowadzenie terminu „graf" przypisuje się XIX-wiecznemu angielskiemu matematykowi Jamesowi Josephowi Sylvesterowi.

No więc czy grafy rządzą światem? Tak. Mamy z nimi do czynienia na co dzień, nawet nieświadomie. Porządkują relacje, pozwalają monitorować zdarzenia, zachowania.

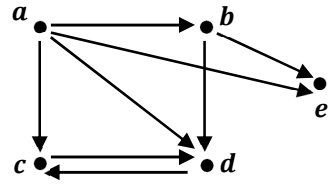
4.2. Podstawowe definicje. Niezmienniki izomorfizmu

Graf jest to niepusty zbiór wierzchołków oraz krawędzi łączących te wierzchołki. Dopuszcza się **krawędzie wielokrotne** i **pętle** (czyli krawędzie o początku i końcu w tym samym wierzchołku).

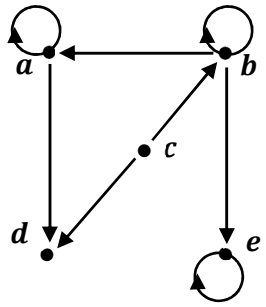
Rozważać można **grafy nieskierowane** (o krawędziach niekierowanych) i **skierowane** (o krawędziach skierowanych) oraz **grafy ważone** (każdej krawędzi przyporządkowana jest liczba, tak zwana waga).
W niektórych grafach wierzchołek może mieć swoją nazwę, mówi się wówczas o **grafach etykietowanych.**
Rysunek grafu to tylko jedna z wielu jego reprezentacji graficznych, można go narysować na kilka sposobów.
Przykładem grafu nieskierowanego może być graf ilustrujący mapę dróg umożliwiających ruch dwukierunkowy.

Przykład 4.1

Przykład grafu skierowanego (krawędzie są skierowane) – z wierzchołka a można przejść do wierzchołków $b,\ c,\ e,\ d,$ z wierzchołka b do wierzchołka e i d itd.:



Graf skierowany, w którym występują pętle $(a,a),(b,b),(e,e)$:



Graf prosty to graf nieskierowany bez wielokrotnych krawędzi, pętli, wag, etykiet.

Bardziej formalna definicja grafu nieskierowanego jest następująca:

Graf nieskierowany (niezorientowany) $G = (V, E)$ składa się ze skończonego zbioru wierzchołków $V(G)$ oraz ze skończonego zbioru krawędzi $E(G)$, z których każda jest utożsamiana z podzbiorem $(u, v) \subset V$.

Graf skierowany (zorientowany) $G = (V, E)$ składa się z dwóch zbiorów: niepustego zbioru $V(G)$ wierzchołków grafu i zbioru $E(G)$ krawędzi grafu oraz funkcji γ odwzorowującej zbiór $E(G)$ w zbiór $V(G) \times V(G)$.

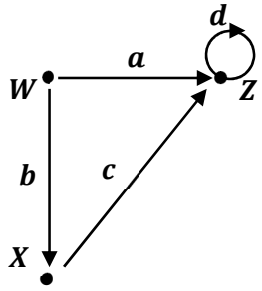
Jeżeli *e* jest krawędzią grafu G i $\gamma(e) = (p, q)$, to p nazywamy początkiem krawędzi e, a q końcem krawędzi e (e biegnie od p do q).

Rysunkiem grafu skierowanego jest wykres składający się z punktów odpowiadających elementom zbioru $V(G)$ oraz strzałek odpowiadających elementom zbioru $E(G)$, takich że jeśli $\gamma(e) = (p, q)$, to strzałka odpowiadająca e biegnie od punktu oznaczonego przez p do punktu oznaczonego przez q.

Przykład 4.2

Narysować graf skierowany, w oparciu o tabelkę funkcji γ.

E	$\gamma(E)$
a	(W, Z)
b	(W, X)
c	(X, Z)
d	(Z, Z)



Graf ma trzy wierzchołki $V(G) = \{W, X, Z\}$ oraz cztery krawędzie $E(G) = \{a, b, c, d\}$, przy czym krawędź d jest pętlą.

Drogą w grafie skierowanym G nazywa się ciąg krawędzi takich, że koniec jednej krawędzi jest początkiem następnej. Jeżeli $e_1, e_2, e_3, \ldots, e_n$ należą do zbioru $E(G)$, to $e_1 e_2 e_3 \ldots e_n$ jest drogą, o ile istnieją wierzchołki $v_1, v_2, v_3, \ldots, v_n, v_{n+1}$ takie, że $\gamma(e_i) = (v_i, v_{i+1})$ dla $i = 1, 2, 3 \ldots, n$.

$e_1 e_2 e_3 \ldots e_n$ jest **drogą (ścieżką) długości n** od wierzchołka v_1 do wierzchołka v_{n+1}.

Drogą zamkniętą nazywa się drogę, w której $v_1 = v_{n+1}$.

Jeżeli każda krawędź e_i jest jedyną krawędzią od v_i do v_{i+1}, to ten ciąg wierzchołków jednoznacznie określa drogę i można opisać tę drogę, wpisując po prostu

po kolei te wierzchołki. Jeśli graf nie ma krawędzi wielokrotnych, wszystkie jego drogi są określone przez ciągi ich wierzchołków.

Długością drogi jest liczba krawędzi w tej drodze.

Przykład 4.3

W *Przykładzie 4.2* drogą długości 2 z wierzchołka W do wierzchołka Z będzie ciąg krawędzi bc.Tę samą drogę wyznacza ciąg wierzchołków WXZ.
Drogą z wierzchołka W do wierzchołka Z będzie również ciąg bcd, jest to droga długości 3 (ciąg wierzchołków $WXZZ$).

W badaniu relacji skończonych grafów skierowanych i nieskierowanych użyteczne jest pojęcie **sąsiedztwa**.

Dla dowolnego grafu G i wierzchołków u, v w zbiorze $V(G)$ mówi się, że wierzchołek u jest sąsiedni do wierzchołka v, jeśli istnieje krawędź w $E(G)$ od u do v. Mówi się wtedy, że **wierzchołki u i v są ze sobą w relacji sąsiedztwa**. Macierz opisująca tę relację nazywa się **macierzą sąsiedztwa**.

Niech G będzie grafem skończonym, a $V(G) = \{v_1, v_2 \dots v_n\}$ zbiorem wierzchołków tego grafu.

Macierzą sąsiedztwa nazywa się macierz M wymiaru $n \times n$, której każdy element m_{ij} jest liczbą krawędzi od wierzchołka v_i do wierzchołka v_j.

Jeśli nie istnieje krawędź od wierzchołka v_i do wierzchołka v_j, to $m_{ij} = 0$; w innym przypadku m_{ij} jest liczbą całkowitą dodatnią.

Macierz sąsiedztwa grafu nieskierowanego jest macierzą symetryczną.

Liczba dróg długości 1 to suma wszystkich elementów macierzy M.
Liczba dróg długości 2 to suma wszystkich elementów macierzy M^2.
Liczba dróg długości 3 to suma wszystkich elementów macierzy M^3 i tak dalej.

Przykład 4.4

Macierz sąsiedztwa grafu z *Przykładu 4.2* jest następująca:

$$M = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Mając daną macierz sąsiedztwa, bardzo wiele można dowiedzieć się o grafie: graf ma trzy wierzchołki (macierz jest wymiaru 3×3); krawędzi ma tyle, ile wynosi suma wszystkich elementów macierzy M, czyli cztery krawędzie w tym jedną pętlę, gdyż na głównej przekątnej macierzy jest tylko jeden element 1.

Przykład 4.5

Co można odczytać dla grafu G, jeśli macierz sąsiedztwa tego grafu jest następująca:

$$M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

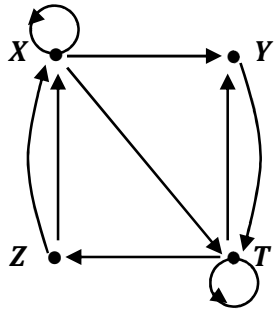
Narysować ten graf.

- Jest to graf skierowany

ponadto ma:

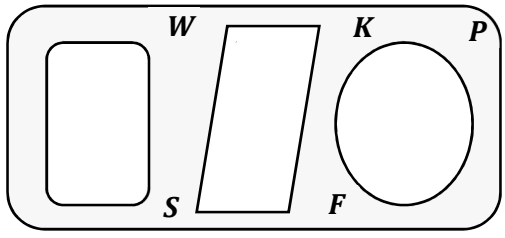
- cztery wierzchołki $V(G) = \{X, Y, Z, T\}$ (macierz M jest macierzą wymiaru 4×4)
- siedem krawędzi (liczonych bez pętli; suma wyrazów macierzy M – bez elementów na głównej przekątnej – wynosi 7)
- dwie pętle (na głównej przekątnej dwie jedynki)
- dwa wierzchołki łączą dwie krawędzie

Graf ten może wyglądać następująco:

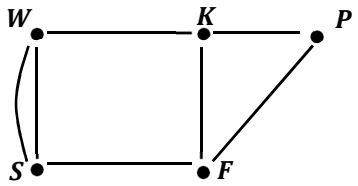


Przykład 4.6

Narysować graf odpowiadający sieci ścieżek spacerowych w parku, gdzie W jest wejściem do parku, K to kawiarnia, P – plac zabaw dla dzieci, F – fontanna a S – stoisko z watą cukrową. Podać macierz sąsiedztwa dla grafu oraz liczbę dróg długości 2.



