Matematyka dyskretna

Mariusz Żynel

25 kwietnia 2017

Spis treści

1 Relacje

1.1 Własności

Niech A będzie niepustym zbiorem. Przez W oznaczmy własność, którą mogą mieć elementy ze zbioru A, natomiast

$$W_A = \{a \in A\colon a \text{ ma własność } W\}$$

będzie podzbiorem A elementów o własności W. Własności W jednoznacznie odpowiada zbiór W_A i na odwrót, wybierając dowolny podzbiór elementów ze zbioru A możemy powiedzieć, że to właśnie one mają pewną własność – należą do tego podzbioru. Widzimy wzjemnie jednoznaczną zależność pomiędzy własnością W a zbiorem W_A.

Przykład 1.1. Niech $A = \mathbb{N}$, a W niech oznacza podzielność przez 3. Wówczas

$$W_A = \{0, 3, 6, 9, \ldots\}.$$

1.2 Iloczyn kartezjański

Niech X, Y będą dowolnymi zbiorami. *Iloczyn kartezjański* zbiorów X i Y to zbiór par uporządkowanych

$$X \times Y = \big\{(x, y)\colon x \in X, y \in Y\big\}.$$

Przykład 1.2. Niech $X = \{1, 2, 3\}$, $Y = \{\alpha, \beta\}$. Wówczas

$$X \times Y = \big\{(1, \alpha), (2, \alpha), (3, \alpha), (1, \beta), (2, \beta), (3, \beta)\big\}.$$

1.3 Relacje

Relacja binarna (dwuargumentowa) to podzbiór iloczynu kartezjańskiego dwóch zbiorów.

Jeśli weźmiemy $A = X \times Y$, to W_A, podobnie jak wyżej, oznacza pewną własność, a zarazem podzbiór, iloczynu kartezjańskiego $X \times Y$. Ten podzbiór, czyli zbiór par o pewnej własności, to właśnie relacja — relacja pomiędzy pierwszą a drugą zmienną w iloczynie kartezjańskim.

Poza relacjami standardowymi, które mają swoje własne oznaczenia, relacje zwykle będziemy oznaczać grecką literą ρ. Także jeśli rozpatrujemy relację ρ pomiędzy elementami zbioru X a elementami zbioru Y, czyli relację w iloczynie kartezjańskim $X \times Y$, to formalnie

$$\rho \subseteq X \times Y.$$

Piszemy

- $(x, y) \in \rho$ i mówimy, że para (x, y) należy do relacji ρ, albo piszemy
- $x \; \rho \; y$ i wtedy mówimy, że element x jest w relacji ρ z elementem y,

dla $x \in X$ oraz $y \in Y$.

Przykład 1.3. Niech $X = \{1, 4, 5\}$, $Y = \{2, 3\}$ oraz

$$\rho = \{(x, y) \colon x + y \text{ jest liczbą parzystą}\}.$$

Wówczas

$$X \times Y = \{(1, 2), (4, 2), (5, 2), (1, 3), (4, 3), (5, 3)\} \quad \text{oraz}$$
$$\rho = \{(4, 2), (1, 3), (5, 3)\}.$$

Mówimy, że relacja $\rho \subseteq X \times Y$ jest określona na zbiorze $X \times Y$. Jeśli $Y = X$, to wówczas $\rho \subseteq X^2$ i mówimy krótko, że relacja ρ jest określona na zbiorze X.

1.4 Własności relacji

Rozważamy relację $\rho \subseteq X \times X$ dla dowolnego zbioru X.

zwrotność Relacja ρ jest zwrotna, wtw., gdy dla każdego $x \in X$ zachodzi $x \; \rho \; x$. Innymi słowy, zwrotność relacji oznacza, że każdy element jest w relacji ze sobą.

symetria Relacja ρ jest symetryczna, wtw., gdy dla dowolnych $x, y \in X$ jeśli $x \; \rho \; y$, to $y \; \rho \; x$. Intuicyjnie, symetria relacji oznacza, że możemy zamienić x z y w parze (x, y) o ile w ogóle $(x, y) \in \rho$. Tak więc kolejność występowania elementów w relacji nie ma tutaj znaczenia.

antysymetria Relacja ρ jest antysymetryczna, wtw., gdy dla dowolnych $x, y \in X$ jeśli $x \; \rho \; y$ oraz $y \; \rho \; x$, to $x = y$. Tak więc antysymetria relacji oznacza, że kolejność występowania różnych elementów w relacji jest istotna. To znaczy, że dla $x \neq y$ albo $x \; \rho \; y$, albo $y \; \rho \; x$, albo nie zachodzi ani jedno, ani drugie.

przechodniość Relacja ρ jest przechodnia, wtw., gdy dla dowolnych $x, y, z \in X$ jeśli $x \; \rho \; y$ oraz $y \; \rho \; z$, to również $x \; \rho \; z$.

1.5 Relacje równoważności i klasy abstrakcji

Relacja binarna jest *relacją równoważności*, gdy jest zwrotna, symetryczna i przechodnia.

PRZYKŁAD 1.4. Niech X = zbiór wszystkich ludzi (o jasno określonej płci). Dla $x, y \in X$ określamy relację ρ w następujący sposób

$$x \,\rho\, y \iff x \text{ jest tej samej płci co } y.$$

- *zwrotność*
  Zawsze człowiek x jest tej samej płci co x, tzn. $x \,\rho\, x$, więc relacja jest zwrotna.
- *symetria*
  Jeśli człowiek x jest tej samej płci co człowiek y, to również na odwrót, y jest tej samej płci co x. Zatem relacja ρ jest symetryczna.
- *przechodniość*
  Załóżmy, że człowiek x jest tej samej płci co y oraz, że y jest tej samej płci co z. Wówczas wszyscy x, y i z są tej samej płci, w szczególności x jest tej samej płci co z. Zatem relacja ρ jest przechodnia.

Pokazaliśmy, że relacja ρ jest relacją równoważności.

PRZYKŁAD 1.5. Niech X = zbiór wszystkich ludzi. Dla $x, y \in X$ określamy relację ρ w następujący sposób

$$x \,\rho\, y \iff x \text{ jest tego samego wzrostu co } y.$$

- *zwrotność*
  Człowiek x jest tego samego wzrostu co x, tzn. $x \,\rho\, x$.
- *symetria*
  Jeśli człowiek x jest tego samego wzrostu co y, to również na odwrót, y jest tego samego wzrostu co x.
- *przechodniość*
  Załóżmy, że człowiek x jest tego samego wzrostu co y oraz, że y jest tego samego wzrostu co z. Wówczas wszyscy x, y i z są tego samego wzrostu, w szczególności x jest tego samego wzrostu co z.

Tutaj również pokazaliśmy, że relacja ρ jest relacją równoważności.

PRZYKŁAD 1.6. Niech X = zbiór wszystkich ludzi. Dla $x, y \in X$ określamy relację ρ w następujący sposób

$$x \,\rho\, y \iff x \text{ jest niższy od } y.$$

- *zwrotność*
  Żaden człowiek nie jest niższy od samego siebie, więc ta relacja nie jest zwrotna.

- *symetria*
  Jeśli człowiek x jest niższy od y, to nie na odwrót, y nie jest niższy od x. Zatem relacja ρ nie jest symetryczna.

- *przechodniość*
  Załóżmy, że człowiek x jest niższy od y oraz, że y jest niższy od z. Wówczas x jest niższy od z i widać, że relacja jest przechodnia.

Ta relacja ρ nie jest relacją równoważnością.

Zauważmy, że w przykładzie 1.4 relacja ρ dzieli wszystkich ludzi na kobiety i mężczyzn. Formalnie zbiór X został podzielony na dwa podzbiory: podzbiór X_1 kobiet oraz podzbiór X_2 mężczyzn. Podzbiory te mają dwie istotne własności. Po pierwsze $X_1 \cap X_2 = \emptyset$, czyli są one *rozłączne*. Po drugie $X_1 \cup X_2 = X$, czyli w sumie dają cały zbiór X.

Mówimy, że rodzina $X_1, X_2, \ldots$ (niekoniecznie skończona) podzbiorów zbioru X jest *podziałem*, gdy $X = X_1 \cup X_2 \cup \ldots$ oraz $X_i \cap X_j = \emptyset$ dla $i \neq j$, czyli gdy w sumie daje cały zbiór X oraz elementy rodziny są parami rozłączne.

Można powiedzieć, że w zbiorze X wszystkich, różnych od siebie ludzi wyabstrachowaliśmy dwie cechy, które powodują, że cały zbiór X rozpada się na dwa podzbiory kobiet i mężczyzn. Z punktu widzenia relacji ρ wszystkie kobiety są nierozróżnialne i wszyscy mężczyźni są nierozróżnialni.

W przypadku relacji równoważności mówimy czasem, że x *przystaje* do y, zamiast mówić, że x jest w relcji z y. Podkreślamy w ten sposób, że x i y są dla tej relacji nierozróżnialne.

Każda relacja równoważności ρ na zbiorze X wyznacza jednoznacznie podział zbioru X na parami rozłączne podzbiory, które w sumie dają X. Podzbiory te nazywamy *klasami abstrakcji*. Elementy w jednej klasie abstrakcji przystają do siebie — są ze soba w relacji ρ. Elementy z różnych klas abstrakcji nie są w relacji ρ.

Zauważmy, że klasa abstrakcji jest jednoznacznie wyznaczona przez dowolny element z tej klasy. Taki element nazywamy *reprezentantem* klasy. Dla elementu $x \in X$ klasa abstrakcji wyznaczona przez x to zbiór

$$[x]_\rho = \{y \in X \colon x \,\rho\, y\}.$$

PRZYKŁAD 1.7. Niech $X = \mathbb{N} \times \mathbb{N}$. Dla $x = (m_1, n_1), y = (m_2, n_2) \in X$ określamy relację ρ w następujący sposób

$$x \,\rho\, y \iff (m_1, n_1) \,\rho\, (m_2, n_2) \iff m_1 + n_2 = n_1 + m_2,$$

czyli, gdy suma skrajnych zmiennych jest taka sama jak suma zmiennych w środku.

- *zwrotność*
  Niech $x = (m, n) \in X$. Oczywiście $m + n = n + m$ bo dodawanie dla liczb naturalnych jest przemienne. To oznacza, że $(m, n) \,\rho\, (m, n)$, czyli $x \,\rho\, x$.

