

GRZEGORZ BOBIŃSKI

# Matematyka Dyskretna

Wydział Matematyki i Informatyki  
Uniwersytet Mikołaja Kopernika w Toruniu  
2013

# MATEMATYKA DYSKRETNA

## SPIS TREŚCI

<b>1</b>	<b>Elementy teorii liczb</b>	<b>1</b>
1.1	Twierdzenie o dzieleniu z resztą . . . . .	1
1.2	Największy wspólny dzielnik . . . . .	5
1.3	Zasadnicze twierdzenie arytmetyki . . . . .	10
1.4	Kongruencje . . . . .	17
1.5	Funkcja i twierdzenie Eulera . . . . .	20
1.6	Zastosowanie teorii liczb w kryptografii . . . . .	23
<b>2</b>	<b>Elementy kombinatoryki</b>	<b>26</b>
2.1	Podstawowe obiekty kombinatoryczne . . . . .	26
2.2	Metoda bijektywna . . . . .	29
2.3	Reguła włączania i wyłączania . . . . .	36
<b>3</b>	<b>Funkcje tworzące</b>	<b>39</b>
3.1	Szeregi formalne . . . . .	39
3.2	Funkcje tworzące . . . . .	40
3.3	Rekurencja . . . . .	43
3.4	Wielomiany wieżowe . . . . .	54
<b>4</b>	<b>Systemy reprezentantów i twierdzenie Halla</b>	<b>60</b>
<b>5</b>	<b>Ważne ciągi liczbowe</b>	<b>65</b>
5.1	Liczby Stirlinga . . . . .	65
5.2	Liczby Bella . . . . .	68

## MATEMATYKA DYSKRETNA

Będziemy korzystać z następujących oznaczeń dla zbiorów liczbowych:

- symbolem  $\mathbb{Z}$  oznaczać będziemy zbiór liczb całkowitych,
- symbolem  $\mathbb{N}$  oznaczać będziemy zbiór liczb całkowitych nieujemnych,
- symbolem  $\mathbb{N}_+$  oznaczać będziemy zbiór liczb całkowitych dodatnich,
- jeśli  $i, j \in \mathbb{Z}$ , to

$$[i, j] := \{k \in \mathbb{Z} : i \leq k \leq j\}.$$

- jeśli  $i \in \mathbb{Z}$ , to

$$[i, \infty[ := \{k \in \mathbb{Z} : i \leq k\}.$$

Jeśli  $n \in \mathbb{N}$  i  $x_1, \dots, x_n \in \mathbb{Z}$ , to dla każdej liczby  $k \in [0, n]$  definiujemy wyrażenia  $\sum_{i \in [1, k]} x_i$  i  $\prod_{i \in [1, k]} x_i$  wzorami

$$\sum_{i \in [1, k]} x_i := \begin{cases} 0 & \text{jeśli } k = 0, \\ \left( \sum_{i \in [1, k-1]} x_i \right) + x_k & \text{jeśli } k > 0, \end{cases}$$

i

$$\prod_{i \in [1, k]} x_i := \begin{cases} 1 & \text{jeśli } k = 0, \\ \left( \prod_{i \in [1, k-1]} x_i \right) \cdot x_k & \text{jeśli } k > 0. \end{cases}$$

Jeśli  $I$  jest zbiorem skończonym oraz  $F : I \rightarrow \mathbb{C}$  jest funkcją, to definiujemy

$$\sum_{i \in I} F(i) := \sum_{j \in [1, |I|]} F(\sigma(j)) \quad \text{i} \quad \prod_{i \in I} F(i) := \prod_{j \in [1, |I|]} F(\sigma(j)),$$

gdzie  $\sigma : [1, |I|] \rightarrow I$  jest ustaloną bijekcją (powyższe definicje nie zależą od wyboru bijekcji  $\sigma$ ).