Graf, który będzie oczywiście grafem nieskierowanym (po ścieżkach można poruszać się w obu kierunkach), może wyglądać tak:



Macierz sąsiedztwa tego grafu będzie macierzą symetryczną (graf nieskierowany), na głównej przekątnej są zera (nie ma pętli), wymiar macierzy M 5×5

$$M = \begin{bmatrix} 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Aby obliczyć liczbę dróg długości 2, należy podnieść macierz M do kwadratu

$$M^2 = \begin{bmatrix} 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 1 & 0 & 3 \\ 0 & 3 & 1 & 3 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 0 & 3 & 1 & 5 & 0 \\ 3 & 1 & 1 & 0 & 3 \end{bmatrix}$$

Dróg o długości 2 jest zatem $9 + 8 + 6 + 9 + 8 = 40$.

Stopniem wierzchołka v nazywamy liczbę dwuwierzchołkowych krawędzi z v jako jednym z wierzchołków plus podwojona liczba pętli o wierzchołku v. Stopnień wierzchołka v oznaczamy $deg(v)$.

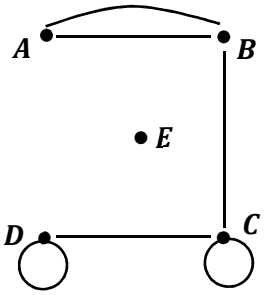
Niech $D_k(G)$ oznacza liczbę wierzchołków stopnia k w grafie G, wówczas ciąg: $(D_0(G), D_1(G), D_2(G), D_3(G), \dots)$ jest **ciągiem liczb wierzchołków kolejnych stopni** grafu G.

Suma stopni wierzchołków grafu jest dwa razy większa od liczby krawędzi:

$$\sum_{v \in V(G)} deg(v) = 2 \cdot |E(G)| \tag{4.1}$$

Przykład 4.7

Na rysunku przedstawiony jest graf:



w którym:

$deg(A) = 2$ (dwie krawędzie mają swoje końce w A)

$deg(B) = 3$

$deg(C) = 4$ (dwie krawędzie: CB i CD oraz jedna pętla CC)

$deg(D) = 3$

$deg(E) = 0$ (wierzchołek izolowany)

W rozpatrywanym przykładzie ciąg liczby wierzchołków kolejnych stopni jest następujący: $(1, 0, 1, 2, 1, 0, \dots)$.

Przykład 4.8

Czy następujące ciągi są ciągami liczb wierzchołków kolejnych stopni grafów?

a) (0, 1, 0, 2, 1, 0, 0, …)

$$\left(\underbrace{0}_{D_0(G)}, \underbrace{1}_{D_1(G)}, \underbrace{0}_{D_2(G)}, \underbrace{2}_{D_3(G)}, \underbrace{1}_{D_4(G)}, \underbrace{0}_{D_5(G)}, \underbrace{0}_{D_6(G)}, \dots \right)$$

Jest: zero wierzchołków zerowego stopnia, jeden wierzchołek pierwszego stopnia, zero wierzchołków drugiego stopnia, dwa wierzchołki trzeciego stopnia, jeden wierzchołek czwartego stopnia i żadnych innych wierzchołków.

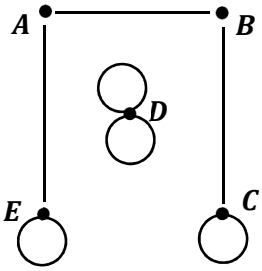
$0 \cdot 0 + 1 \cdot 1 + 0 \cdot 2 + 2 \cdot 3 + 1 \cdot 4 + 0 \cdot 0 = 11$ – nie jest to liczba parzysta, więc nie ma takiego grafu.

b) (0, 0, 2, 2, 1, 0, 0, …)

$$\left(\underbrace{0}_{D_0(G)}, \underbrace{0}_{D_1(G)}, \underbrace{2}_{D_2(G)}, \underbrace{2}_{D_3(G)}, \underbrace{1}_{D_4(G)}, \underbrace{0}_{D_5(G)}, \underbrace{0}_{D_6(G)}, \dots \right)$$

$0 \cdot 0 + 0 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + 1 \cdot 4 + 0 \cdot 0 = 14 = 2 \cdot 7$, więc istnieje taki graf.

Ma on $2 + 2 + 1 = 5$ wierzchołków i 7 krawędzi. Może wyglądać następująco:

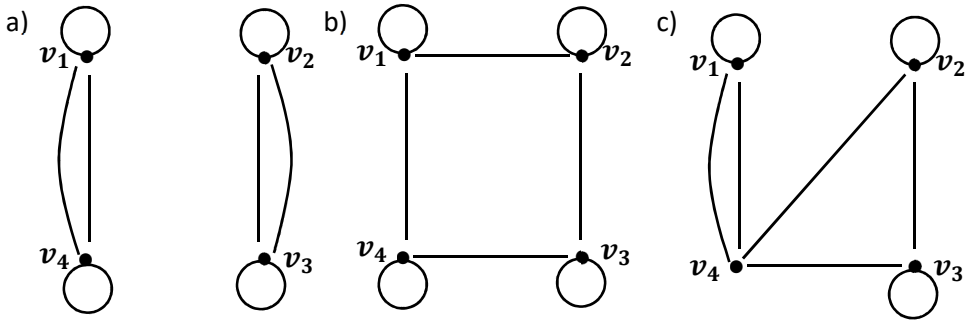


$deg(A) = deg(B) = 2\,, deg(C) = deg\,(E) = 3, deg(D) = 4$

Grafy, w których wszystkie wierzchołki są tego samego stopnia, nazywa się **grafami regularnymi**.

Przykład 4.9

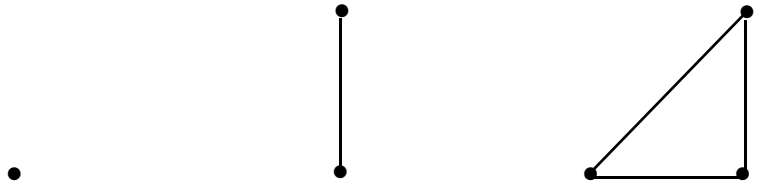
Grafy na rysunkach a), b) i c) są regularne (wszystkie wierzchołki mają stopień 4).



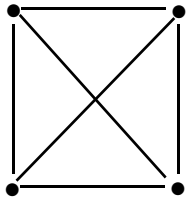
Grafy niemające pętli ani krawędzi wielokrotnych i takie, w których każdy wierzchołek połączony jest krawędziami ze wszystkimi pozostałymi wierzchołkami, nazywamy **grafami pełnymi**.

Przykład 4.10

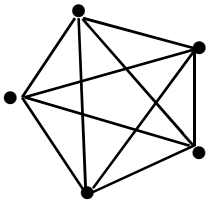
Na rysunku poniżej przedstawione jest pierwsze sześć grafów pełnych. Grafy pełne są oczywiście grafami regularnymi, każdy wierzchołek grafu K_n ma stopień $n - 1$.



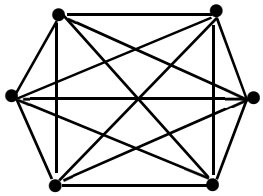
K_1 K_2 K_3



K_4



K_5



K_6

Często zdarza się, że grafy są „właściwie takie same", pomimo że różnią się nazwami wierzchołków i krawędzi.
Ważne, czy podobieństwo jest tylko wizualne, czy też strukturalnie dwa grafy są identyczne.

Dwa zbiory wyposażone w pewne struktury matematyczne nazywamy izomorficznymi, jeśli istnieje przekształcenie wzajemnie jednoznaczne pomiędzy tymi zbiorami zachowujące struktury.

Izomorfizmem grafu G na graf H nazywa się przekształcenie wzajemnie jednoznaczne α: $V(G) \to V(H)$ takie, że $\{u, v\}$ jest krawędzią grafu G wtedy i tylko wtedy, gdy $\{\alpha(u), \alpha(v)\}$ jest krawędzią w grafie H.

Zapisuje się to jako: $G \cong H$.

Stwierdzenie to jest poprawne dla grafów bez krawędzi wielokrotnych. Jeśli graf ma krawędzie wielokrotne, wymaga się jeszcze wzajemnej jednoznaczności dodatkowego przekształcenia β: $E(G) \to E(H)$ pomiędzy zbiorami krawędzi grafów.

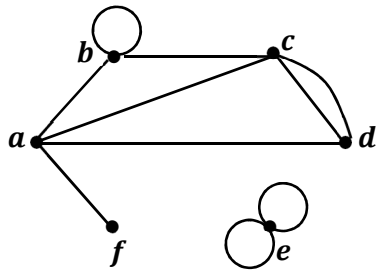
Istnieją pewne cechy grafów, zwane **niezmiennikami izomorfizmu**, które pozwalają ocenić, czy dwa grafy są tożsame w sensie strukturalnym.

Przykładami niezmienników izomorfizmu grafów są:

- liczba wierzchołków (LW);
- liczba krawędzi (LK) (bez pętli);
- liczba pętli (LP);
- liczba dróg prostych określonej długości (np. liczba dróg prostych długości 1, długości 2 itd.) (LDD_1, LDD_2, …);
- stopnie wierzchołków;
- ciąg liczby wierzchołków kolejnych stopni.

Przykład 4.11

Niech dany będzie graf jak na poniższym rysunku. Wyznaczyć niezmienniki izomorfizmu tego grafu.