- *symetria*
  Niech $x = (m_1, n_1), y = (m_2, n_2) \in X$. Załóżmy, że $x \,\rho\, y$, to znaczy, że

$m_1 + n_2 = n_1 + m_2$. Przestawmy składniki w pierwszej sumie i zamieńmy strony równości, dostaniemy $m_2 + n_1 = n_2 + m_1$. Z określenia ρ mamy

$$(m_2, n_2)\ \rho\ (m_1, n_1),$$

co oznacza, że $y\ \rho\ x$.

- *przechodniość*
  Niech teraz $x = (m_1, n_1), y = (m_2, n_2), z = (m_3, n_3) \in X$. Zakładamy, że $x\ \rho\ y$ oraz $y\ \rho\ z$. Z definicji ρ to daje

  $$m_1 + n_2 = n_1 + m_2 \qquad \text{oraz} \qquad m_2 + n_3 = n_2 + m_3.$$

  Przenieśmy wyrazy o tych samych indeksach na jedną stronę w każdej z obu równości. Dostajemy

  $$m_1 - n_1 = m_2 - n_2 \qquad \text{oraz} \qquad m_2 - n_2 = m_3 - n_3.$$

  Zauważmy, że zamiast słowa „oraz" możemy wstawić znak „=", czyli

  $$m_1 - n_1 = m_3 - n_3,$$

  co po przestawieniu wyrazów daje

  $$m_1 + n_3 = n_1 + m_3.$$

  Ta równość z określenia ρ oznacza, że $(m_1, n_1)\ \rho\ (m_3, n_3)$, czyli $x\ \rho\ z$.

Relacja ρ jest relacją równoważności. Wyznaczmy teraz kilka klas abstrakcji naszej relacji ρ:

$$\begin{aligned}
[(1,3)]_\rho &= \{(0,2),(1,3),(2,4),\ldots\} \\
[(1,2)]_\rho &= \{(0,1),(1,2),(2,3),\ldots\} \\
[(2,1)]_\rho &= \{(1,0),(2,1),(3,2),\ldots\}
\end{aligned}$$

Klasie $[(1,3)]_\rho$ możemy przyporządkować liczbę 2, klasie $[(1,2)]_\rho$ liczbę 1, a klasie $[(2,1)]_\rho$ liczbę -1. Ogólnie klasie $[(m,n)]_\rho$ odpowiada wzajemnie jednoznacznie liczba $n - m$, która jest liczbą całkowitą, niekoniecznie naturalną. Inaczej mówiąc, w zbiorze par liczb naturalnych (m,n) wyabstrachowaliśmy cechę przystawania tych par, a mianowicie stałą różnicę zmiennych $n - m$ będącą liczbą całkowitą.

Powyższy przykład to konstrukcja liczb całkowitych na zbiorze liczb naturalnych.

TWIERDZENIE 1.8. *Relacja binarna na zbiorze wyznacza jego podział, wtw., gdy jest ona relacją równoważności.*

2 Funkcje

Niech X, Y będą dowolnymi, niepustymi zbiorami. Mówi się, że relacja binarna $f \subseteq X \times Y$ jest *funkcją*, gdy

(1) dla każdego $x \in X$ istnieje taki $y \in Y$, że $(x, y) \in f$,

(2) dla dowolnych $x \in X$, $y_1, y_2 \in Y$ jeśli $(x, y_1) \in f$ oraz $(x, y_2) \in f$, to musi być $y_1 = y_2$.

Druga własność funkcji oznacza, że element $x \in X$ jednoznacznie wyznacza element $y \in Y$, który jest z nim w relacji f. Pozwala to dla funkcji f pisać $f(x)$ zamiast y, czyli $f(x) = y$, zamiast $(x, y) \in f$.

PRZYKŁAD 2.1. Niech $X = \{1, 2, 3\}$, $Y = \{a, b, c, d\}$, $\rho_1, \rho_2 \subseteq X \times Y$ oraz

$$\rho_1 = \{(1, a), (2, b), (1, d)\}, \qquad \rho_2 = \{(1, a), (2, b), (3, d)\}.$$

Relacja ρ_1 nie jest funkcją, bo dla $3 \in X$ nie ma $y \in Y$ takiego, aby $(3, y) \in \rho_1$. Poza tym, 1 jest w relacji z a oraz z d. Relacja ρ_2 jest funkcją.

Zamiast pisać, że $f \subseteq X \times Y$ dla funkcji piszemy $f \colon X \to Y$ i mówimy, że f odwzorowuje zbiór X w zbiór Y.

Funkcja f jest *iniekcją* (jest *różnowartościowa*), gdy dla dowolnych $x_1, x_2 \in X$ jeśli $f(x_1) = f(x_2)$, to musi być $x_1 = x_2$.

PRZYKŁAD 2.2. Rozważmy funkcję $f \colon \mathbb{R} \to \mathbb{R}$, daną wzorem $f(x) = x+2$. Sprawdzimy, czy jest ona różnowartościowa. Niech $x_1, x_2 \in \mathbb{R}$. Załóżmy, że $f(x_1) = f(x_2)$. Po podstawieniu do wzoru mamy $x_1 + 2 = x_2 + 2$, co jest prawdą tylko gdy $x_1 = x_2$. To oznacza, że funkcja f jest różnowartościowa.

PRZYKŁAD 2.3. Funkcja $f \colon \mathbb{R} \to \mathbb{R}$, dana wzorem $f(x) = x^2$ nie jest różnowartościowa bo dla $x_1 = -1$ i $x_2 = 1$ mamy $f(x_1) = 1 = f(x_2)$.

Funkcja f jest *surjekcją* (jest *na*), gdy dla dowolnego $y \in Y$ istnieje taki $x \in X$, że $f(x) = y$.

PRZYKŁAD 2.4. Funkcja $f \colon \mathbb{R} \to \mathbb{R}$, dana wzorem $f(x) = x^2$ nie jest na (nie jest surjekcją) bo dla $y = -1$ nie ma takiego $x \in \mathbb{R}$ aby $f(x) = x^2 = -1$. Funkcja g dana tym samym wzorem $g(x) = x^2$, ale określona na innym zbiorze $g \colon \mathbb{R} \to (0, \infty)$ jest surjekcją bo dla każdej nieujemnej liczby rzeczywistej y możemy wziąć pierwiastek i równanie $y = x^2$ ma zawsze przynajmniej jedno rozwiązanie: $x = \sqrt{y}$.

Zuważmy, że w powyższym przykładzie, gdy zmienimy przeciwdziedzinę funkcji f na zbiór liczb rzeczywistych nieujemnych, to znaczy weźmiemy funkcję $g \colon \mathbb{R} \to [0, \infty)$ określoną tym samym wzorem $g(x) = x^2$, wówczas funkcja g jest surjekcją. Mimo, że obie funkcje mają ten sam wzór i tę samą dziedzinę, to nie są one równe, bo mają różne przeciwdziedziny.

Funkcja, która jest jednocześnie iniekcją i surjekcją to *bijekcja*. Przykładem bijekcji jest funkcja z przykładu 2.2. Wystarczy bowiem zauważyć, że jest ona surjekcją, gdyż dla dowolnego $y \in \mathbb{R}$ bierzemy $x = y - 2$ i sprawdzamy, że

$$f(x) = x + 2 = y - 2 + 2 = y.$$

3 Równoliczność zbiorów

Niech X i Y będą dowolnymi zbiorami. Gdy możemy policzyć ile jest elementów w obu zbiorach to tym samym jesteśmy w stanie stwierdzić, czy są one *równoliczne.* Ilość elementów w zbiorze X oznaczamy przez $|X|$. Zatem X i Y są równoliczne, gdy $|X| = |Y|$. Problem pojawia się, gdy w obu zbiorach znajduje się nieskończenie wiele elementów. Wówczas twierdzimy, że zbiory X i Y są równoliczne, gdy istnieje bijekcja $f\colon X \to Y$.

Przykład 3.1. Zbiór $X = \mathbb{N}$ wszystkich liczb naturalnych oraz zbiór $Y = \{n \in \mathbb{N}\colon n = 2k \text{ dla pewnego } k \in \mathbb{N}\}$ parzystych liczb naturalnych są równoliczne bo odwzorowanie dane wzorem $f(x) = 2x$ jest bijekcją z X na Y.

Przykład 3.2. Zbiór $X = \mathbb{N}$ wszystkich liczb naturalnych oraz zbiór $Y = \mathbb{Z}$ wszystkich liczb całkowitych są równoliczne bo odwzorowanie dane wzorem

$$f(x) = \begin{cases} \frac{x}{2}, & \text{gdy } x \text{ jest parzysta,} \\ -\frac{x+1}{2}, & \text{gdy } x \text{ jest nieparzysta.} \end{cases}$$

jest bijekcją z X na Y.

Zbiór skończony lub równoliczny ze zbiorem $\mathbb{N}$ nazywamy *przeliczalnym.* Przykładem zbioru przeliczalnego jest zbiór wszystkich liczb całkowitych jak to zostało pokazane w 3.1, zbiór wszystkich liczb parzystych $\{2k\colon k \in \mathbb{N}\}$ lub zbiór dzielników liczby 24 czyli $\{1, 2, 3, 4, 6, 8, 12\}$.

4 Indukcja matematyczna

4.1 Zasada minimum

Twierdzenie 4.1. *W każdym niepustym podzbiorze zbioru liczb naturalnych jest element najmniejszy.*

Przykład 4.2. Sprawdzimy, że suma początkowych n liczb nieparzystych wynosi

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2. \tag{1}$$

Dla kilku początkowych wartości n łatwo ten wzór sprawdzić:

$$\begin{aligned} n &= 1 & 1 &= 1^2, \\ n &= 2 & 1 + 3 = 4 &= 2^2, \\ n &= 3 & 1 + 3 + 5 = 9 &= 3^2, \\ n &= 4 & 1 + 3 + 5 + 7 = 16 &= 4^2. \end{aligned}$$

Nie jest to jednak dowód. Przypuśćmy, że podany wzór nie jest prawdziwy. Rozważmy zbiór

$$S = \{n \in \mathbb{N}\colon 1 + 3 + 5 + \cdots + (2n - 1) \neq n^2\}$$

wszystkich liczb dla, których wzór (1) nie zachodzi. Jest to podzbiór $\mathbb{N}$, a więc korzystając z zasady minimum musi w nim być element najmniejszy, nazwijmy go k. Nie może on być równy 0, 1, 2, 3, 4, bo dla tych wartości sprawdziliśmy, że wzór (1) jest prawdziwy. Tak, czy inaczej dla $k-1$ wzór (1) jest prawdziwy, bo $k-1 \notin S$ jako, że k jest w S elementem najmniejszym. Zatem

$$1+3+5+\cdots+(2(k-1)-1) = 1+3+5+\cdots+(2k-3) = (k-1)^2.$$

Dodajmy do obu stron kolejną liczbę nieparzystą, czyli $2k-1$. Dostaniemy

$$1+3+5+\cdots+(2k-3)+(2k-1) = (k-1)^2+(2k-1) = k^2-2k+1+2k-1 = k^2,$$

ale to oznacza, że dla k nasz wzór (1) jest prawdziwy. Nasze przypuszczenie było więc fałszywe i wzór (1) jest prawdziwy dla wszystkich liczb naturalnych różnych od 0.