## MATEMATYKA DYSKRETNA

### 1. ELEMENTY TEORII LICZB

#### 1.1. TWIERDZENIE O DZIELENIU Z RESZTĄ

##### DEFINICJA.

Niech  $a$  i  $b$  będą liczbami całkowitymi. Mówimy, że LICZBA  $a$  DZIELI LICZBĘ  $b$ , jeśli istnieje liczba całkowita  $k$  taka, że  $b = k \cdot a$ .

##### UWAGA.

Jeśli  $a$  i  $b$  są liczbami całkowitymi i  $a \neq 0$ , to liczba  $a$  dzieli liczbę  $b$  wtedy i tylko wtedy, gdy liczba  $\frac{b}{a}$  jest całkowita.

##### OZNACZENIE.

Jeśli liczba całkowita  $a$  dzieli liczby całkowitą  $b$ , to piszemy  $a \mid b$ .

##### PRZYKŁAD.

$$2 \mid 4.$$

##### OZNACZENIE.

Jeśli liczba całkowita  $a$  nie dzieli liczby całkowitej  $b$ , to piszemy  $a \nmid b$ .

##### PRZYKŁAD.

$$2 \nmid 3.$$

##### FAKT 1.1.

Jeśli  $a$  jest liczbą całkowitą, to  $a \mid a$ .

##### DOWÓD.

Teza wynika z równości  $a = 1 \cdot a$ . □

##### FAKT 1.2.

Jeśli  $a, b$  i  $c$  są liczbami całkowitymi,  $a \mid b$  i  $b \mid c$ , to  $a \mid c$ .

##### DOWÓD.

Ustalmy liczby całkowite  $k$  i  $l$  takie, że  $b = k \cdot a$  i  $c = l \cdot b$ . Wtedy  $c = (k \cdot l) \cdot a$ . □

##### FAKT 1.3.

Jeśli  $a$  i  $b$  są liczbami całkowitymi,  $a \mid b$  i  $b \mid a$ , to  $b = \pm a$ .

##### DOWÓD.

Jeśli  $a = 0 = b$ , to teza jest oczywista. Bez straty ogólności możemy zatem założyć, że  $a \neq 0$ . Ustalmy liczby całkowite  $k$  i  $l$  takie, że  $b = k \cdot a$  i  $a = l \cdot b$ . Wtedy  $a = l \cdot k \cdot a$ , zatem  $l \cdot k = 1$ . W szczególności  $k = \pm 1$ , co kończy dowód. □

##### FAKT 1.4.

Jeśli  $a$  jest liczbą całkowitą, to  $1 \mid a$ . W szczególności, jeśli  $a$  jest liczbą

## MATEMATYKA DYSKRETNA

całkowitą, to  $a \mid 1$  wtedy i tylko wtedy, gdy  $a = \pm 1$ .

DOWÓD.

Pierwsza część wynika z równości  $a = a \cdot 1$ . Dla dowodu drugiej części zauważmy, że jeśli  $a = \pm 1$ , to oczywiście  $a \mid 1$ , gdyż  $1 = \pm 1 \cdot \pm 1$ . Załóżmy zatem, że  $a \mid 1$ . Ponieważ  $1 \mid a$  na mocy pierwszej części, więc teza wynika z Faktu 1.3.  $\square$

FAKT 1.5.

Jeśli  $a$  jest liczbą całkowitą, to  $a \mid 0$ . W szczególności, jeśli  $a$  jest liczbą całkowitą, to  $0 \mid a$  wtedy i tylko wtedy, gdy  $a = 0$ .

DOWÓD.

Pierwsza część wynika z równości  $0 = 0 \cdot a$ . Dla dowodu drugiej części zauważmy, że jeśli  $a = 0$ , to oczywiście  $0 \mid a$ , gdyż  $0 = 1 \cdot 0$ . Załóżmy zatem, że  $0 \mid a$ . Ponieważ  $a \mid 0$  na mocy pierwszej części, więc teza wynika z Faktu 1.3.  $\square$

FAKT 1.6.