Liczba wierzchołków: LW = 6

Liczba krawędzi (bez pętli) : LK = 7

Liczba pętli: LP = 3

Stopnie wierzchołków:

$deg(a) = deg(b) = deg(c) = deg(e) = 4$

$deg\ (d) = 3$

$deg(f) = 1$

Ciąg liczby wierzchołków kolejnych stopni: $(0, 1, 0, 1, 4, 0, \dots)$

Macierz sąsiedztwa tego grafu (i jej kwadrat):

$$M = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 2 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \qquad M^2 = \begin{bmatrix} 4 & 2 & 3 & 2 & 0 & 0 \\ 2 & 3 & 2 & 3 & 0 & 1 \\ 3 & 2 & 6 & 1 & 0 & 1 \\ 2 & 3 & 1 & 5 & 0 & 1 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Liczba dróg długości 1, to suma elementów macierzy: 17

Liczba dróg długości 2, to suma elementów macierzy M^2: 55

4.3. Grafy eulerowskie i hamiltonowskie

Grafem spójnym nazywamy graf, w którym każda para wierzchołków jest połączona drogą.

Liczba krawędzi k w grafie spójnym prostym o n wierzchołkach spełnia warunki:

$$n - 1 \leq k \leq \frac{n(n-1)}{2} \tag{4.2}$$

Zagadnienia związane z poruszaniem się po krawędziach grafu

Czy w grafie spójnym istnieje możliwość wyznaczenia drogi zawierającej wszystkie krawędzie tego grafu?

Drogę prostą zawierającą wszystkie krawędzie grafu G nazywa się **drogą Eulera**. Jeśli ta droga jest zamknięta (czyli tworzy cykl), to mówi się o **cyklu Eulera**.

Twierdzenie 4.1 (L. Euler)

Skończony graf spójny, w którym każdy wierzchołek jest parzystego stopnia, ma cykl Eulera.

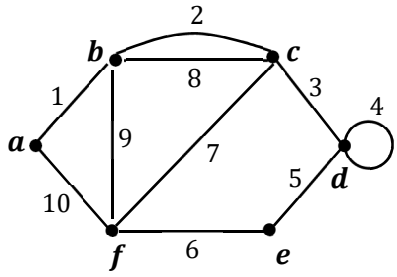
Wniosek wypływający z tego twierdzenia jest następujący:

Skończony graf spójny, w którym dokładnie dwa wierzchołki mają stopień nieparzysty, ma drogę Eulera.

Grafy, w których jest cykl Eulera, nazywamy **grafami eulerowskimi**, a grafy, w których nie ma cyklu, ale jest droga Eulera – **grafami półeulerowskimi**.

Przykład 4.12

Niech dany będzie graf:



Jest więc:

$deg(a) = deg(e) = 2,\ \ deg(b) = deg(c) = deg(d) = deg(f) = 4$

Jak widać, wszystkie wierzchołki są stopnia parzystego (2 lub 4), więc zgodnie z twierdzeniem Eulera w tym grafie jest cykl przebiegający wszystkie krawędzie (każdą dokładnie raz).

Jak znaleźć taki cykl?

Wybierając dowolny wierzchołek – w tym przykładzie wybrano a – i usuwając kolejno krawędzie, ale tak, aby po każdym usunięciu graf nadal był spójny. Kolejność usuwanych krawędzi zaznaczona jest kolejnymi liczbami przy krawędziach.

Wybiera się dowolne krawędzie, które są styczne z obecnie rozważanym wierzchołkiem, i zapamiętuje się ich kolejność. W każdym kroku należy unikać **mostów** (krawędzi, których usunięcie sprawi, że graf przestanie być spójny).

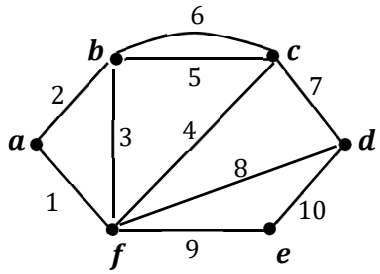
Działania te powtarza się aż do wyczerpania wszystkich krawędzi, a zaznaczone krawędzie tworzą kolejno cykl Eulera.

Opisany algorytm wyznaczania cyklu Eulera nosi nazwę **algorytmu Fleury'ego.**

Podając cykl Eulera, można podać kolejne usuwane krawędzie: $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ lub kolejne wierzchołki: $a, b, c, d, d, e, f, c, b, f, a$.

Przykład 4.13

Czy w grafie istnieje cykl lub droga Eulera?



$deg(a) = deg(e) = 2,\ \ deg(b) = deg(c) = 4,\ \ \ deg(d) = 3,\ \ \ deg(f) = 5$

Dwa wierzchołki (e i f) są nieparzystego stopnia, więc zgodnie z wnioskiem, w grafie tym nie będzie cyklu Eulera, ale będzie droga Eulera.
Drogę konstruuje się analogicznie jak cykl, z tą różnicą, że zaczyna się od jednego z wierzchołków nieparzystego stopnia i kończy w drugim z tych wierzchołków.

Droga Eulera: $f, a, b, f, c, b, c, d, f, e, d$.

Zagadnienia związane z poruszaniem się po wierzchołkach grafu

Można zadać tu trochę podobne pytanie jak w poprzednim zagadnieniu:

Czy w grafie spójnym istnieje możliwość wyznaczenia drogi zawierającej wszystkie wierzchołki tego grafu?

Drogę prostą nazywa się **drogą Hamiltona**, jeśli przechodzi ona przez każdy wierzchołek grafu dokładnie jeden raz.
Drogę zamkniętą, która przechodzi przez każdy wierzchołek grafu dokładnie jeden raz, z wyjątkiem wierzchołka, będącego początkiem i końcem drogi, nazywa się **cyklem Hamiltona**.

Grafy, w których jest cykl Hamiltona, to **grafy hamiltonowskie**, a grafy, w których nie ma cyklu, ale jest droga Hamiltona, to **grafy półhamiltonowskie**.

Pojęcie cyklu Hamiltona wydaje się być bliskie pojęciu cyklu Eulera, jednak teoria cykli Hamiltona jest znacznie bardziej złożona. Nie jest znany żaden efektywny algorytm znajdowania cykli Hamiltona.
Jest jednak kilka twierdzeń, wystarczających do tego, aby graf był hamiltonowski (niespełnienie jednak założeń tych twierdzeń nie powoduje, że graf nie będzie hamiltonowski).

Uwaga:
Graf hamiltonowski o n wierzchołkach musi mieć co najmniej n krawędzi.
Pętle i krawędzie wielokrotne, przy wyznaczaniu drogi/cyklu Hamiltona, są bezużyteczne.

Twierdzenie 4.2 (G.A. Dirac) [1, 3]

Jeżeli graf G nie ma pętli ani krawędzi wielokrotnych, jeśli $|V(G)| = n \geq 3$ oraz jeśli $deg(v) \geq \frac{n}{2}$ dla każdego wierzchołka v w grafie G, to graf G jest grafem hamiltonowskim.

Twierdzenie 4.3 [1, 3]

Jeżeli graf mający n wierzchołków i niemający pętli ani krawędzi wielokrotnych ma co najmniej $\frac{(n-1)(n-2)}{2} + 2$ krawędzi, to jest hamiltonowski.

Twierdzenie 4.4 (O. Ore) [1, 3]

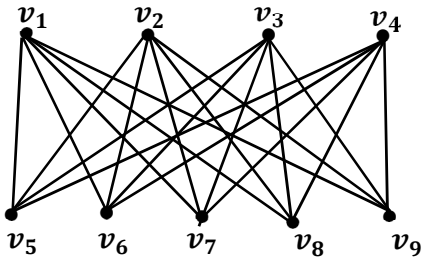
Załóżmy, że graf G nie ma pętli ani krawędzi wielokrotnych i $|V(G)| = n \geq 3$.
Jeśli $deg(v) + deg(w) \geq n$ dla każdej pary wierzchołków v i w niepołączonych krawędzią, to graf jest hamiltonowski.

Twierdzenie 4.5 (J.A. Bondy, V. Chvátal) [1]

Załóżmy, że graf G nie ma pętli ani krawędzi wielokrotnych i $|V(G)| = n \geq 3$
oraz $deg(v) + deg(w) \geq n$ dla pewnej pary wierzchołków v i w niepołączonych krawędzią. Załóżmy ponadto, że graf G' jest grafem skonstruowanym z grafu G poprzez dodanie krawędzi vw. Wówczas G jest hamiltonowski wtedy i tylko wtedy, gdy G' jest hamiltonowski.

Przykład 4.14

Czy jest to graf hamiltonowski?



Graf ma $n = 9$ wierzchołków:

$deg(v_1) = deg(v_2) = deg(v_3) = deg(v_4) = 5 > \frac{9}{2}$

$deg(v_5) = deg(v_6) = deg(v_7) = deg(v_8) = deg(v_9) = 4 < \frac{9}{2}$

Więc już nie działają założenia *Twierdzenia 4.2*.

Graf ma 20 krawędzi, więc mniej niż wymaga *Twierdzenie 4.3*:

$\frac{(9-1)(9-2)}{2} + 2 = 30$

Jedyne wierzchołki, które nie są połączone krawędzią, to $\{v_1, v_2, v_3, v_4\}$ (między sobą) i $\{v_5, v_6, v_7, v_8, v_9\}$ (między sobą), wówczas suma stopni wynosi odpowiednio 10 lub 8, więc znów nie są spełnione założenia *Twierdzenia 4.4* (ze względu na sformułowanie „*dla każdej pary wierzchołków v i w niepołączonych krawędzią*").