4.2 Zasada indukcji

Twierdzenie 4.3. *Niech $S \subseteq \mathbb{N}$, $n \in \mathbb{N}$ spełniają dwa warunki:*

(i) *$n \in S$ oraz*

(ii) *jeśli $k \in S$, to również $k+1 \in S$.*

Wówszas $\{n, n+1, n+2, \ldots\} \subseteq S$.

Przykład 4.4. Wykażemy, że wzór

$$2n+1 < 2^n. \tag{2}$$

jest prawdziwy dla $n \geqslant 3$. Niech

$$S = \{k \in \mathbb{N}\colon 2k+1 < 2^k\}$$

będzie zbiorem wszystkich takich liczb naturalnych, dla których zachodzi wzór (2). Zauważmy, że $n = 3 \in S$ bo

$$2 \cdot 3 + 1 = 7 < 8 = 2^3.$$

Załóżmy teraz, że $k \in S$. Sprawdzimy, czy $k+1 \in S$. Mamy

$$2(k+1)+1 = 2k+1+2 < 2^k+2 \leqslant 2^k+2^k = 2 \cdot 2^k = 2^{k+1}.$$

Zatem $k+1 \in S$. Na mocy zasady indukcji $S = \{3, 4, 5, \ldots\}$, co kończy dowód.

Przykład 4.5. Zbadamy dla jakich $n \in \mathbb{N}$ zachodzi wzór

$$n^2 < 2^n. \tag{3}$$

Dla małych n mamy

n	n^2		2^n
0	$0 = 0^2$	$<$	$2^0 = 1$
1	$1 = 1^2$	$<$	$2^1 = 2$
2	$4 = 2^2$	$\not<$	$2^2 = 4$
3	$9 = 3^2$	$\not<$	$2^3 = 8$
4	$16 = 4^2$	$\not<$	$2^4 = 16$
5	$25 = 5^2$	$<$	$2^5 = 32$
6	$36 = 6^2$	$<$	$2^6 = 64$

Udowodnimy, że wzór (3) jest prawdziwy dla wszystkich $n \geqslant 6$. Zakładamy, że dla k wzór ten zachodzi. Sprawdzimy, czy zachodzi również dla $k+1$. Korzystając z znaszego założenia i z przykładu 4.4 mamy

$$(k+1)^2 = k^2 + 2k + 1 < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1},$$

co oznacza, że wzór (3) jest prawdziwy dla $k+1$.

4.3 Zasada indukcji zupełnej

Twierdzenie 4.6. *Niech $S \subseteq \mathbb{N}$, $n \in \mathbb{N}$ spełniają warunek:*

(i) *jeśli $\{n, n+1, n+2, \ldots, k\} \subseteq S$, to $k+1 \in S$.*

Wówszas $\{n, n+1, n+2, \ldots\} \subseteq S$.

Przykład 4.7. Mamy prostokątną czekoladę złożoną z $n = ab$, gdzie $0 < a, b$, kwadratowych kawałków. Przez ułamanie rozumiemy rozcięcie wzdłóż linii pomiędzy kawałkami, tak aby dostać dwa prostokątne kawałki. Ile razy trzeba ułamać czekoladę aby rozdzielić jej wszystkie kawałki?

Stosując zasadę indukcji zupełnej pokażemy, że trzeba wykonać $n-1$ ułamań.

Najmniejsze możliwe a i b to $a = b = 1$. Zatem najmniejsza czekolada składa się z $n = ab = 1$ kawałków i do jej podzielenia wystarczy $n - 1 = 0$ ułamań.

Zgodnie z zasadą indukcji zupełnej rozważmy zbiór

$$S := \{n \in \mathbb{N} \colon \text{dla prostokątnej czekolady o } n \text{ kawałkach potrzeba } n-1 \text{ ułamań}\}$$

i załóżmy, że $\{0, 1, 2, \ldots, k\} \subseteq S$. Pokażemy, że $k+1 \in S$. Gdy czekolada ma $k+1$ kawałków, to pierwsze ułamanie podzieli ją na dwa prostokąty złożone z odpowiednio k_1 i k_2 kawałków, przy czym $k_1 + k_2 = k+1$ oraz $1 \leqslant k_1, k_2$. Zauważmy, że $k_1, k_2 \in S$, to znaczy, że aby połamać te mniejsze kawałki potrzeba odpowiednio $k_1 - 1$ oraz $k_2 - 1$ ułamań. W sumie, od początku, wykonaliśmy więc

$$1 + k_1 - 1 + k_2 - 1 = (k+1) - 1$$

ułamań, co kończy dowód.

4.4 Zasada maksimum

Twierdzenie 4.8. *W każdym niepustym i ograniczonym z góry podzbiorze zbioru liczb naturalnych jest element największy.*

5 Rekurencja

Ciąg liczbowy o wartościach rzeczywistych to funkcja $a : \mathbb{N} \to \mathbb{R}$. Ciąg liczbowy możemy określić na kilka sposobów:

- poprzez podanie wszystkich jego wyrazów, np. $1, 0, 1, 0, 1, \ldots$,
- poprzez podanie jawnego wzoru w postaci jawnej, np. $a_n = n^2$,
- poprzez podanie przepisu jak tworzyć kolejne wyrazy wykorzystując wyrazy już znane, czyli *rekurencyjnie*.

Mówimy, że ciąg liczbowy a_n, $n \in \mathbb{N}$ jest zadany *rekurencyjnie*, gdy

- dane są jego początkowe wyrazy $a_0, a_1, \ldots, a_k$, gdzie $k \geqslant 0$, oraz
- dana jest reguła pozwalająca wyznaczyć wyraz a_{n+1} w zależności od wyrazów $a_0, a_1, \ldots, a_n$, dla $n \geqslant k$.

Typowymi przykładami cięgów rekurencyjnych są ciągi arytemtyczne i geometryczne.

5.1 Ciąg arytmetyczny

Niech a_0 i r będą dowolnymi, ustalonymi liczbami rzeczywistymi. Reguła rekurencyjna

$$a_{n+1} = a_n + r$$

definiuje *ciąg arytmetyczny* o początkowym wyrazie a_0 i różnicy r. Wzór w postaci jawnej tego ciągu wygląda następująco:

$$a_n = a_0 + nr$$

dla dowolnego $n \in \mathbb{N}$.

5.2 Ciąg geometryczny

Niech a_0 i q będą dowolnymi, ustalonymi liczbami rzeczywistymi. Reguła rekurencyjna

$$a_{n+1} = a_n \cdot q$$

definiuje *ciąg geometryczny* o początkowym wyrazie a_0 i ilorazie q. Wzór w postaci jawnej tego ciągu wygląda następująco:

$$a_n = a_0 \cdot q^n$$

dla dowolnego $n \in \mathbb{N}$.

5.3 Silnia

Rozważmy następujący ciąg rekurencyjny:

$$\begin{aligned} a_0 &= 1, \\ a_n &= n \cdot a_{n-1}, \quad \text{dla } n \geqslant 1. \end{aligned}$$

Wartość n-tego wyrazu tego ciągu nazywa się *silnią* liczby n i oznaczana jest przez $n!$. Zatem postać jawna tego ciągu wygląda następująco:

$$a_n = n!.$$

5.4 Ciąg Fibonacciego

Spośród ciągów rekurencyjnych najsłynniejszym jest chyba *ciąg Fibonacciego*:

$$\begin{aligned} a_0 &= 0, \\ a_1 &= 1, \\ a_n &= a_{n-1} + a_{n-2}, \quad \text{dla } n \geqslant 2. \end{aligned}$$

Każdy wyraz tego ciągu, poza dwoma pierwszymi, jest sumą poprzednich dwóch wyrazów. Postać jawna nie jest trywialna, a mianowicie:

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

5.5 Wieże Hanoi

Na jednej z trzech wież znajdują się 64 krążki takie, że krążki umieszczone wyżej mają mniejsze promienie. Zadanie polega na przełożeniu wszystkich tych kążków z pierwszej na trzecią wieżę, ale tak aby:

- w jednym ruchu można przenieść tylko jeden krążek,
- większy krążek nigdy nie może leżeć na mniejszym,
- można posługiwać się trzema wieżami.

Ile czasu zajmmie przełożenie tych krążków jeśli przyjmiemy, że przełożenie jednego zajmuje sekundę?

Przez a_n oznaczmy liczbę ruchów potrzebnych do przeniesienia n krążków z jednej wieży na drugą. Łatwo sprawdzić, że

$$\begin{aligned} a_0 &= 0, \\ a_1 &= 1, \\ a_2 &= 3, \\ a_3 &= 7. \end{aligned}$$

Już przy $n = 3$ widać regułę rekurencyjną. Oznaczmy kolejne wieże przez A, B, C. Aby przenieść n krążków z A na C:

1. przenosimy $n-1$ górnych krążków z A na B posługując się wieżą C, wymaga to a_{n-1} ruchów,
2. przenosimy dolny, największy krążek z A na C, to jest jeden ruch,
3. przenosimy $n-1$ krążków z B na C posługując się wieżą A, wymaga to a_{n-1} ruchów.

Ostatecznie mamy

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

i w postaci jawnej

$$a_n = 2^n - 1.$$

Możemy teraz odpowiedzieć na zadane na początku pytanie. Przeniesienie n krążków zajmie ponad 3 000 000 000 000 lat. Komputer z procesorem 3GHz wykonywał by to zadanie ponad 1000 lat.

6 Metody zliczania zbiorów i funkcji

Licząc samochody na parkingu, komputery w pracowni, albo studentów na wykładzie, zliczanym elementom „przyczepiamy” etykietki z kolejnymi liczbami naturalnymi zaczynając od 1. Gdy wyczerpiemy liczone elementy to ostatnia z przyczepionych etykiet mówi ile w zbiorze jest elementów. Ta procedura to nic innego jak konstrukcja bijekcji f z zadanego zbioru X na podzbiór $\{1, 2, \ldots, n\}$ zbioru $\mathbb{N}$.