Jeśli  $a$  i  $b$  są liczbami całkowitymi,  $a \mid b$  i  $b \neq 0$ , to  $|a| \leq |b|$ .

DOWÓD.

Ustalmy liczbę całkowitą  $k$  taką, że  $b = k \cdot a$ . Ponieważ  $b \neq 0$ , więc  $k \neq 0$ . W szczególności  $|k| \geq 1$ . Stąd

$$|b| = |k| \cdot |a| \geq |a|. \quad \square$$

FAKT 1.7.

Jeśli  $a$ ,  $b$  i  $c$  są liczbami całkowitymi,  $a \mid b$  i  $a \mid c$ , to  $a \mid b \pm c$ .

DOWÓD.

Ustalmy liczby całkowite  $k$  i  $l$  takie, że  $b = k \cdot a$  i  $c = l \cdot a$ . Wtedy  $b \pm c = (k \pm l) \cdot a$ .

FAKT 1.8.

Jeśli  $a$ ,  $b$  i  $c$  są liczbami całkowitymi i  $a \mid b$ , to  $a \mid b \cdot c$ .

DOWÓD.

Ustalmy liczbę całkowitą  $k$  taką, że  $b = k \cdot a$ . Wtedy  $b \cdot c = (k \cdot c) \cdot a$ .  $\square$

FAKT 1.9.

Jeśli  $a$ ,  $b$  i  $c$  są liczbami całkowitymi i  $c \neq 0$ , to  $a \cdot c \mid b \cdot c$  wtedy i tylko wtedy, gdy  $a \mid b$ .

DOWÓD.

Załóżmy najpierw, że  $a \mid b$  i wybierzmy liczbę całkowitą  $k$  taką, że  $b = k \cdot a$ . Wtedy  $b \cdot c = k \cdot (a \cdot c)$ .

## MATEMATYKA DYSKRETNA

Z drugiej strony jeśli  $a \cdot c \mid b \cdot c$ , to istnieje liczba całkowita  $k$  taką, że  $b \cdot c = k \cdot (a \cdot c)$ . Ponieważ  $c \neq 0$ , więc  $b = k \cdot a$ .  $\square$

DEFINICJA.

Niech  $a$  i  $b$  będą liczbami całkowitymi takimi, że  $b \neq 0$ . IŁORAZEM CAŁKOWITYM Z DZIELENIA LICZBY  $a$  PRZEZ LICZBĘ  $b$  nazywamy każdą liczbę całkowitą  $q$  taką, że

$$q \cdot b = \max\{q' \cdot b : q' \in \mathbb{Z} \text{ i } q' \cdot b \leq a\}.$$

FAKT 1.10.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to istnieje iloraz całkowity z dzielenia liczby  $a$  przez liczbę  $b$ .

DOWÓD.

Wystarczy pokazać, że zbiór  $\{q \in \mathbb{Z} : q \cdot b \leq a\}$  jest niepusty. Zauważmy jednak, że  $\text{sign } b \cdot b = |b| \geq 1$ , gdyż  $b \neq 0$ . Stąd

$$(-\text{sign } b \cdot |a|) \cdot b = -|a| \cdot (\text{sign } b \cdot |b|) \leq -|a| \cdot 1 = -|a| \leq a. \quad \square$$

FAKT 1.11.

Niech  $a$  i  $b$  będą liczbami całkowitymi takimi, że  $b \neq 0$ . Jeśli  $q_1$  i  $q_2$  są ilorazami całkowitymi z dzielenia liczby  $a$  przez liczbę  $b$ , to  $q_1 = q_2$ .

DOWÓD.