Dodając dowolną krawędź między niepołączonymi wierzchołkami, np. v_1v_2, nadal nie otrzymuje się grafu hamiltonowskiego.

W grafie tym nie można wyznaczyć cyklu Hamiltona.

4.4. Grafy dwudzielne

Przedstawiony na rysunku w *Przykładzie 4.14* graf jest **grafem dwudzielnym**, tzn. zbiór wierzchołków grafu $V(G)$ jest sumą dwóch niepustych, rozłącznych podzbiorów V_1, V_2, takich, że każda krawędź w grafie G łączy wierzchołek ze zbioru V_1 z wierzchołkiem ze zbioru V_2. Można powiedzieć więcej: jest to **graf pełny dwudzielny**, tzn. każdy wierzchołek zbioru V_1 jest połączony z każdym wierzchołkiem zbioru V_2 dokładnie jedną krawędzią.

Twierdzenie 4.6 [3]

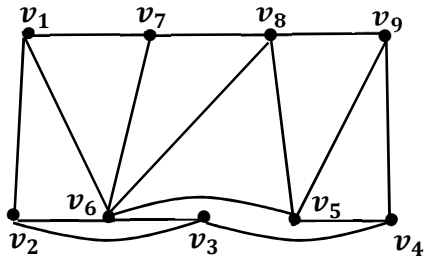
Niech G będzie grafem dwudzielnym i niech $V(G) = V_1 \cup V_2$ będzie podziałem jego wierzchołków. Jeśli graf G ma cykl Hamiltona, to $|V_1| = |V_2|$. Jeśli graf G ma drogę Hamiltona, to liczby $|V_1|, |V_2|$ różnią się co najwyżej o 1.

Dla pełnych grafów dwudzielnych o co najmniej trzech wierzchołkach prawdziwe są również stwierdzenia odwrotne.

W *Przykładzie 4.14* można przyjąć: $V_1 = \{v_1, v_2, v_3, v_4\}$, $V_2 = \{v_5, v_6, v_7, v_8, v_9\}$. Jest więc: $|V_2| = |V_1| + 1$, zatem zgodnie z powyższym twierdzeniem w grafie tym nie ma cyklu Hamiltona, ale jest droga Hamiltona, np.: $v_5v_1v_6v_2v_7v_3v_8v_4v_9$.

Przykład 4.15

Czy jest to graf hamiltonowski?



W przypadku tego grafu nie trzeba sprawdzać twierdzeń, gdyż widać, że łatwo można stworzyć cykl Hamiltona, np. taki:

$v_1v_2v_6v_3v_4v_9v_5v_8v_7v_1$, czyli jest to graf hamiltonowski.

4.5. Drzewa

Graf nieposiadający cykli nazywamy **grafem acyklicznym**.

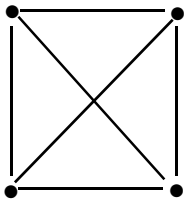
Grafy, które są acykliczne i spójne, nazywamy **drzewami**.

Drzewem spinającym nazywamy minimalny podgraf T grafu spójnego G, podgraf ten musi być acykliczny, gdyż można usunąć jedną krawędź dowolnego cyklu, nie tracąc przy tym własności spójności.

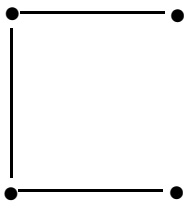
Drzewo spinające zawiera każdy wierzchołek grafu ($V(T)$ = $V(G)$) i niekoniecznie wszystkie krawędzie grafu G.

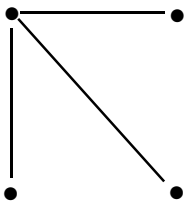
Przykład 4.16

Drzewami spinającymi dla grafu:



są:





Twierdzenie 4.7

Każdy skończony graf spójny ma drzewo spinające.

Twierdzenie 4.8 [3]

Niech e będzie krawędzią grafu spójnego G. Następujące warunki są równoważne:

a) graf $G\backslash\{e\}$ jest spójny;

b) e jest krawędzią w pewnym cyklu w grafie G;

c) e jest krawędzią w pewnej zamkniętej drodze prostej w grafie G.

Uwaga:
Charakteryzacja drzew nie traci na ogólności, jeśli rozważa się tylko drzewa bez pętli i krawędzi wielokrotnych.

Twierdzenie 4.9 [3]

Niech G będzie grafem bez pętli i krawędzi wielokrotnych, mającym więcej niż jeden wierzchołek. Następujące warunki są równoważne:

a) G jest drzewem;

b) każde dwa różne wierzchołki są połączone dokładnie jedną drogą prostą;

c) graf G jest spójny (mający $n-1$ krawędzi), ale przestaje być spójny po usunięciu dowolnej krawędzi;

d) graf G jest acykliczny (mający $n-1$ krawędzi), ale przestaje być acykliczny po dodaniu jakiejkolwiek krawędzi.

Wierzchołki stopnia pierwszego w drzewie nazywamy **liśćmi**.

Uwaga:
Drzewo skończone, mające co najmniej jedną krawędź, ma co najmniej dwa liście.
Drzewo mające n wierzchołków ma dokładnie $n-1$ krawędzi.

Twierdzenie 4.10 [3]

Niech G będzie grafem skończonym mającym n wierzchołków i niemającym pętli i krawędzi wielokrotnych. Następujące warunki są równoważne:

a) G jest drzewem;

b) G jest grafem acyklicznym mającym $n-1$ krawędzi;

c) G jest grafem spójnym mającym $n-1$ krawędzi.

(Każde dwie spośród własności: „spójność”, „acykliczność” i „posiadanie $n-1$ krawędzi” implikują trzecią z nich).

Graf acykliczny, który niekoniecznie jest spójny, nazywamy **lasem**. Spójne składowe lasu są drzewami.

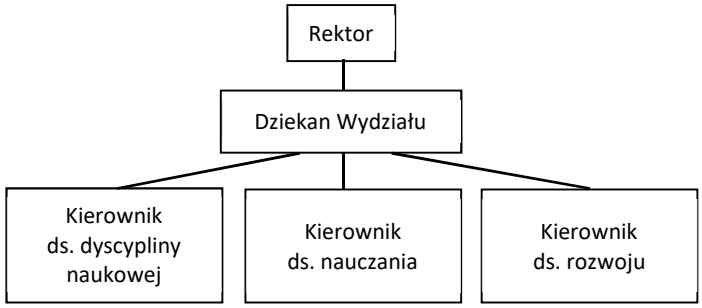
Drzewo z wyróżnionym korzeniem jest to drzewo, w którym jest wyróżniony jeden wierzchołek, nazywany **korzeniem**.

Drzewa z wyróżnionym korzeniem mają zastosowanie jako struktury danych, pomagają opisywać i wizualizować zachodzące relacje w wielu różnorodnych sytuacjach.

Drzewa z wyróżnionym korzeniem zazwyczaj rysuje się tak, że korzeń znajduje się na górze.

Przykład 4.17

Na poniższym rysunku przedstawione jest drzewo obrazujące strukturę na wydziale uczelni.



Drzewa z wyróżnionym korzeniem można traktować jako graf skierowany. Zazwyczaj jednak nie rysuje się strzałek na krawędziach, przyjmując, że wszystkie wskazują w dół. Drzewo T z wyróżnionym korzeniem r będziemy oznaczać przez T_r.

Korzenia, mimo że może być wierzchołkiem stopnia 1 (*Przykład 4.17*), nie nazywa się liściem.

Wierzchołki różne od korzenia i liści nazywa się też **węzłami gałęzi** (węzłami wewnętrznymi), a liście **węzłami końcowymi**.

Przyjmuje się, że jeśli para (v, w) jest krawędzią drzewa z wyróżnionym korzeniem, to v jest **rodzicem**, a w jest **dzieckiem** v.

Każdy wierzchołek poza korzeniem ma dokładnie jednego rodzica. Rodzic może mieć kilkoro dzieci.

Wierzchołek w jest **potomkiem** v, jeśli $w \neq v$ i v jest wierzchołkiem jedynej drogi prostej z korzenia r do wierzchołka v.

Dla dowolnego wierzchołka v **poddrzewo** o korzeniu v jest to dokładnie drzewo T_v składające się z wierzchołka v, wszystkich jego potomków i krawędzi skierowanych łączących ich.

Drzewo z wyróżnionym korzeniem jest **drzewem binarnym** wtedy, gdy każdy węzeł ma co najwyżej dwoje dzieci:

- dziecko lewe,
- dziecko prawe,
- dziecko lewe i dziecko prawe,
- nie ma dzieci.

Przykłady takich drzew zostaną omówione w *Rozdziale 5*.

Drzewem o m rozgałęzieniach ($m > 2$) nazywa się drzewo, w którym dzieci każdego rodzica są oznaczone różnymi elementami zbioru $\{1, 2, \dots, m\}$. Rodzic nie musi mieć całego zbioru dzieci (dziecko i jest nieobecne, jeśli nie ma dziecka oznaczonego liczbą i).

Drzewo o m rozgałęzieniach (lub drzewo binarne) jest **drzewem regularnym o m rozgałęzieniach**, jeśli stopień wyjściowy każdego wierzchołka jest równy m lub 0.