Tak więc podstawy formalne do zagadnienia zliczania zbiorów i funkcji już mamy. Zostały one wprowadzone w podrozdziale 3 jako równoliczność zbiorów. Aby policzyć ile dany zbiór X zawiera elementów należy wskazać bijekcję f z X na zbiór, którego ilość elementów znamy.

6.1 Zasada mnożenia

Twierdzenie 6.1 (Zasada mnożenia)**.** *Dla dowolnych zbiorów skończonych A_1, $A_2, \ldots, A_n$ mamy*

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|.$$

Przykład 6.2. W turnieju szachowym biorą udział dwie drużyny: czerwonych i niebieskich. Drużyna czerwonych liczy 5 zawodników, natomiast drużyna niebieskich 7 zawodników. Ile różnych indywidualnych pojedynków może być stoczonych, jeśli zawodnicy jednej drużyny nigdy ze sobą nie walczą?

Niech C i N będą zbiorami odpowiednio czerwonych i niebieskich. Każdy pojedynek może być interpretowany jako uporządkowana para (c, n), gdzie $c \in C$, $n \in N$. Zatem liczba pojedynków to liczność zbioru $C \times N$. Z zasady mnożenia 6.1 mamy

$$|C \times N| = |C| \cdot |N| = 5 \cdot 7 = 35.$$

6.2 Zasada dodawania

Twierdzenie 6.3 (Zasada dodawania)**.** *Dla dowolnych parami rozłącznych zbiorów skończonych* $A_1, A_2, \ldots, A_n$ *mamy*

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Dowód. Dla $n = 1$ dowód jest trywialny. Dla $n = 2$ załóżmy, że $|A_1| = p$ i $|A_2| = q$. Elementy A_1 możemy ponumerować $1, 2, \ldots, p$, natomiast elementy A_2 ponumerujemy $p+1, p+2, \ldots, p+q$. Ponieważ $A_1 \cap A_2 = \emptyset$, więc w A_1 nie ma elementów z A_2 i żaden element nie był numerowany dwukrotnie. Tak więc

$$|A_1 \cup A_2| = p + q = |A_1| + |A_2|.$$

Załóżmy teraz indukcyjnie dla $n = k$, że

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.$$

Dla $n = k + 1$ mamy

$$|A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1}| = |(A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}| = \\ |A_1 \cup A_2 \cup \cdots \cup A_k| + |A_{k+1}| = |A_1| + |A_2| + \cdots + |A_k| + |A_{k+1}|$$

ponieważ w A_{k+1} nie ma żadnego elementu ze zbiorów $A_1, A_2, \ldots, A_k$, to znaczy $(A_1 \cup A_2 \cup \cdots \cup A_k) \cap A_{k+1} = \emptyset$ i postępujemy jak dla dwóch zbiorów. □

Przykład 6.4. Powiedzmy, że mamy 5 czerwonych guzików i 7 niebieskich. Zbiór A czerwonych guzików jest rozłączny ze zbiorem B niebieskich guzików. Zatem z zasady dodawania 6.3, aby policzyć ile jest w sumie guzików, czyli w zbiorze $A \cup B$, dodajemy $|A| + |B| = 5 + 7 = 12$.

6.3 Metoda włączania-wyłączania

Twierdzenie 6.5 (Metoda włączania-wyłączania dla dwóch zbiorów)**.** *Dla dowolnych zbiorów skończonych* A, B *mamy*

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

Dowód. Zliczając elemety zbioru $A \cup B$ dwukrotnie liczymy te elementy, które występują jednocześnie w A i w B, czyli w $A \cap B$. Tak więc od sumy $|A| + |B|$ musimy odjąć ilość elementów w przekroju $A \cap B$. □

Inny dowód można przeprowadzić w oparciu o zasadę dodawania 6.3, gdy zauważymy, że po pierwsze, zbiory $A \setminus B$, $A \cap B$ oraz $B \setminus A$ są parami rozłączne i w sumie dają $A \cup B$, po drugie, $|(A \setminus B) \cup (A \cap B)| = |A|$ i $|(B \setminus A) \cup (A \cap B)| = |B|$. A więc

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

Twierdzenie 6.6 (Metoda włączania-wyłączania dla trzech zbiorów)**.** *Dla dowolnych zbiorów skończonych A, B, C mamy*

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

Dowód. Zliczając elementy zbioru $A \cup B \cup C$ dwukrotnie liczymy elementy, które są dokładnie w dwu z trzech zbiorów, czyli w $A \cap B$, w $B \cap C$ lub w $C \cap A$. Elementy z przekroju $A \cap B \cap C$ najpierw liczymy trzykrotnie, potem trzy razy je usuwamy z $A \cap B$, z $B \cap C$ i z $C \cap A$, tak więc musimy je z powrotem uzupełnić dodając ilość elementów w $A \cap B \cap C$. □

Przykład 6.7. W pewnym klubie trenuje 13 osób grających w tenisa, 16 osób grających w siatkówkę i 14 osób grających w koszykówkę. Sposród z nich 4 grają w tenisa i siatkówkę, 6 osób gra w tenisa i koszykówkę, 3 grają w siatkówkę i koszykówkę, a tylko dwie osoby grają we wszystkie trzy gry. Ile osób jest w tym klubie?

Niech

$$\begin{aligned} T &- \text{zbiór osób grających w tenisa,} \\ S &- \text{zbiór osób grających w siatkówkę,} \\ K &- \text{zbiór osób grających w koszykówkę.} \end{aligned}$$

Zatem $|T| = 13$, $|S| = 16$, $|K| = 14$, $|T \cap P| = 4$, $|T \cap B| = 6$, $|P \cap B| = 3$, $|T \cap P \cap B| = 2$ i na mocy 6.6 mamy

$$|T \cup S \cup K| = 13 + 16 + 14 - 4 - 6 - 3 + 2 = 32.$$

6.4 Zasada szufladkowa Dirichleta

Twierdzenie 6.8 (Zasada szufladkowa Dirichleta)**.** *Jeśli n obiektów jest rozmieszczonych w m szufladach i $n > m$, to istnieje szuflada z przynajmniej dwoma obiektami.*

Bardziej formalnie można powiedzieć, że nie istnieje bijekcja ze zbioru o n elementach na zbiór m-elementowy, gdy $n > m$.

Przykład 6.9. W grupie 13 osób muszą być co najmniej dwie osoby, które urodziły się w tym samym miesiącu.

Weźmy bowiem 12 szufladek z nazwami miesięcy i „wkładajmy” do nich osoby, które urodziły się w danym miesiącu. Ponieważ osób jest 13, a szufladek 12, to w jednej z nich muszą być co najmniej dwie osoby.

Przykład 6.10. Pewna grupa osób wita się podając sobie ręce. Nikt nie wita się z samym sobą i żadna para osób nie wita się podwójnie. Czy muszą być dwie osoby, które witały taką samą liczbę osób?

Gdy jest n osób, to każda z nich przywita 0 lub 1 lub 2 lub … $n-1$ osób. Utwórzmy więc n szuflad z etykietami $0, 1, 2, \ldots, n-1$. W szufladzie z etykietą k umieszczamy osobę, która witała się z dokładnie k innymi osobami. Skoro jest n osób i n szuflad, to z zasadzy szufladkowej niewiele wynika. Przyjrzyjmy się jednak, czy możliwe jest, aby we wszystkich szufladach było po dokładnie jednej osobie. Wówczas zajęte byłyby szuflady pierwsza z etykietą 0 i ostatnia z etykietą $n-1$. Nie jest to możliwe, bo nie może być osoby, która przywitała wszystkie pozostałe i równocześnie takiej, która nie przywitała nikogo. Zatem pierwsza lub ostatnia musi być pusta. W takim razie n osób zajęło co najwyżej $n-1$ szuflad, więc w jednej z nich są co najmniej dwie osoby — takie, które przywitały tę samą liczbę osób.

Powyższy przykład można sformułować bardziej formalnie w języku teorii grafów. Otóż w grafie skończonym o n wierzchołkach bez pętli istnieją co najmniej dwa wierzchołki tego samego stopnia.

Przykład 6.11. Wybierzmy 10 różnych liczb naturalnych $a_1, a_2, \ldots, a_{10}$ spośród $0, 1, 2, \ldots, 100$. Pokażemy, że w zbiorze $\{a_1, a_2, \ldots, a_{10}\}$ można wybrać dwa rozłączne podzbiory, dające tę samą sumę.

Szuflady poetykietujmy liczbami reprezentującymi możliwe sumy liczb w co najwyżej 10-cio elementowych podzbiorach zbioru $\{0, 1, 2, \ldots, 100\}$. Ponieważ największa możliwa taka suma to $91+92+93+\cdots+99+100 = 955$, więc mamy 955 szuflad z etykietami: $0, 1, 2, \ldots, 955$. Zrugiej strony 10-cio elementowy zbiór $\{a_1, a_2, \ldots, a_{10}\}$ ma $2^{10} = 1024$ podzbiory, więc muszą być dwa podzbiory zbioru $\{a_1, a_2, \ldots, a_{10}\}$ o tej samej sumie.

Te dwa podzbiory nie muszą być rozłączne. Jeśli jednak z obu z nich usuniemy wspólne liczby, to pozostałe dalej będą dawać takie same sumy, a powstałe zbiory będą już rozłączne.

6.5 Zliczanie funkcji

Niech X i Y będą dowolnymi zbiorami takimi, że $|X| = n > 0$ oraz $|Y| = m > 0$. Rozważmy dowolną funkcję $f\colon X \to Y$. Ile jest takich funkcji? Aby odpowiedzieć na to pytanie musimy przypomnieć, że funkcja każdemu $x \in X$ przyporządkowuje dokładnie jeden $y \in Y$. Dla ustalonego x możliwych przyporządkowań elementu y jest tyle, na ile sposobów możemy wybrać y z Y, czyli dokładnie m. Z zasady mnożenia 6.1 wynika, że wszystkich funkcji jest

$$\underbrace{m \cdot m \cdot \cdots \cdot m}_{n \text{ razy}} = m^n. \tag{4}$$

Przykład 6.12. Kod PIN złożony jest z 4 cyfr dziesiętnych. Ile jest różnych takich PIN-kodów?

Wybór każdego PIN-kodu to funkcja ze zbioru $X = \{1, 2, 3, 4\}$ pozycji cyfr w PIN-kodzie w dziesięcioelementowy zbiór cyfr dziesiętnych $Y = \{0, 1, \ldots, 9\}$. Z (4) mamy zatem $10^4 = 10000$ różnych czterocyfrowych PIN-kodów.