Z definicji ilorazu całkowitego wiemy, że

$$q_1 \cdot b = \max\{q' \cdot b : q' \in \mathbb{Z} \text{ i } q' \cdot b \leq a\} = q_2 \cdot b.$$

Stąd  $q_1 \cdot b = q_2 \cdot b$ . Ponieważ  $b \neq 0$ , więc  $q_1 = q_2$ .  $\square$

OZNACZENIE.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to przez  $a \text{ div } b$  oznaczamy iloraz całkowity z dzielenia liczby  $a$  przez liczbę  $b$ .

DEFINICJA.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to RESZTĄ Z DZIELENIA LICZBY  $a$  PRZEZ LICZBĘ  $b$  nazywamy liczbę  $a - (a \text{ div } b) \cdot b$ .

OZNACZENIE.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to przez  $a \text{ mod } b$  oznaczamy resztę z dzielenia liczby  $a$  przez liczbę  $b$ .

OZNACZENIE.

Jeśli  $a$  jest liczbą całkowitą, to definiujemy

$$\text{sign } a := \begin{cases} -1 & \text{jeśli } a < 0, \\ 0 & \text{jeśli } a = 0, \\ 1 & \text{jeśli } a > 0. \end{cases}$$

FAKT 1.12.

Jeśli  $a$  jest liczbą całkowitą, to  $|a| = \text{sign } a \cdot a$  i  $a = \text{sign } a \cdot |a|$ .

DOWÓD.

Oczywiste. □

STWIERDZENIE 1.13.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to

$$0 \leq a \bmod b < |b| \quad \text{i} \quad a = (a \text{ div } b) \cdot b + a \bmod b.$$

DOWÓD.

Równość

$$(*) \quad a = (a \text{ div } b) \cdot b + a \bmod b$$

wynika natychmiast z definicji reszty. Z definicji ilorazu całkowitego wiemy, że  $(a \text{ div } b) \cdot b \leq a$ , a więc równość  $(*)$  implikuje, że  $a \bmod b \geq 0$ . Pozostaje udowodnić, że  $a \bmod b < |b|$ . Przypuśćmy, że  $a \bmod b \geq |b|$ , a więc  $(a \text{ div } b) \cdot b \leq a - |b|$ . Jeśli  $q := a \text{ div } b + \text{sign } b$ , to

$$q \cdot b \leq a \quad \text{i} \quad a - q \cdot b < a - (a \text{ div } b) \cdot b,$$

co prowadzi do sprzeczności z definicją ilorazu całkowitego. □

TWIERDZENIE 1.14 (TWIERDZENIE O DZIELENIU Z RESZTĄ).

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to istnieją jednoznacznie wyznaczone liczby całkowite  $q$  i  $r$  takie, że

$$0 \leq r < |b| \quad \text{i} \quad a = q \cdot b + r.$$

DOWÓD.

Istnienie liczb  $q$  i  $r$  wynika natychmiast ze Stwierdzenia 1.13.

Przypuśćmy teraz, że istnieją liczby całkowite  $q_1, q_2, r_1$  i  $r_2$  takie, że

$$0 \leq r_1, r_2 < |b| \quad \text{i} \quad q_1 \cdot b + r_1 = a = q_2 \cdot b + r_2.$$

Wtedy  $r_1 - r_2 = (q_2 - q_1) \cdot b$ , więc  $b \mid r_1 - r_2$ . Ponieważ  $|r_1 - r_2| < |b|$ , więc  $r_1 - r_2 = 0$  (tzn.  $r_1 = r_2$ ) na mocy Faktu 1.6. Stąd  $(q_2 - q_1) \cdot b = 0$ , zatem  $q_2 - q_1 = 0$  (tzn.  $q_1 = q_2$ ), gdyż  $b \neq 0$ . □

WNIOSEK 1.15.

Niech  $a$  i  $b$  będą liczbami całkowitymi takimi, że  $b \neq 0$ . Jeśli  $q$  i  $r$  są takimi liczbami całkowitymi takimi, że

$$0 \leq r < |b| \quad \text{i} \quad a = q \cdot b + r,$$

to  $q = a \operatorname{div} b$  i  $r = a \operatorname{mod} b$ .