Numerem poziomu wierzchołka v nazywa się długość jedynej drogi prostej od korzenia do v. Korzeń ma numer poziomu równy 0. Wysokość drzewa z wyróżnionym korzeniem jest to największy numer poziomu wierzchołka.

Regularne drzewo o m rozgałęzieniach jest **pełnym drzewem o m rozgałęzieniach**, jeśli wszystkie liście mają ten sam numer poziomu równy wysokości drzewa.

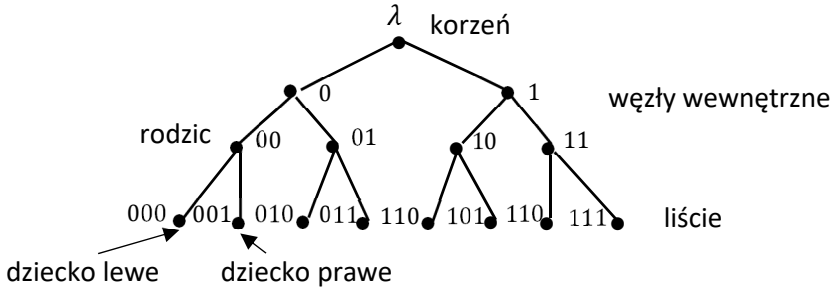
Jeśli uporządkuje się dzieci każdego rodzica w drzewie, otrzyma się tzw. **uporządkowane drzewo z wyróżnionym korzeniem**. (Kiedy rysuje się takie drzewo, rysuje się dzieci w porządku od lewej do prawej).

Przykład 4.18

Na poniższym rysunku przedstawione jest uporządkowane pełne drzewo binarne o wysokości 3.

Słowa $\Sigma^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111\}$

(λ – słowo puste, korzeń), otrzymane z liter alfabetu $\sum = \{0, 1\}$



4.6. Zadania do rozwiązania

1. Dla każdej macierzy narysować odpowiadający jej graf skierowany. Podać liczbę dróg długości 1 oraz 2.

a) $M = \begin{bmatrix} 0 & 0 & 2 & 1 \\ 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ b) $M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 3 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 \end{bmatrix}$

c) $M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$ d) $M = \begin{bmatrix} 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

2. Dla każdej macierzy narysować odpowiadający jej graf nieskierowany. Podać liczbę dróg długości 1 oraz 2.

a) $M = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{bmatrix}$ b) $M = \begin{bmatrix} 1 & 2 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 1 & 0 & 3 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$

c) $M = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ d) $M = \begin{bmatrix} 0 & 2 & 0 & 1 & 0 \\ 2 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

3. W zbiorze $S = \{1, 2, 3, 4, 5\}$ relacja R jest określona następująco:

   $(m, n) \epsilon R \Leftrightarrow m \cdot n + 1$ jest podzielne przez 3.

   Zbudować graf i odpowiednią macierz reprezentującą relację R. Oblicz, ile jest dróg o długości 2 pomiędzy wierzchołkami grafu tej relacji.

4. Ile jest wszystkich grafów skierowanych o:

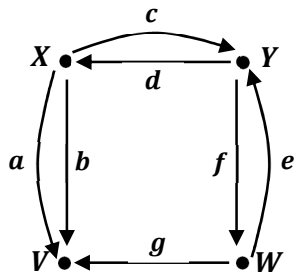
   a) dwóch wierzchołkach,

   b) trzech wierzchołkach,

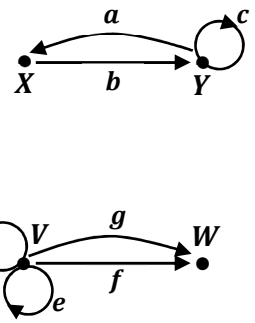
   c) czterech wierzchołkach?

5. Dla poniższych grafów podać: tabelę funkcji γ, macierz sąsiedztwa, liczbę dróg długości 1 (dla grafu a), liczbę dróg długości 2 (dla grafu b). Podać przykłady dróg długości $2, 3$ i 4.

a)



b)



6. Dla danych macierzy sąsiedztwa zbudować graf i wyznaczyć jego niezmienniki izomorfizmu:

a) $M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 2 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

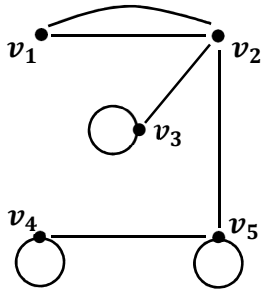
b) $M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 2 & 2 & 0 \\ 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

c) $M = \begin{bmatrix} 2 & 1 & 1 & 0 & 2 \\ 1 & 3 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 \\ 2 & 1 & 1 & 0 & 0 \end{bmatrix}$

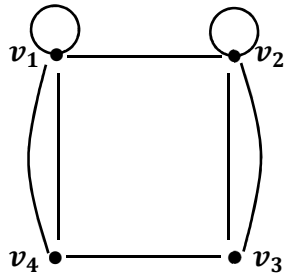
d) $M = \begin{bmatrix} 2 & 1 & 1 & 0 & 2 \\ 1 & 3 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 & 0 \\ 2 & 1 & 1 & 0 & 0 \end{bmatrix}$

7. Wyznaczyć niezmienniki izomorfizmu następujących grafów:

a)



b)



8. Które z następujących ciągów są ciągami liczb wierzchołków kolejnych stopni grafów? W każdym przypadku albo narysować graf o danym ciągu liczb wierzchołków kolejnych stopni tego grafu, albo wyjaśnić, dlaczego graf nie istnieje:

a) $(3, 2, 0, 3, 1, 0, 0, \dots)$

b) $(1, 0, 1, 0, 1, 2, 2, 0, \dots)$

c) $(1, 2, 3, 4, 0, 0, 0, \dots)$

d) $(0, 0, 1, 2, 1, 0, 0, 1, 0, \dots)$

e) $(4, 3, 2, 0, 0, 0, 0, \dots)$

f) $(2, 1, 2, 3, 2, 0, 1, 0, \dots)$

g) $(2, 3, 2, 0, 0, 0, 0, \dots)$

h) $(0, 0, 2, 2, 2, 0, 0, \dots)$

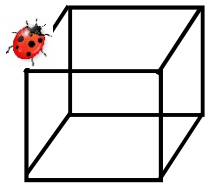
9. Zrobić rysunki pięciu grafów regularnych o pięciu wierzchołkach, z których każdy ma stopień 2.

10. Zrobić rysunki wszystkich grafów o czterech wierzchołkach i czterech krawędziach, które nie mają pętli ani krawędzi wielokrotnych. Ile będzie takich grafów, jeśli uwzględni się również pętle i krawędzie wielokrotne?

11. Graf o 21 krawędziach ma 7 wierzchołków stopnia 1, 3 wierzchołki stopnia 2, 7 wierzchołków stopnia 3, a pozostałe wierzchołki mają stopień 4. Ile ma on wierzchołków? Narysować ten graf.

12. Pewien graf ma 16 krawędzi oraz: 3 wierzchołki stopnia 0, 1 wierzchołek stopnia 2, 3 wierzchołki stopnia 4, pewną liczbę wierzchołków stopnia 3 i dwa wierzchołki stopnia 5.

13. Które grafy pełne mają cykle Eulera? Podać przykłady.



14. Czy biedronka poruszająca się wzdłuż krawędzi sześcianu może przejść każdą krawędź i to tylko raz? Odpowiedź uzasadnić.
Jaka byłaby odpowiedź, gdyby biedronka spacerowała po krawędziach ośmiościanu foremnego?

15. Macierze sąsiedztwa dla pewnych grafów mają postać:

a) $M = \begin{bmatrix} 0 & 2 & 2 & 1 \\ 2 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$ b) $M = \begin{bmatrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix}$

c) $M = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$ d) $M = \begin{bmatrix} 0 & 2 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

Przeanalizować, czy istnieją w tych grafach drogi lub cykle Eulera oraz drogi lub cykle Hamiltona. Jeśli tak, to je skonstruować, jeśli nie, wytłumaczyć dlaczego?

16. Znaleźć wszystkie drzewa o 5, 6 i 7 wierzchołkach.

17. Pewne drzewo ma 1 wierzchołek stopnia 5, 2 wierzchołki stopnia 3 i 3 wierzchołki stopnia 2. Pozostałe wierzchołki są stopnia 1. Narysować dwa takie drzewa.

18. Pewne drzewo ma 2 wierzchołki stopnia 4, 1 wierzchołek stopnia 3 i 1 wierzchołek stopnia 2. Jeśli inne wierzchołki są stopnia 1, to ile wierzchołków jest w tym grafie? Narysować opisane drzewo.

19. Pokazać, że istnieje drzewo mające 6 wierzchołków stopnia 1, 1 wierzchołek stopnia 2, 1 wierzchołek stopnia 3, 1 wierzchołek stopnia 5 i żadnych innych.

20. Narysować uporządkowane pełne drzewo o wysokości 3, w którym wierzchołki są słowami ze zbioru Σ^* powstałymi ze zbioru (alfabetu) $\Sigma = \{a, b, c\}$. Podać przykład poddrzewa.