Załóżmy teraz dodatkowo, że $n \leqslant m$. Pytamy ile jest funkcji różnowartościowych $f\colon X \to Y$? Zliczając takie funkcje musimy przypomnieć, że iniekcja różnym argumentom, czyli elementom z X, przyporządkowuje różne wartości, czyli elementy z Y. To znaczy, że jeśli jakiemuś $x_1 \in X$ przyporządkowaliśmy pewien $y_1 \in Y$, to kolejnemu $x_2 \neq x_1$ nie możemy już przyporządkować y_1. Tak więc ilość możliwości wyboru $y \in Y$ dla $x \in X$ zmniejsza się o 1 z każdym przyporządkowaniem y do x.

Zgodnie z zasadą mnożenia 6.1 funkcji różnowartościowych jest

$$m(m-1)(m-2)\ldots(m-n+1) = \frac{m!}{(m-n)!}. \tag{5}$$

PRZYKŁAD 6.13. Ile jest czterocyfrowych PIN-kodów, w których cyfry nie powtarzają się?

Zbiory X i Y są jak w 6.12, zatem z uwagi na (5) mamy $10 \cdot 9 \cdot 8 \cdot 7 = 5040$ takich PIN-kodów.

6.6 Zliczanie podzbiorów

Niech X będzie dowolnym zbiorem o n elementach. Policzmy ile jest wszystkich podzbiorów w X. W tym celu przez A oznaczmy dowolny podzbiór X. Rozważmy funkcję $f\colon X \to \{0,1\}$ daną następującym wzorem

$$f(x) = \begin{cases} 0, & \text{gdy } x \notin A, \\ 1, & \text{gdy } x \in A. \end{cases}$$

Taką funkcję f nazywamy *funkcją charakterystyczną* zbioru A.

Zauważmy, że ustalony podzbiór A wyznacza jednoznacznie funkcję f i na odwrót, gdy mamy taką funkcję to $A = \{x \in X\colon f(x) = 1\}$. Zatem podzbiory X wzajemnie jednoznacznie odpowiadają funkcjom charakterystycznym. Aby więc policzyć podzbiory wystarczy policzyć funkcje charakterystyczne zbioru A a to już umiemy – patrz podpunkt 6.5. Tak więc wszystkich podzbiorów w zbiorze n elementowym jest dokładnie 2^n.

Wyznaczeniem ilości k-elementowych podzbiorów w zbiorze n-elementowym zajmiemy się później.

7 Permutacje

Permutacja zbioru skończonego X to bijekcja z X na X.

Niech $\mathbb{Z}_n$ oznacza zbiór reszt przy dzieleniu przez liczbę n, to znaczy

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n\}.$$

Zbiór permutacji zbioru $\mathbb{Z}_n$ oznaczamy przez S_n. Zbiór n-elementowy ma dokładnie $n!$ permutacji,

$$|S_n| = n!.$$

PRZYKŁAD 7.1. Rozważmy funkcję $\pi\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ zadaną poniższą tabelą:

n	0	1	2	3	4	5	6
$\pi(n)$	2	3	6	0	4	1	5

Funkcja π jest bijekcją z $\mathbb{Z}_7$ w $\mathbb{Z}_7$, zatem jest permutacją i $\pi \in S_7$.

7.1 Cykle

Cykl zbioru n-elementowego X to taka permutacja α zbioru X, dla której

$$\{x, \alpha(x), \alpha^2(x), \ldots, \alpha^{n-1}(x)\} = X,$$

dla dowolnego $x \in X$. Łatwo zauważyć, że jeśli dla pewnego $x_0 \in X$ mamy $\{x_0, \alpha(x_0), \alpha^2(x_0), \ldots, \alpha^{n-1}(x_0)\} = X$, to jest tak dla wszystkich $x \in X$, czyli α jest cyklem na X. Cykl α zbioru X zapisujemy jako

$$(x, \alpha(x), \ldots, \alpha^{n-1}(x))$$

dla dowolnie wybranego $x \in X$.

PRZYKŁAD 7.2. Rozważmy permutację $\alpha \in S_6$ daną przez tabelę:

n	0	1	2	3	4	5
$\alpha(n)$	3	5	0	1	2	4

Zauważmy, że dla $x_0 = 0$ mamy

$$\{0, \alpha(0) = 3, \alpha^2(0) = 1, \alpha^3(0) = 5, \alpha^4(0) = 4, \alpha^5(0) = 2\} = \mathbb{Z}_6$$

zatem $\alpha = (0, 3, 1, 5, 4, 2)$ jest cyklem.

Dowolną permutację π zbioru X można rozłożyć na rozłączne cykle w sposób następujący:

1. wybieramy dowolny element $x \in X$, który nie jest jeszcze w żadnym cyklu,
2. iterujemy permutację π otrzymując kolejno: $x, \pi(x), \pi^2(x), \pi^3(x), \ldots$ aż do uzyskania $\pi^j(x) = x$,
3. dodajemy do rozkładu cykl $(x, \pi(x), \ldots, \pi^{j-1}(x))$,
4. jeśli w zbiorze X pozostały jeszcze elementy niepokryte przez żaden cykl, to wracamy do pierwszego punktu naszej procedury.

Jeśli permutacja π złożona jest z k rozłącznych cykli, to zapisujemy ją $\pi = (x_0, \ldots)(x_1, \ldots)\ldots(x_{k-1}, \ldots)$, gdzie w kolejnych nawiasach są elementy kolejnych cykli zaczynających się od odpowiednio: $x_0, x_1, \ldots, x_{k-1}$.

PRZYKŁAD 7.3. Rozważmy jeszcze permutację $\pi \in S_9$:

n	0	1	2	3	4	5	6	7	8
$\pi(n)$	2	3	6	0	4	1	5	8	7

Rozkład π na cykle:

- pierwszy cykl: $0, \pi(0) = 2, \pi(2) = 6, \pi(6) = 5, \pi(5) = 1, \pi(1) = 3, \pi(3) = 0$,
- drugi cykl: $4, \pi(4) = 4$,
- trzeci cykl: $7, \pi(7) = 8, \pi(8) = 7$,

Ostatecznie $\pi = (0, 2, 6, 5, 1, 3)(4)(7, 8)$.

TWIERDZENIE 7.4. *Rozkład permutacji na cykle jest jednoznaczny z dokładnością do kolejności.*

Typ permutacji $\pi \in S_n$ to wektor $(c_1, c_2, \dots, c_n)$, gdzie c_i jest liczbą cykli długości i w rozkładzie π. Zazwyczaj typ permutacji zapisujemy jako

$$[1^{c_1} 2^{c_2} \dots n^{c_n}],$$

przy czym często pomijamy te wartości, dla których $c_i = 0$.

Permutacja z przykładu 7.3 ma jeden cykl długości 1, jeden cykl długości 2 oraz jeden cykl długości 6, a więc jej typ to $[1^1, 2^1, 6^1]$.

7.2 Transpozycje

Transpozycja to permutacja zbioru n-elementowego X (dla $n \leqslant 2$) typu $[1^{n-2} 2^1]$. Innymi słowy, transpozycja dokonuje tylko jednego przestawienia dwóch elementów ze zbioru X.

PRZYKŁAD 7.5. Dla permutacji $\pi \in S_7$ takiej, że:

n	0	1	2	3	4	5	6
$\pi(n)$	0	1	5	3	4	2	6

mamy $\pi = (0)(1)(2, 5)(3)(4)(6) = (2, 5)$, a więc π ma typ $[1^5 2^1]$, co oznacza, że π jest transpozycją.

TWIERDZENIE 7.6. *Dowolny cykl z* S_n *jest złożeniem* $n - 1$ *transpozycji.*

Ponieważ, na mocy 7.4 dowolna permutacja jest rozkładalna na cykle, zatem z powyższego twierdzenia wynika, że każda permutacja jest złożeniem transpozycji. W szczególności każda permutacja typu $[1^{c_1} 2^{c_2} \dots n^{c_n}]$, ma rozkład na co najwyżej $c_2 + 2c_3 + \cdots + (n-1)c_n$ transpozycji.

Permutacja jest *parzysta*, gdy jest złożeniem parzystej liczby transpozycji, natomiast permutacja jest *nieparzysta*, gdy jest złożeniem nieparzystej liczby transpozycji. Znak permutacji π to

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

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

8 Współczynniki dwumianowe

Wiemy już, że zbiór n-elementowy X ma dokładnie 2^n podzbiorów, tyle ile jest funkcji charakterystycznych podzbiorów. Teraz zajmiemy się pytaniem ile taki zbiór ma podzbiorów o dokładnie k elementach. Rodzinę wszystkich k-elementowych podzbiorów zbioru X będziemy oznaczać przez $\mathcal{P}_k(X)$.

Współczynnik dwumianowy $\binom{n}{k}$ to ilość k-elementowych podzbiorów zbioru n-elementowego, czyli

$$\binom{n}{k} = |\mathcal{P}_k(\mathbb{Z}_n)|.$$

Twierdzenie 8.1. *Dla dowolnych* $0 \leqslant k \leqslant n$

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

Dowód. Ustalmy pewien n-elementowy zbiór X, i wybierajmy po kolei k różnych jego elementów, tzn. utwórzmy iniekcję $\mathbb{Z}_k \to X$. Wiemy, że takich iniekcji jest

$$n(n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}.$$

W wyniku takiego wyboru, dostajemy wszakże pewien uporządkowany ciąg k elementów zbioru X. Wiele takich ciągów wyznacza ten sam k-elementowy podzbiór zbioru X. Ciągi takie różnią się jedynie kolejnością elementów, a zatem jest ich tyle ile permutacji zbioru k-elemetowego, czyli $k!$. Zatem jest dokładnie

$$\frac{n(n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{(n-k)!k!}$$

podzbiorów k-elementowych zbioru n-elementowego. □

To samo twierdzenie można dowieść indukcyjnie.

Twierdzenie 8.2. *Dla* $n, k \in \mathbb{N}$ *zachodzi:*

(i) $\binom{n}{0} = \binom{n}{n} = 1$,

(ii) $\binom{n}{k} = 0$, *dla* $k > n$,

(iii) $\binom{n}{1} = n$, *dla* $n > 0$,

(iv) $\binom{n}{k} = \binom{n}{n-k}$, *dla* $n \geqslant k \geqslant 0$.