W szczególności jeśli  $0 \leq a < |b|$ , to  $a \operatorname{mod} b = a$  i  $a \operatorname{div} b = 0$ .

DOWÓD.

Ze Stwierdzenia 1.13 wiemy, że

$$0 \leq a \operatorname{mod} b < |b| \quad \text{i} \quad a = (a \operatorname{div} b) \cdot b + a \operatorname{mod} b,$$

zatem pierwsza część wynika z Twierdzenia 1.14.

Druga część wynika natychmiast z pierwszej. □

WNIOSEK 1.16.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to  $b \mid a$  wtedy i tylko wtedy, gdy  $a \operatorname{mod} b = 0$ .

DOWÓD.

Jeśli  $b \mid a$ , to istnieje liczba całkowita  $q$  taka, że  $a = q \cdot b$ . Wtedy

$$0 \leq 0 < |b| \quad \text{i} \quad a = q \cdot b + 0,$$

więc  $0 = a \operatorname{mod} b$  na mocy Wniosku 1.15. Z drugiej strony, jeśli  $a \operatorname{mod} b = 0$ , to  $a = (a \operatorname{div} b) \cdot b$  (a więc  $b \mid a$ ) na mocy Stwierdzenia 1.13.

## 1.2. NAJWIĘKSZY WSPÓLNY DZIELNIK

DEFINICJA.

Niech  $a$  i  $b$  będą liczbami całkowitymi. Liczbę całkowitą  $d$  nazywamy NAJWIĘKSZYM WSPÓLNYM DZIELNIKIEM LICZB  $a$  I  $b$ , jeśli spełnione są następujące warunki:

- (1)  $d \geq 0$ ,
- (2)  $d \mid a$  i  $d \mid b$ ,
- (3) jeśli  $c$  jest liczbą całkowitą,  $c \mid a$  i  $c \mid b$ , to  $c \mid d$ .

PRZYKŁAD.

Liczba 0 jest największym wspólnym dzielnikiem liczb 0 i 0.

FAKT 1.17.

Jeśli  $a$  i  $b$  są liczbami całkowitymi, to istnieją liczby całkowite  $k$  i  $l$  takie, że liczba  $k \cdot a + l \cdot b$  jest największym wspólnym dzielnikiem liczb  $a$  i  $b$ . W szczególności istnieje największy wspólny dzielnik liczb  $a$  i  $b$ .



DOWÓD.

Jeśli  $a = 0 = b$ , to  $0 = 0 \cdot a + 0 \cdot b$  jest największym wspólnym dzielnikiem liczb  $a$  i  $b$ . Załóżmy, że  $a \neq 0$  lub  $b \neq 0$ . Niech

$$I := \{k \cdot a + l \cdot b : k, l \in \mathbb{Z}\} \cap \mathbb{N}_+.$$

Ponieważ  $|a| = \text{sign } a \cdot a + 0 \cdot b$  i  $|b| = 0 \cdot b + \text{sign } b \cdot b$ , więc  $I \neq \emptyset$ . Niech  $d := \min I$  i ustalmy liczby całkowite  $k$  i  $l$  takie, że  $d = k \cdot a + l \cdot b$ . Pokażemy, że liczba  $d$  jest największym wspólnym dzielnikiem liczb  $a$  i  $b$ . Oczywiście  $d \geq 0$ . Ponadto, jeśli  $c$  jest liczbą całkowitą,  $c \mid a$  i  $c \mid b$ , to  $c \mid d$  na mocy Faktów 1.7 i 1.8. Pozostaje udowodnić, że  $d \mid a$  i  $d \mid b$ . Korzystając ze Stwierdzenia 1.13 otrzymujemy, że

$$a \bmod d = a - (a \text{ div } d) \cdot d = (1 - (a \text{ div } d) \cdot k) \cdot a - ((a \text{ div } d) \cdot l) \cdot b.$$