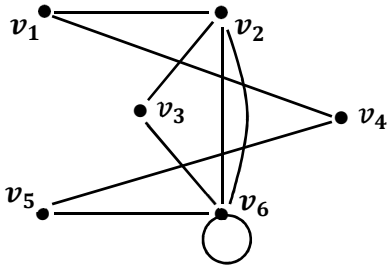
21. Narysować uporządkowane drzewo o wierzchołkach ze zbioru:

    $\Sigma = \{\lambda, 0, 1, 2, 00, 01, 10, 11, 12, 20, 000, 201, 202, 121, 122, 010, 011, 100, 101, 0001, 2021\}$

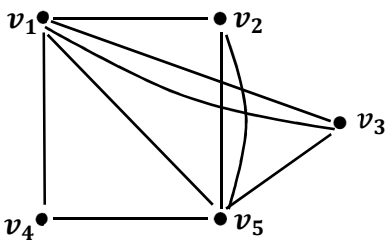
    Wypisać liście tego drzewa. Jaka jest wysokość tego drzewa? Czy jest to drzewo binarne? Czy można wskazać przykład dziecka lewego i dziecka prawego? Czy jest to drzewo regularne?

22. Dla podanych grafów narysować po 2 drzewa spinające, a następnie, wyróżniając w nich jeden z wierzchołków jako korzeń, narysować drzewa z wyróżnionym korzeniem. Jaką wysokość mają te drzewa?

a)



b)



4.7. Wskazówki i odpowiedzi do zadań

1. a) $LDD_1=11$, $LDD_2=30$,
   d) $LDD_1=13$, $LDD_2=35$.

2. b) $LDD_1=13$, $LDD_2=45$,
   c) $LDD_1=7$, $LDD_2=11$.

4. a) $2^4 = 16$ b) $2^9 = 516$ c) $2^{16} = 65536$

5. b)

E	a	b	c	d	e	f	g
$\gamma(E)$	(Y,X)	(X,Y)	(Y,Y)	(V,V)	(V,V)	(V,W)	(V,W)

6. c) LW=5, LK=7, LP=7, $LDD_1=21$, $LDD_2=95$, $(0, 0, 0, 1, 1, 1, 0, 0, 2, 0, \dots)$

7. b) LW=4, LK=6, LP=2, $LDD_1=14$, $LDD_2=50$, $(0, 0, 0, 2, 0, 2, 0, \dots)$

8. e) Graf nie istnieje, bo suma stopni wierzchołków wynosi 7 (nie jest liczbą parzystą).

   f) Graf istnieje bo suma stopni wierzchołków wynosi 28 (graf ma więc 11 wierzchołków i 14 krawędzi).

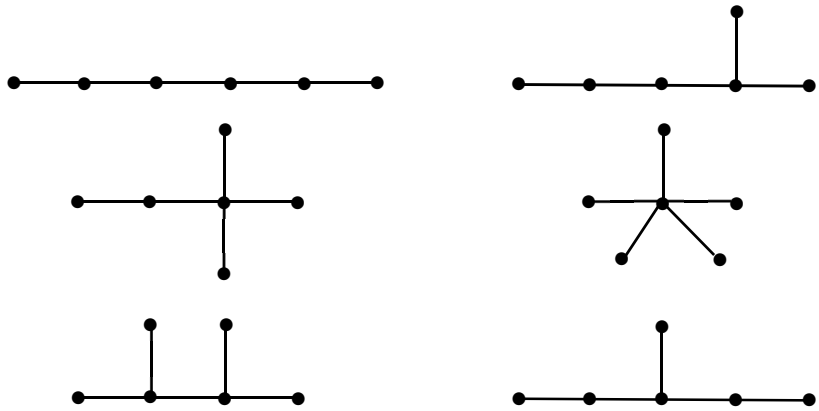
11. Dwa wierzchołki są stopnia 4, więc wszystkich wierzchołków w grafie jest 19.

15. b) Są drogi Eulera i Hamiltona, brak cykli.

    c) Jest cykl Eulera (a więc i droga) oraz droga Hamiltona (nie ma cyklu).

    d) Brak drogi i cyklu Eulera, jest droga Hamiltona.

16. Drzewa o sześciu wierzchołkach:



18. Wskazówka: Drzewo o n wierzchołkach ma dokładnie $n-1$ krawędzi, więc suma stopni wierzchołków wynosi $2n-2$. Jeśli drzewo ma n wierzchołków, to $n-4$ z nich będą miały stopień 1.

21. Liście: $0001, 010, 011, 100, 101, 121, 122, 2021$. Dzieckiem lewym jest np. 10 czy 121, a dzieckiem prawym $101, 202$. Nie jest to drzewo regularne.

4.8. Literatura

[1] W. Broniowski, *Matematyka dyskretna*, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2014.

[2] J. Chrostowski, *Grafy wiedzą lepiej*, „Polityka" 2013, nr 20(2907).

[3] K.A. Ross, Ch.R.B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[4] N.L. Biggs, *Discrete Mathematics*, Oxford University Press, New York 2002.

[5] R.L. Graham, D.E. Knuth, O. Patashnik, *Matematyka konkretna*, Państwowe Wydawnictwo Naukowe, Warszawa 2008.

[6] J. Grygiel, *Wprowadzenie do matematyki dyskretnej*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2007.

[7] M. Libura, J. Sikorski, *Wykłady z matematyki dyskretnej. Część II: Teoria grafów*, Wydawnictwo WIT, Warszawa 2005.

[8] L. Lovász, K. Vesztergombi, *Discrete Mathematics*, Lecture Notes, Yale University 1999.

[9] M. Sipser, *Wprowadzenie do teorii obliczeń*, Wydawnictwa Naukowo-Techniczne, Warszawa 2009.

[10] A. Szepietowski, *Matematyka dyskretna*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2004.

[11] R.J. Wilson, *Wprowadzenie do teorii grafów*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[12] M. Zakrzewski, *Markowe wykłady z matematyki*, Oficyna Wydawnicza GiS, Wrocław 2014.

[13] http://wazniak.mimuw.edu.pl

Rozdział 5

Elementy teorii kodowania. Kod Huffmana

5.1. Wybrane aspekty kodowania informacji

Jednym ze znanych kodów jest kod ASCII [1, 2]. W kodzie tym każdy symbol jest kodowany za pomocą słowa binarnego o długości 8. Istotną cechą kodu ASCII, jak i wielu innych kodów, jest to, że każdy symbol ma kod o tej samej długości (tzw. *fixed length character code*). Ma to swoje plusy i minusy.

- Plusem jest to, że nie potrzeba żadnego specjalnego symbolu do oddzielania symboli w informacji. Dzięki temu łatwo jest odkodować informację.
- Minusem jest to, że często powtarzające się symbole mają kod o takiej samej długości jak występujące rzadko. Jest to więc strata czasu i przestrzeni w procesie kodowania i odkodowywania.

Powstała więc idea używania kodów o zmiennej długości charakterów, tzn. symbolom często występującym przypisuje się krótkie charaktery, zaś tym o małej częstości odpowiadają dłuższe charaktery.

O ile nie ma problemu z wyborem możliwie krótkich charakterów kodujących, to może wystąpić problem z odczytem kodu, gdyż przy zmiennej długości charakterów trzeba wiedzieć, gdzie kończy się kod jakiegoś symbolu, a gdzie zaczyna następny.

Przykład 5.1

Dany jest zbiór symboli $C = \{a, b, c, d, e, f\}$. Założono, że a oraz b mają największą częstość występowania. Można więc wybrać następujący kod: $a - 0, b - 1, c - 00$, $d - 01, e - 10, f - 11$. Kod ten jest bardzo „krótki" w tym sensie, że indywidualne symbole są kodowane przez najkrótsze możliwe charaktery.

Jak jednak odczytać następującą zakodowaną informację: 010011? Czy „010011" oznacza „$abaabb$" czy też „dcf"?

Można problem niejednoznaczności odczytu rozwiązać, wprowadzając dodatkowy charakter, np. „/" do oddzielania indywidualnych charakterów. Jednak taki zabieg wydłuża kodowaną informację.

5.2. Kod prefiksowy

Istnieje metoda ominięcia niejednoznaczności dekodowania. Metoda ta wykorzystuje tzw. kody prefiksowe.

Definicja 5.1

Słowo w jest **prefiksem** słowa u, jeśli u ma postać $u = wx$, gdzie x jest innym słowem. Słowo wx oznacza konkatenację słów w i x.

Może się zdarzyć, że kod dla jednego symbolu jest prefiksem dla innego, to powoduje, że nie wiadomo, jak interpretować informację.

Kod o tej własności, że kod indywidualnego symbolu nie jest prefiksem żadnego innego symbolu, nazywa się **kodem prefiksowym**. Taki kod jest jednoznacznie dekodowalny. Każdy kod prefiksowy można przedstawić w formie drzewa. Dla kodów dwójkowych jest to drzewo binarne.

Przykład 5.2

Czy podany kod $a - 11, b\ - 0, c - 100, d\ -\ 1010, e\ -\ 1011$ jest kodem prefiksowym dla zbioru symboli $\{a, b, c, d, e\}$? Jeśli tak, to odczytać informację zawartą w: 101110101010100111001100.

Jest to kod prefiksowy. Można łatwo odczytać informację, dzieląc ciąg binarny. $10111010\ 1010100111001100\ (= 1011\ 1010\ \ 1010\ 100\ 11\ 100\ 11\ 0\ 0)$.
Odczytana informacja to: $eddcacabb$.

W dalszej części rozważań pokazano, jak zbudować jak najkrótszy kod prefiksowy. Do zbudowania kodu potrzebna jest znajomość częstości występowania symboli w kodowanym języku. Jest to charakterystyka, która występuje w badaniu nad językiem. Przypisuje się każdemu symbolowi częstość f względem zbioru symboli.