Dowód. (i) Natychmiastowa konsekwencją faktu, że dowolny zbiór n-elementowy X ma tylko jeden 0-elementowy podzbiór, a mianowicie podzbiór pusty $\emptyset$ i tylko jeden podzbiór n-elementowy, to znaczy cały zbiór X.

(ii) Zbiór n-elementowy nie może mieć podzbiorów o $k > n$ elementach.

(iii) Podzbiorów jednoelementowych jest dokładnie tyle ile elementów w zbiorze.

(iv) Załóżmy, że $n \geqslant k \geqslant 0$. Wówczas k-elementowych podzbiorów A w n-elementowym zbiorze X jest tyle samo co ich $(n-k)$-elementowych dopełnień $X \setminus A$. Innymi słowy funkcja

$$\mathcal{P}_k(X) \ni A \to X \setminus A \in \mathcal{P}_{n-k}(X)$$

jest bijekcją, a więc $\left|\mathcal{P}_k(X)\right| = \left|\mathcal{P}_{n-k}(X)\right|$. □

Twierdzenie 8.3. *Dla $0 < k \leqslant n$ mamy:*

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

Dowód. Załóżmy, że $|X| = n$. Po usunięciu ze zbioru X elementu $a \in X$ dostajemy $(n-1)$-elementowy zbiór X'. Niech $A \in \mathcal{P}_k(X)$. Mamy dwie możliwości

1. $a \in A$,
2. $a \notin A$.

W drugim przypadku zbiór A to k-elementowy podzbiór $(n-1)$-elementowego zbioru X', czyli $A \in \mathcal{P}_k(X')$.

W pierwszym przypadku podzbiór A jest jednoznacznie wyznaczony przez swoje pozostałe $k-1$ elementów. To znaczy $A = A' \cup \{a\}$, gdzie $A' \in \mathcal{P}_{k-1}(X')$ i podzbiorów A jest tyle samo co podzbiorów A'. A zatem

$$\binom{n}{k} = |\mathcal{P}_k(X)| = |\mathcal{P}_k(X')| + |\mathcal{P}_{k-1}(X')| = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

□

8.1 Trójkąt Pascala

Trójkąt Pascala bazuje na własności 8.3 i ustawia liczby w następujący sposób:

- wiersze numerowane są kolejnymi liczbami naturalnymi, $n = 0, 1, 2, \ldots,$
- w każdym wierszu występuje dokładnie $n+1$ liczb, kolejno:

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}, \binom{n}{n}$$

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0} & & & & & & \\
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\cdots & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots & & \cdots
\end{array}$$

Przesunięcie w wierszach, pozwala wyliczyć $\binom{n}{k}$ jako sumę $\binom{n-1}{k-1} + \binom{n-1}{k}$ (por. 8.3) dwu liczb stojących bezpośrednio nad $\binom{n}{k}$.

8.2 Dwumiany

Poniższe twierdzenie wyjaśnia pochodzenie nazwy współczynnika dwumianowego.

TWIERDZENIE 8.4. *Dla* $x, y \in \mathbb{R}$ *i* $n \in \mathbb{N}$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Rozwińmy klika początkowych dwumianów zgodnie z tym twierdzeniem:

$$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2,\\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3,\\ (a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.\end{aligned}$$

8.3 Przykłady zastosowań

PRZYKŁAD 8.5. Znajdujemy się w mieście zbudowanym na planie prostopadle przecinających się ulic. Ile jest najkrótszych dróg z A do B, gdy B znajduje się na szóstej przecznicy na wschód i na trzeciej przecznicy na północ od A?

Zauważmy, że każda najkrótsza droga biegnie przez dokładnie 9 skrzyżowań (licząc skrzyżowanie w punkcie A i nie licząc skrzyżowania w punkcie B). Na każdym takim skrzyżowaniu musimy podjąć decyzję, czy pójść na wschód czy na północ, przy czym musimy iść dokładnie 3 razy na północ i dokładnie 6 razy na wschód. Zatem liczba najkrótszych dróg z A do B to liczba wyborów spośród 9 skrzyżowań, trzech, na których pójdziemy na północ, bądź 6 na których pójdziemy na wschód. A zatem liczba ta wynosi $\binom{9}{3} = \binom{9}{6} = 84$.

W ogólności załóżmy, że mamy kratkę $m \times n$ i chcemy narysować najkrótszą łamaną po krawędziach kratki łączącą lewy dolny wierzchołek z prawym górnym. Na ile sposobów możemy narysować taką łamaną?

Widzimy, że musimy narysować $m+n$ odcinków jednostkowych, z których dokładnie m jest pionowych i dokładnie n jest poziomych. Zatem jest

$$\binom{m+n}{m} = \binom{m+n}{n} = \frac{(m+n)!}{m!n!}$$

sposobów połączenia dwóch przeciwległych wierzchołków.

PRZYKŁAD 8.6. Ile rozwiązań ma równanie

$$x_0 + x_1 + x_2 + x_3 + x_4 = 7,$$

gdzie x_i są liczbami naturalnymi?

Użyjmy kratki rozważanej w poprzednim przykładzie do połączenia przeciwległych jej rogów. W kratce rozmiaru 4×7 suma poziomych odcinków daje 7 i jest dokładnie 5 takich odcinków, po jednym na każdym poziomie. Jeśli długości tych odcinków oznaczymy odpowiednio przez x_0, x_1, x_2, x_3, x_4, to każda taka droga (łamana) na kratce ustala pewne rozwiązanie naszego równania, i każde rozwiązanie równania wyznacza dokładnie jedną drogę (łamaną).

Zatem istnieje $\binom{7+4}{4} = 330$ rozwiązań naszego równania.

Przykład 8.7. Rozważmy pokratkowaną kartkę wielkości $n \times n$ i policzmy na ile sposobów można w jej wnętrzu narysować prostokąt tak, aby wszystkie jego boki były równoległe do krawędzi kartki?

Zauważmy, że każdy taki prostokąt jest jednoznacznie wyznaczony przez dwie spośród $n+1$ poziomych linii oraz przez dwie spośród $n+1$ pionowych linii. Rzeczywiście, dowolny prostokąt wyznacza dwie linie poziome i dwie pionowe. I na odwrót dowolny wybór linii pozwoli nam nakreślić jednoznacznie prostokąt na kartce.

Poziome linie możemy wybrać na $\binom{n+1}{2}$ sposobów i pionowe linie także na $\binom{n+1}{2}$ sposobów. Zatem taki prostokąt możemy narysować na dokładnie

$$\binom{n+1}{2}^2 = \left(\frac{n(n+1)}{2}\right)^2.$$

Ilość	Losujemy	Powtórzenia	Kolejność	Nazwa	Wzór
n	n	nie	tak	permutacje bez powtórzeń	$P_n = n!$
n	n	tak	tak	permutacje z powtórzeniami	$P_n^{n_1 \ldots n_k} = \frac{n!}{n_1! \ldots n_k!}$
n	k	nie	tak	wariacje bez powtórzeń	$V_n^k = \frac{n!}{(n-k)!}$
n	k	tak	tak	wariacje z powtórzeniami	$W_n^k = n^k$
n	k	nie	nie	kombinacje bez powtórzeń	$C_n^k = \binom{n}{k} = \frac{n!}{(n-k)!k!}$
n	k	tak	nie	kombinacje z powtórzeniami	$\overline{C_n^k} = \frac{(n+k-1)!}{(n-1)!k!}$

Tabela 1: Wzory na permutacje, wariacje i kombinacje.

9 Elementy teorii liczb

9.1 Podzielność, NWD, NWW

Niech $a, b \in \mathbb{Z}$ i $b > 0$, wtedy istnieją jednoznacznie wyznaczone: iloraz $q \in \mathbb{Z}$ i reszta $r \in \mathbb{N}$ spełniające:

$$a = bq + r \qquad \text{i} \qquad 0 \leqslant r < b.$$

Resztę z dzielenia a przez b zapisujemy jako

$$r = a \bmod b.$$

Mówimy, że b dzieli a (lub a jest podzielne przez b), i piszemy $b \mid a$, jeśli istnieje $q \in \mathbb{Z}$ takie, że $a = bq$. W takim wypadku mówimy też, że b jest dzielnikiem a lub, że a jest wielokrotnością b. Innymi słowy, jeśli b dzieli a to reszta z dzielenia a przez b równa jest 0, innymi słowy $a \bmod b = 0$.

Stwierdzenie 9.1. *Dla dowolnych a, b, c zachodzi:*

(i) *jeśli $a \mid b$ to $a \mid bc$,*

(ii) *jeśli $a \mid b$ i $b \mid c$ to $a \mid c$,*

(iii) *jeśli $a \mid b$ i $a \mid c$ to $a \mid (b+c)$.*

Dowód. (i) Z założenia wiemy, że istnieje $q \in \mathbb{Z}$ takie, że $aq = b$. Mnożąc obie strony równości przez c dostajemy $aqc = bc$. A więc dla $q' = qc \in \mathbb{Z}$ mamy $aq' = bc$, co z kolei oznacza, że $a \mid bc$.

(ii) Z założenia istnieją $p, q \in \mathbb{Z}$ takie, że $aq = b$ i $bp = c$. Łatwo zauważamy, że dla $q' = pq$ mamy $aq' = apq = bp = c$, czyli $a \mid c$.

(iii) Z założenia istnieją p, q takie, że $aq = b$ i $ap = c$. Dodając stronami ostatnie równości otrzymujemy $a(p+q) = b + c$, czyli $a \mid b + c$. □

Największy wspólny dzielnik liczb a i b, zapisywany jako $\mathrm{NWD}(a, b)$, gdzie chociaż jedna z liczb a, b jest różna od 0, to największa liczba d taka, że $d \mid a$ i $d \mid b$. Oczywiście,

$$1 \leqslant \mathrm{NWD}(a, b) \leqslant \min(a, b).$$

Najmniejsza wspólna wielokrotność liczb $a, b > 0$, oznaczana przez $\mathrm{NWW}(a, b)$, to najmniejsza liczba dodatnia w taka, że $a \mid w$ i $b \mid w$. Zauważmy, że

$$\max(a, b) \leqslant \mathrm{NWW}(a, b) \leqslant ab.$$

9.2 Algorytm Euklidesa

Algorytm Euklidesa to algorytm wyznaczania największego wspólnego dzielnika dwu dodatnich liczb całkowitych.

1. Wczytaj liczby $a, b > 0$.
2. Oblicz r jako resztę z dzielenia a przez b.
3. Zastąp a przez b, zaś b przez r.
4. Jeżeli $b = 0$, to zwróć a w przeciwnym wypadku przejdź do punktu 2.

Przykład 9.2. Przebieg obliczenia $\mathrm{NWD}(1029, 1071)$.

$a = 1029$	$b = 1071$	$1029 = 0 \cdot 1071 + 1029$	$r = 1029$
$a = 1071$	$b = 1029$	$1071 = 1 \cdot 1029 + 42$	$r = 42$
$a = 1029$	$b = 42$	$1029 = 24 \cdot 42 + 21$	$r = 21$
$a = 42$	$b = 21$	$42 = 2 \cdot 21 + 0$	$r = 0$
$a = 21$	$b = 0$		

Algorytm zwraca $a = 21$.

9.3 Liczby pierwsze i rozkład na czynniki pierwsze

Każda liczba naturalna $a > 1$ ma przynajmniej dwa dodatnie dzielniki: 1 oraz a. *Liczba pierwsza* to taka liczba naturalna p, która posiada dokładnie dwa różne dzielniki: 1 oraz p. Oto lista wszystkich liczb pierwszych mniejszych od 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Liczba złożona to liczba naturalna a, która nie jest pierwsza, a więc ma jakiś dodatni dzielnik różny od 1 i a. *Liczby względnie pierwsze* to takie liczby a i b, dla których $\mathrm{NWD}(a, b) = 1$.

TWIERDZENIE 9.3. *Liczb pierwszych jest nieskończenie wiele.*

DOWÓD. Załóżmy niewprost za Euklidesem, że liczb pierwszych jest skończenie wiele i są to: $p_1, \ldots, p_k$. Rozważmy liczbę

$$n = p_1 p_2 \ldots p_k + 1.$$

Jest ona oczywiście większa od każdej liczby p_i. Ponadto żadna z liczb pierwszych p_i nie dzieli n, bo przy dzieleniu przez p_i daje resztę 1. A zatem n, albo jest nową liczbą pierwszą, albo w rozkładzie n są nowe liczby pierwsze. Sprzeczność. □

STWIERDZENIE 9.4 (Lemat Euklidesa)**.** *Jeśli $n \mid ab$ i $\mathrm{NWD}(n, a) = 1$, to $n \mid b$.*

DOWÓD. Ponieważ $\mathrm{NWD}(a, n) = 1$, to istnieją x, y takie, że $xa + yn = 1$. Mnożąc obie strony równości przez b otrzymujemy:

$$xab + ynb = b.$$

Z założenia wiemy, że n dzieli lewą stronę powyższej równości. Musi zatem dzielić też prawą. □

TWIERDZENIE 9.5 (Fundamentalne Twierdzenie Arytmetyki)**.** *Każda liczba naturalna $n > 1$ ma jednoznaczny (z dokładnością do kolejności) rozkład na iloczyn liczb pierwszych.*

STWIERDZENIE 9.6. *Jeśli $0 < a, b \in \mathbb{N}$, $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ i $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, gdzie p_i są liczbami pierwszymi oraz $0 \leqslant \alpha_i, \beta_i \in \mathbb{N}$, to*

$$\mathrm{NWD}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)},$$
$$\mathrm{NWW}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_k^{\max(\alpha_k, \beta_k)},$$
$$\mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b) = ab.$$

10 Arytmetyka

10.1 Rozwiązywanie równań modularnych

Niech $0 < n \in \mathbb{N}$. Mówimy, że dwie liczby $a, b \in \mathbb{Z}$ przystają do siebie modulo n, co zapisujemy

$$a \equiv_n b \quad \text{wtedy i tylko wtedy, gdy} \quad a \bmod n = b \bmod n,$$

czyli gdy a, b dają tę samą resztę przy dzieleniu przez n.

Dla dowolnych $a, b, c \in \mathbb{Z}$ oraz $0 < n \in \mathbb{N}$ zachodzi:

- $a \equiv_n a$,
- jeśli $a \equiv_n b$, to $b \equiv_n a$,
- jeśli $a \equiv_n b$ i $b \equiv_n c$, to $a \equiv_n c$.

Powyższe własności świadczą o tym, że przystawanie $\equiv_n$ modulo n jest relacją równoważności na zbiorze $\mathbb{Z}$. Dlatego czasem relacja ta nazywana jest równością modulo n. Okazuje się też, że relacja $\equiv_n$ jest zgodna z działaniami arytmetycznymi: dodawania, odejmowania i mnożenia, a więc jest kongruencją ze względu na te działania.

Stwierdzenie 10.1. *Dla dowolnych $a, b, c, d \in \mathbb{Z}$ oraz $0 < n \in \mathbb{N}$ zachodzi:*

- *jeśli $a \equiv_n b$ i $c \equiv_n d$, to $a + c \equiv_n b + d$,*
- *jeśli $a \equiv_n b$ i $c \equiv_n d$, to $a - c \equiv_n b - d$,*
- *jeśli $a \equiv_n b$ i $c \equiv_n d$, to $ac \equiv_n bd$.*

Twierdzenie 10.2. *Dla dowolnych $0 \neq a, b \in \mathbb{Z}$ istnieją takie $n, m \in \mathbb{Z}$, że:*

$$an + bm = \mathrm{NWD}(a, b).$$

Zbiór reszt modulo n wraz z operacjami dodawania i mnożenia tworzy pierścień przemienny z jedynką $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Pierścień ten nie zawsze jest jednak ciałem bo nie zawsze możemy skracać w mnożeniu czynnik zachowując kongruencję. Na przykład:

$$2 \cdot 2 = 4 \equiv_6 10 = 2 \cdot 5,$$

ale $2 \not\equiv_6 5$. W równości modulo n możemy skracać czynniki względnie pierwsze z n.

Stwierdzenie 10.3. *Dla $a, b, d, n \in \mathbb{N}$ jeśli $0 < n$, $ad \equiv_n bd$ i $\mathrm{NWD}(d, n) = 1$, to $a \equiv_n b$.*

W takim piercieniu $\mathbb{Z}_n$ można rozwiązywać tzw. *równania modularne*. Dla $a, b \in \mathbb{Z}$, $a \neq 0$ rozwiązania równania modularnego

$$ax \equiv_n b,$$

z jedną niewiadomą x zależą od wielkości $\mathrm{NWD}(a, n)$ w następujący sposób:

- jeśli $\mathrm{NWD}(a, n) = 1$,

  to istnieje nieskończenie wiele rozwiązań; wszystkie one są postaci $x = x_0 + kn$, gdzie $0 \leqslant x_0 < n$ jest jakimś rozwiązaniem, a $k \in \mathbb{Z}$.

- jeśli $\mathrm{NWD}(a, n) =: d > 1$,

  to równanie ma rozwiązanie wtedy i tylko wtedy, gdy również $d \mid b$. W tym przypadku rozwiązania równania $ax \equiv_n b$ pokrywają się z rozwiązaniami równania

  $$\frac{a}{d} x \equiv_{\frac{n}{d}} \frac{b}{d}.$$

10.2 Chińskie twierdzenie o resztach

Twierdzenie 10.4 (Chińskie twierdzenie o resztach). *Niech* $0 < n_1, n_2, \ldots, n_k \in \mathbb{N}$ *będą parami względnie pierwsze, tzn.* $\mathrm{NWD}(n_i, n_j) = 1$ *dla* $i \neq j$*. Wówczas dla dowolnych* $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ *istnieje dokładnie jedna liczba całkowita* x *taka, że* $0 \leqslant x < n_1 n_2 \cdot \cdots \cdot n_k$ *i*

$$\begin{aligned} x &\equiv_{n_1} a_1, \\ x &\equiv_{n_2} a_2, \\ &\vdots \\ x &\equiv_{n_k} a_k. \end{aligned}$$

W celu znalezienia rozwiązania układu rownań z twierdzenia 10.4:

1. Sprawdzamy czy współczynniki n_i, $i = 1, \ldots, k$ są parami wzlędnie pierwsze. Jeśli nie, to 10.4 nie gwarantuje istnienia rozwiązania układu.

2. Obliczamy
$$N = n_1 n_2 \ldots n_k.$$

3. Obliczamy
$$N_i = \frac{N}{n_i}, \quad i = 1, \ldots, k.$$

4. Szukamy $t_i, x_i \in \mathbb{Z}$ (por. 10.2) takich, aby
$$\mathrm{NWD}(n_i, N_i) = n_i t_i + N_i x_i, \quad i = 1, \ldots, k.$$

5. Najmniejszym rozwiązaniem układu jest
$$x = a_1 x_1 N_1 + a_2 x_2 N_2 + \cdots + a_k x_k N_k.$$

10.3 Małe twierdzenie Fermata

Twierdzenie 10.5 (Małe Twierdzenie Fermata). *Dla dowolnej liczby pierwszej* p *i dowolnego* $a \in \mathbb{Z}$ *zachodzi:*
$$a^p \equiv_p a.$$

Wniosek 10.6. *Dla dowolnej liczby pierwszej* p *i dowolnych* $a, n \in \mathbb{Z}$ *zachodzi:*

$$a^{p-1} \equiv_p 1 \quad \textit{oraz} \quad a^n \equiv_p a^{(p-1)m + (n \bmod (p-1))} \equiv_p a^{n \bmod (p-1)},$$

gdzie m *to pewna liczba całkowita.*

10.4 Twierdzenie Eulera

Dla liczby naturalnej n, przez $\varphi(n)$ oznaczmy ilość liczb ze zbioru $\{1, 2, \ldots, n\}$, które sa względnie pierwsze z n, tzn.

$$\varphi(n) = \big|\{m \in \mathbb{N}\colon 1 \leqslant m \leqslant n \text{ oraz } \mathrm{NWD}(m, n) = 1\}\big|.$$

Funkcję tę nazywamy *funkcją Eulera.*

Stwierdzenie 10.7. *Jeśli $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, gdzie p_i to liczby pierwsze i $1 \leqslant \alpha_i$, to wtedy*

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1}\Big(1 - \frac{1}{p_1}\Big)p_2^{\alpha_2}\Big(1 - \frac{1}{p_2}\Big) \ldots p_k^{\alpha_k}\Big(1 - \frac{1}{p_k}\Big) \\ &= n \prod_{p \mid n}\Big(1 - \frac{1}{p}\Big). \end{aligned}$$

Twierdzenie 10.8 (Twierdzenie Eulera)**.** *Jeśli liczby a, n są względnie pierwsze, tzn. jeśli* $\mathrm{NWD}(a, n) = 1$*, to*

$$a^{\varphi(n)} \equiv_n 1.$$

11 Teoria grafów

Niech V będzie niepustym zbiorem i niech E będzie rodziną co najwyżej dwu-elementowych podziorów zbioru V, czyli

$$E = \big\{\{v, w\} \colon v, w \in V\big\}.$$

Elementy zbioru V będziemy nazywać *wierzchołkami* (ang. vertices) lub czasem *węzłami* albo *punktami*, natomiast elementy zbioru E *krawędziami* (ang. edges). Strukturę

$$\mathbb{G} = \langle V, E \rangle$$

będziemy nazywać *grafem.* Jeżeli w grafie $\mathbb{G}$ dla wierzchołków $v, w \in V$ istnieje krawędź je łącząca, oznaczana jako $vw = \{v, w\} \in E$, to mówimy, że wierzchołki v, w są *sąsiednie.* Mówimy, że wierzchołek $v \in V$ *incyduje* z krawędzią $e \in E$, gdy krawedź e wychodzi z wierzchołka V, czyli formalnie $v \in e$. Liczba krawędzi incydentnych z wierzchołkiem v to *stopień wierzchołka* v w grafie $\mathbb{G}$ i oznaczana jest przez $\deg(v)$.