Przykład 5.3

Dany jest zbiór symboli $C = \{e, g, h, i\}$ i przypisane im częstości $f(e) = 3$, $f(g) = 3, f(h) = 8, f(i) = 6$. Co oznaczają częstości? Oznaczają, że w danym języku zapisywanym przy pomocy tych czterech symboli na każde 3 wystąpienia symbolu e symbol g pojawia się też 3 razy, symbol h 8 razy, a symbol i 6 razy. Wynika z tego, że dla tych czterech wymienionych symboli symbol h pojawia się najczęściej.

Częstości symboli są niezbędne do obliczenia wagi kodu.

Definicja 5.2

Niech $C = \{a_{1,}\, a_2, \dots, a_k\}$ jest zbiorem symboli, zaś $f(a_1), f(a_2), \dots, f(a_k)$ są częstościami tych symboli, gdzie k jest dowolną liczbą naturalną dodatnią nie mniejszą od 1. Przyjęto, że dany jest zbiór charakterów kodujących poszczególne symbole oraz że $l(a_1), l(a_2), \dots, l(a_k)$ są długościami tych charakterów kodujących. Wtedy **wagą kodu** jest $w = \sum_{i=1}^{i=k} f(a_i) l(a_i)$.

Przykład 5.4

Obliczyć wagę kodu: $a - 11, b - 0, c - 101, d - 1000, e - 1001$ o częstościach $f(a) = 5, f(b) = 8, f(c) = 8, f(d) = f(e) = 1$.

Waga kodu wynosi:

$$w = f(a) \cdot l(a) + f(b) \cdot l(b) + f(c) \cdot l(c) + f(d) \cdot l(d) + f(e) \cdot l(e) =$$
$$= 5 \cdot 2 + 8 \cdot 1 + 8 \cdot 3 + 1 \cdot 4 + 1 \cdot 4 = 50$$

5.3. Kod Huffmana

Im mniejsza waga kodu, tym kod jest efektywniejszy. W podrozdziale zostanie zaprezentowana metoda konstruowania najefektywniejszego kodu prefiksowego. Kod ten został skonstruowany przez D.A. Huffmana [3]. Produktem algorytmu Huffmana jest zawsze optymalne rozwiązanie dla znanego zbioru wejściowego. Algorytm należy do najefektywniejszych systemów bezstratnej kompresji danych. Niestety nie jest on efektywny obliczeniowo. Algorytmu Huffmana nie używa się samodzielnie. Wykorzystywany jest jako ostatni etap kompresji np. MP3 lub JPEG.

Fenomen algorytmu Huffmana:

- prostota działania,
- brak ograniczeń patentowych.

Idea kodu Huffmana [1, 2] polega na tworzeniu słów kodowych (ciągów bitowych), które tym mniej zajmują bitów, im częściej dany symbol występuje. Jeśli chodzi o kod Huffmana, to:

- Jest kodem prefiksowym.
- Jego średnia długość słowa kodowego jest najmniejsza spośród kodów prefiksowych.

Algorytm konstrukcji statycznego kodu Huffmana

Algorytm składa się z kilku charakterystycznych kroków [1, 2]:

Krok 1. Zlicza się liczbę wystąpień każdego symbolu w używanym języku.

Krok 2. Tworzy się drzewo binarne.

1. Dla każdego symbolu tworzy się wierzchołek, który przechowuje pary: symbol oraz wartość liczby równej liczbie wystąpień tego symbolu w badanym języku.
2. Porządkuje się wierzchołki względem wzrastającej częstości.
3. Następnie łączy się dwa wierzchołki z najmniejszymi wartościami częstości, które tworzą nowy wierzchołek. Wierzchołek ten ma wartość równą sumie wartości obu połączonych węzłów. Tworzy się listę drzew binarnych.

Czynności 2 i 3 powtarza się tak długo, dopóki jest wolny więcej niż jeden węzeł.

Drzewo, które pozostanie na liście, jest nazywane **drzewem Huffmana**. Prawdopodobieństwo zapisane w korzeniu jest równe 1. W liściach drzewa zapisane są symbole. Następnie na podstawie drzewa tworzone są słowa kodowe. Każdej lewej krawędzi i prawej krawędzi przypisuje się odpowiednio 0 i 1. Jest też możliwe przypisanie odwrotne, ale w dalszej części rozdziału korzysta się z pierwszego przypisania. Kolejnym etapem jest odczytanie kodu dla każdego symbolu (liścia). Kod ma początek w korzeniu, a koniec w symbolu (liściu) i jest on ciągiem zer i jedynek. Długość słowa kodowego jest zależna od położenia symbolu w drzewie.

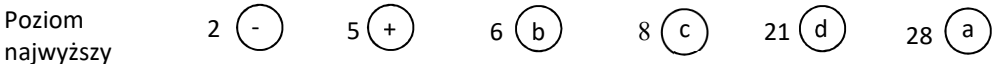
Wady algorytmu Huffmana

Algorytm jest algorytmem niedeterministycznym. Nie określa w jasny sposób kolejności wybierania drzewa z listy w przypadku takiego samego prawdopodobieństwa drzew oraz tego, gdzie umieścić usuwane drzewo, na pozycji lewego czy prawego poddrzewa. To wszystko nie ma wpływu na średnią długość kodu, która pozostaje taka sama bez względu na przyjęte rozwiązanie.

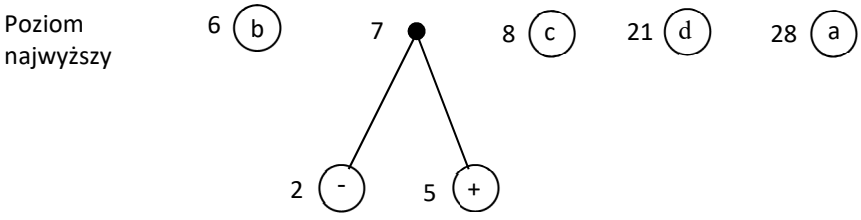
Przykład 5.5

Skonstruować drzewo Huffmana dla zbioru symboli od podanych częstościach występowania: $f(a) = 28, f(b) = 6, f(c) = 8, f(d) = 21, f(-) = 2, f(+) = 5$.

Krok 1. Umieszczenie jednego wierzchołka dla każdego symbolu na najwyższym poziomie. Oznaczenie wierzchołków odpowiadającymi im symbolami i przypisanie im częstości występowania symboli w języku. Uporządkowanie wierzchołków względem wzrastającej częstości.

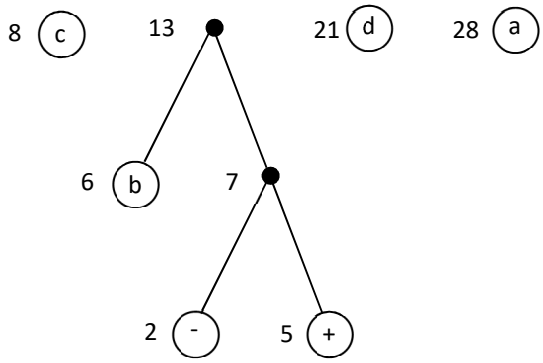


Krok 2. Łączenie dwóch wierzchołków o najmniejszej częstości do nowego wierzchołka na poziomie o jeden wyższym. Oznaczanie nowego wierzchołka sumą częstości. Podniesienie pozostałych wierzchołków o jeden poziom wyżej, tak je przestawiając, aby zachowane było uporządkowanie wierzchołków względem wzrastającej częstości.

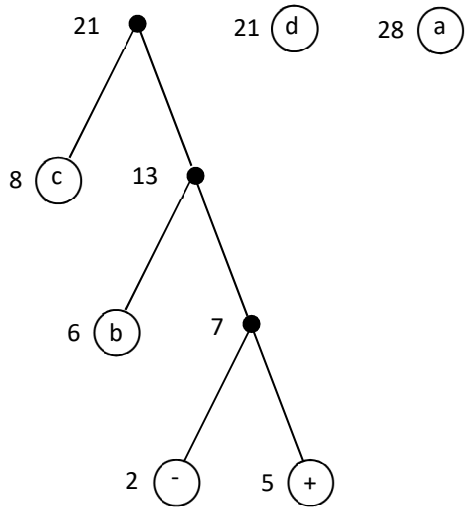


Krok 3. Powtarzanie *Kroku 2* tak długo, aż na najwyższym poziomie zostanie jeden wierzchołek.