Graf prosty to taka struktura $\mathbb{G}$, gdzie E jest zbiorem krawędzi między różnymi wierzchołkami, czyli

$$E = \big\{\{v, w\} \colon v, w \in V, v \neq w\big\}.$$

jest rodziną dwu-elementowych podzbiorów V.

Stwierdzenie 11.1. *Jeśli $\mathbb{G} = \langle V, E \rangle$ jest grafem prostym, to*

$$\sum_{v \in V} \deg(v) = 2|E|.$$

Dowód. Każda krawędź incyduje z dwoma wierzchołkami. Zliczając krawędzie incydentne do kolejnych wierzchołków, a następnie sumując te wartości, każda krawędź vw zostanie zliczona dwa razy: raz przy rozpatrywaniu wierzchołka v, a drugi raz przy w. □

Jeśli graf $\mathbb{G}$ miałby nieparzyście wiele wierzchołków o nieparzystym stopniu to suma $\sum_{v\in V}\deg(v)$ byłaby nieparzysta, wbrew temu, co mówi 11.1.

Wniosek 11.2. *Liczba wierzchołków o nieparzystym stopniu w grafie prostym jest parzysta.*

Graf $\mathbb{G} = \langle V, E\rangle$ nazywamy *skierowanym*, gdy

$$E = \{(v, w) \colon v, w \in V\} \subseteq V \times V,$$

czyli gdy krawędzie to pary uporządkowane.

Graf pusty to graf bez krawędzi. *Antyklika* lub graf *niezależny* to inne nazwy grafu pustego. Antyklikę o n wierzchołkach oznaczać będziemy przez $\mathcal{A}_n$.

Graf pełny to graf, w którym każde dwa wierzchołki połączone są krawędzią. Graf pełny nazywany jest także *kliką* i oznaczany przez $\mathcal{K}_n$, gdzie n jest liczbą jego wierzchołków. Liczba krawędzi w klice $\mathcal{K}_n$ wynosi

$$\frac{n(n-1)}{2}.$$

Graf dwudzielny, w którym zbiór wierzchołków V da się podzielić na dwa rozłączne podzbiory V_1 oraz V_2 tak, by żadne dwa wierzchołki w obrębie tego samego podzbioru V_i nie były sąsiadami. Podział taki nie jest jednoznaczny bo na przykład w antyklice dowolny podział zbioru wierzchołków na dwa podzbiory jest podziałem dwudzielnym. *Pełny graf dwudzielny* to graf dwudzielny, w którym każdy wierzchołek z V_1 jest połączony z każdym wierzchołkiem z V_2. Pełny graf dwudzielny oznaczać będziemy przez $\mathcal{K}_{r,s}$, gdzie r jest rozmiarem V_1, a s rozmiarem V_2.

11.1 Ścieżki, cykle i drzewa

Ścieżka w grafie $\mathbb{G}$ z wierzchołka w do wierzchołka u to skończony ciąg krawędzi postaci

$$wv_1, v_1v_2, \ldots, v_{k-1}u.$$

W skrócie ścieżkę taką oznaczamy przez

$$w \to v_1 \to v_2 \to \cdots \to v_{k-1} \to u.$$

Wierzchołek w nazywać będziemy *początkowym*, a u *końcowym*. *Długość* ścieżki to ilość jej krawędzi, w naszym wypadku wynosi ona k. Ścieżka *zamknięta* to ścieżka kończąca się w punkcie wyjścia, czyli taka, w której $w = u$. Pojęcie ścieżki ma sens również w grafie skierowanym, należy jednak wówczas uwzględnić skierowanie krawędzi.

Cykl to ścieżka zamknięta, w kórej jedynym powtarzającym się wierzchołkiem jest jej początek (będący jednocześnie jej końcem).

Graf jest *spójny*, gdy między dwoma dowolnymi wierzchołkami istnieje ścieżka. Wierzchołek *izolowany* to wierzchołek nie posiadający sąsiadów.

Drzewo to graf spójny nie zawierający cykli. *Las* to suma drzew, czyli graf nie zawierający cykli jako podgrafy. *Liść* to wierzchołek o stopniu 1. *Gwiazda* to drzewo, w którym co najwyżej jeden wierzchołek nie jest liściem.

Twierdzenie 11.3. *Dla grafu $\mathbb{G} = \langle V, E \rangle$ następujące warunki są równoważne:*

(i) *$\mathbb{G}$ jest drzewem.*

(ii) *$\mathbb{G}$ nie zawiera cykli i ma $|V| - 1$ krawędzi.*

(iii) *$\mathbb{G}$ jest spójny i ma $|V| - 1$ krawędzi.*

(iv) *$\mathbb{G}$ jest spójny, zaś usunięcie dowolnej krawędzi tworzy dokładnie dwie składowe.*

(v) *Dowolne dwa wierzchołki grafu $\mathbb{G}$ są połączone dokładnie jedną drogą.*

(vi) *$\mathbb{G}$ nie zawiera cykli, lecz dodanie dowolnej nowej krawędzi tworzy dokładnie jeden cykl.*

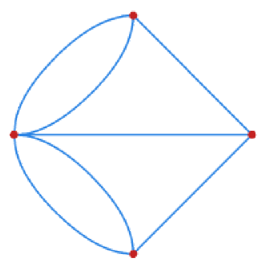
11.2 Cykle Eulera

Leonhard Euler stanął przed następującym problemem. W Królewcu (wówczas Konigsbergu) na rzece Pregole, na której są dwie wyspy wybudowano siedem mostów łączące wyspy ze sobą, oraz z oboma brzegami rzeki. Układ mostów został przedstawiony na rys. 1.

Rysunek 1: Mapa mostów w Królewcu.

Pytanie, jakie zostało postawione Eulerowi, to czy można tak ułożyć spacer po wszystkich mostach Królewca, by po każdym przejść tylko raz i wrócić do punktu startowego. Euler oczywiście odpowiedział na zadane mu pytanie.

Powyższy problem można przedstawić w języku grafów. Niech każdy spójny kawałek lądu w Królewcu odpowiada wierzchołkowi. Otrzymamy w ten sposób dwa wierzchołki odpowiadające wyspom oraz dwa obu brzegom Pregoły. Most pomiędzy dwoma kawałkami lądu będziemy interpretować jako krawędź łączącą wierzchołki odpowiadające tym skrawkom lądu. W ten sposób otrzymamy graf (nie będący grafem prostym) jak na rys. 2.



Rysunek 2: Graf połączeń mostami w Królewcu.

Cykl Eulera to zamknięta ścieżka przechodząca przez każdą krawędź grafu dokładnie raz. Mówimy, że graf jest *eulerowski*, gdy posiada cykl Eulera.

Twierdzenie 11.4. *Graf $\mathbb{G} = \langle V, E\rangle$ jest eulerowski wtedy i tylko wtedy, gdy jest spójny i stopień każdego wierzchołka jest parzysty.*

Twierdzenie 11.5. *Niech $\mathbb{G} = \langle V, E\rangle$ będzie spójnym grafem planarnym. Wówczas w dowolnej planarnej reprezentacji grafu $\mathbb{G}$ liczba regionów (obszarów, na jakie krawędzie grafu dzielą płaszczyznę) jest równa*

$$|S| = |E| + |V| + 2.$$

11.3 Cykle Hamiltona

Inny, ciekawy problem można przedstawić na przykładzie firmy rozwożącej przesyłki. Dotyczy on pracy kuriera mającego rozwieźć przesyłki do odbiorców, w ten sposób by odwiedzić każdego klienta jedynie raz, a na końcu wrócić do siedziby firmy. Jest to tzw. problem komiwojażera.

Cykl Hamiltona to cykl przechodzący przez wszystkie wierzchołki grafu (czyli ścieżka zamknięta odwiedzająca każdy wierzchołek dokładnie raz). *Graf hamiltonowski* to graf posiadający cykl Hamiltona. *Ścieżka Hamiltona* to ścieżka przechodząca przez wszystkie wierzchołki, każdy odwiedzając jedynie jeden raz.

W odróżnieniu od grafów eulerowskich, grafy hamiltonowskie nie posiadają prostej i szybkiej w użyciu charakteryzacji. Nie znana jest żadna metoda, pozwalająca szybko (tzn. w czasie wielomianowym) stwierdzić czy dany graf jest hamiltonowski. Są natomiast znane pewne warunki wystarczające na to, by graf był hamiltonowski.

Twierdzenie 11.6 (Ore 1960)**.** *Jeśli w grafie prostym $\mathbb{G} = \langle V, E\rangle$ o co najmniej 3 wierzchołkach dowolne dwa niesąsiednie wierzchołki v i w spełniają*

$$\deg(v) + \deg(w) \geqslant |V|,$$

to graf $\mathbb{G}$ jest hamiltonowski.

Literatura

[1] Graham, R. L., Knuth, D. E., Patashnik, O. *Matematyka konkretna.* Państwowe Wydawnictwo Naukowe, Warszawa, 1996.

[2] Lipski, W. *Kombinatoryka dla programistów.* Wydawnictwa Naukowo-Techniczne, Warszawa, 2004.

[3] Ross, K. A., Wright, Ch. R. B. *Matematyka dyskretna.* Państwowe Wydawnictwo Naukowe, Warszawa, 1998.

[4] Pałka, Z., Ruciński, A. *Wykłady z kombinatoryki.* Wydawnictwa Naukowo-Techniczne, Warszawa, 1998.