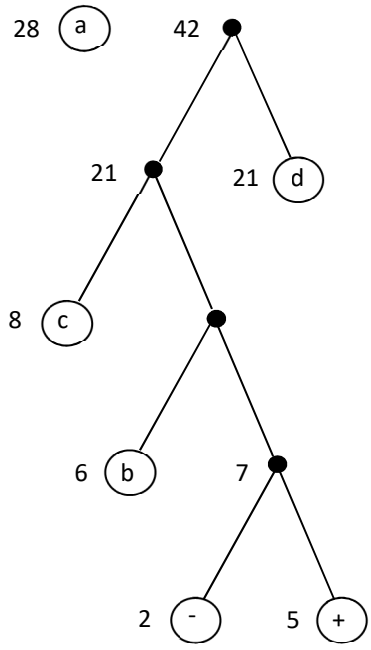
Poziom najwyższy



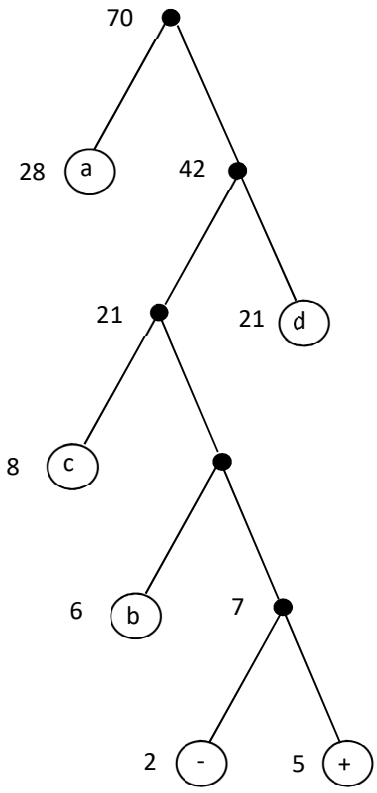
Poziom najwyższy



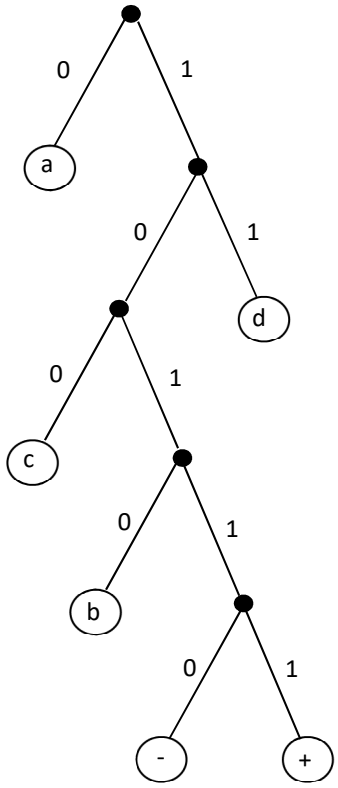
Poziom najwyższy



Poziom najwyższy



Krok 4. Usunięcie wszystkich etykiet częstości oraz oznaczenie każdej lewej krawędzi przez 0, a każdej prawej krawędzi przez 1.



Tak otrzymany graf nazywa się **drzewem Huffmana**.

Przykład 5.6

Dla drzewa skonstruowanego w *Przykładzie 5.5* zbudować tabelę kodu.

Kod wybranego symbolu otrzymuje się, wypisując wszystkie 0 i 1, jakie napotyka się na drodze o początku w korzeniu drzewa i końcu w wierzchołku przypisanemu danemu symbolowi.

Symbol	Częstość	Kod Huffmana
a	28	0
b	6	1010
c	8	100
d	21	11
$+$	5	10111
$-$	2	10110

Przykład 5.7

Na podstawie danych zawartych w tabeli w *Przykładzie 5.6* obliczyć wagę kodu.

Jest to **kod prefiksowy**, ponadto symbole o wysokiej częstości występowania mają krótsze kody niż te o małej częstości. Waga naszego kodu wynosi:

$$w = 28 \cdot 1 + 6 \cdot 4 + 8 \cdot 3 + 21 \cdot 2 + 5 \cdot 5 + 2 \cdot 5 = 153$$

Kod Huffmana jest kodem o najmniejszej możliwej wadze pośród wszystkich kodów prefiksowych.

Podane w powyższym algorytmie częstości występowania symboli można zastąpić prawdopodobieństwami pojawienia się poszczególnych symboli. Procedura przejścia od częstotliwości do prawdopodobieństw jest następująca:

Symbol	**Częstość** f_i	**Prawdopodobieństwo** $p_i = \frac{f_i}{\sum_{i=1,6} f_i}$
a	28	$\frac{28}{70}$
b	6	$\frac{6}{70}$
c	8	$\frac{8}{70}$
d	21	$\frac{21}{70}$
$+$	5	$\frac{5}{70}$
$-$	2	$\frac{2}{70}$
	$\sum_{i=1,6} f_i = 70$	$\sum_{i=1,6} p_i = 1$

Entropia, w ramach teorii informacji, jest definiowana jako średnia ilość informacji przypadająca na znak symbolizujący zajście zdarzenia z pewnego zbioru. Zdarzenia w tym zbiorze mają przypisane prawdopodobieństwa wystąpienia.

Przykład 5.8

Na podstawie danych z *Przykładu 5.7* obliczyć entropię odpowiadającą kodowi i porównać ją z entropią Shanona.

Symbol	p_i	**Kod Huffmana**	**Długość [bit]**
a	$\frac{28}{70}$	0	1
b	$\frac{6}{70}$	1010	4
c	$\frac{8}{70}$	100	3
d	$\frac{21}{70}$	11	2
$+$	$\frac{5}{70}$	10111	5
$-$	$\frac{2}{70}$	10110	5

$$S_{KOD} = 1 \cdot \frac{28}{70} + 4 \cdot \frac{6}{70} + 3 \cdot \frac{8}{70} + 2 \cdot \frac{21}{70} + 5 \cdot \frac{5}{70} + 5 \cdot \frac{2}{70} = \frac{161}{70} = 2.3$$

$$S_{SHANON} = -\sum_{i=1,6} p_i \log_2 p_i \approx 2.13$$

Kod Huffmana ma najmniejszą entropię spośród kodów prefiksowych. Wartość tej entropii jest bliska teoretycznej granicy danej wartością entropii Shanona.

Kody Huffmana mają duże znaczenie w praktyce, ze względu na zastosowania do efektywnego przesyłania wiadomości oraz do projektowania struktur danych będących drzewami poszukiwań.

Więcej informacji na temat kodu Huffmana można znaleźć w [4].

5.4. Zadania do rozwiązania

1. Rozważyć następującą tabelę kodów:

Symbol	Częstość	Kod 1	Kod 2
A	2	111	1000
B	12	110	01
C	1	10	11111
D	6	0	10

   a) Obliczyć wagi kodów.

   b) Który z kodów jest kodem prefiksowym? Uzasadnić odpowiedź.

2. Zbudować optymalne drzewo binarne z podanymi wagami i obliczyć wagę tego optymalnego drzewa binarnego.

   a) $2, 3, 5, 7, 10, 13, 19$ [4]

   b) $2, 4, 6, 7, 7, 9$ [4]

   c) $1, 1, 2, 4, 7, 9, 15$

3. Znaleźć najbardziej efektywny kod prefiksowy dla zbioru częstości $\{5, 5, 10, 11, 19, 20, 30\}$. Jaka jest średnia długość zakodowanej wiadomości mająca sto liter?

4. Czy zbiór $\{00, 01, 100, 1010, 1011, 11\}$ jest kodem prefiksowym? Czy da się odkodować słowo 0010011101010100001? [4]

5. Rozważyć następujący alfabet:

Symbol	Częstość
a	3
b	1
c	2

   a) Znaleźć kod Huffmana dla podanego alfabetu i obliczyć jego wagę.
   b) Zakodować informację: $baccab$.
   c) Odkodować wiadomość: 01001001.
   d) Obliczyć entropię odpowiadającą kodowi i porównać ją z entropią Shanona.

6. Rozważyć następujący alfabet:

Symbol	Częstość
e	4
f	5
$+$	7
$*$	8
$($	12
$)$	25

   a) Znaleźć kod Huffmana dla podanego alfabetu i obliczyć jego wagę.
   b) Zakodować informację: $e \cdot (e + f)$.
   c) Odkodować wiadomość: $11001011101101111110010011010$.
   d) Obliczyć entropię odpowiadającą kodowi i porównać ją z entropią Shanona.

7. Zaprojektować kod Huffmana dla podanego alfabetu. Obliczyć wagę kodu [5].

Symbol	Częstość	Symbol	Częstość
A	16	M	4
H	7	T	12
I	8	♡	5

   Odkodować informację: 1010010001101100.

8. Dany jest fikcyjny alfabet składający się z sześciu liter: n, f, u, m, h, a z następującymi częstościami liter: $n - 22, f - 5, u - 18, m - 17, h - 2, a - 7$. Zaprojektować optymalny binarny kod prefiksowy dla tego alfabetu. Obliczyć wagę i entropię kodu. Odkodować wiadomość: 000010000100010100111. Zakodować informację: $human$.

9. Dany jest fikcyjny alfabet składający się z sześciu liter: r, x, m, t, i, a z następującymi częstościami liter: $r-13, x-7, m-6, t-3, i-29, a-2$. Zaprojektować optymalny binarny kod prefiksowy dla tego alfabetu. Obliczyć wagę i entropię kodu. Odkodować wiadomość: 1110110011011001111. Zakodować informację: $tram$.

10. Dany jest fikcyjny alfabet składający się z siedmiu liter: a, b, c, x, y, z, w z następującymi częstościami liter: $a-22, b-17, c-20, x-5, y-12, z-21, \mathrm{w}-3$. Zaprojektować optymalny binarny kod prefiksowy dla tego alfabetu. Jaka jest średnia długość zakodowanej wiadomości składającej się ze 100 liter alfabetu?

5.5. Wskazówki i odpowiedzi do zadań

1. a) $w_1 = 50, w_2 = 49$ b) Kod 1

3. 260

4. Tak.

5.6. Literatura

[1] http://wazniak.mimuw.edu.pl

[2] https://pl.wikipedia.org

[3] D.A. Huffman, *A Method for the Construction of Minimum Redundancy Codes*, „Proceedings of the IRE", 1952, Vol. 40, s. 1098-1101.

[4] K.A. Ross, Ch.R.B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[5] Z. Domański, wykłady z matematyki dyskretnej, niepublikowane.