Korzystając ponownie ze Stwierdzenia 1.13 wiemy, że  $a \bmod d < d$ , więc  $a \bmod d \notin I$ , gdyż  $d = \min I$ . Ponieważ  $a \bmod d \geq 0$  na mocy Stwierdzenia 1.13, więc definicja zbioru  $I$  implikuje, że  $a \bmod d = 0$ . Wniosek 1.16 oznacza, że  $d \mid a$ . Analogicznie pokazujemy, że  $d \mid b$ .

FAKT 1.18.

Niech  $a$  i  $b$  będą liczbami całkowitymi. Jeśli  $d_1$  i  $d_2$  są największymi wspólnymi dzielnikami liczb  $a$  i  $b$ , to  $d_1 = d_2$ .

DOWÓD.

Z warunku (2) definicji największego wspólnego dzielnika wiemy, że  $d_1 \mid a$  i  $d_1 \mid b$ . Wykorzystując warunek (3) definicji (dla  $c = d_1$  i  $d = d_2$ ), otrzymujemy, że  $d_2 \mid d_1$ . Analogicznie pokazujemy, że  $d_1 \mid d_2$ . Fakt 1.3 implikuje, że  $d_1 = \pm d_2$ . Ponieważ  $d_1, d_2 \geq 0$  na mocy warunku (1) definicji, więc  $d_1 = d_2$ .  $\square$

OZNACZENIE.

Jeśli  $a$  i  $b$  są liczbami całkowitymi, to największy wspólny dzielnik liczb  $a$  i  $b$  oznaczamy symbolem  $\text{gcd}(a, b)$ .

WNIOSEK 1.19.

Jeśli  $a$  i  $b$  są liczbami całkowitymi, to istnieją liczby całkowite  $k$  i  $l$  takie, że  $\text{gcd}(a, b) = k \cdot a + l \cdot b$ .

DOWÓD.

Z Faktu 1.17 wynika, że istnieją liczby całkowite  $k$  i  $l$  takie, że liczba  $k \cdot a + l \cdot b$  jest największym wspólnym dzielnikiem liczb  $a$  i  $b$ . Fakt 1.18 implikuje, że  $k \cdot a + l \cdot b = \text{gcd}(a, b)$ .  $\square$

PRZYKŁAD.

Jeśli  $a$  jest liczbą całkowitą, to  $\text{gcd}(a, a) = |a|$ ,  $\text{gcd}(a, 1) = 1$  i  $\text{gcd}(a, 0) = |a|$ .

## MATEMATYKA DYSKRETNA

DOWÓD.

Ćwiczenie. □

PRZYKŁAD.

Jeśli  $a, b \in \mathbb{Z}$ , to  $\gcd(a, b) = \gcd(b, a)$ .

DOWÓD.

Ćwiczenie. □

LEMAT 1.20.

Jeśli  $a$  i  $b$  są liczbami całkowitymi takimi, że  $b \neq 0$ , to

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Ponadto, jeśli

$$\gcd(b, a \bmod b) = k \cdot b + l \cdot (a \bmod b)$$

dla pewnych liczb całkowitych  $k$  i  $l$ , to

$$\gcd(a, b) = l \cdot a + (k - l \cdot (a \operatorname{div} b)) \cdot b.$$

DOWÓD.

Niech

$$I_1 := \{c \in \mathbb{Z} : c \mid a \text{ i } c \mid b\} \quad \text{i} \quad I_2 := \{c \in \mathbb{Z} : c \mid b \text{ i } c \mid a \bmod b\}.$$

Dla dowodu pierwszej części wystarczy pokazać, że  $I_1 = I_2$ . Wiemy, że

$$(*) \quad a = (a \operatorname{div} b) \cdot b + a \bmod b$$

na mocy Stwierdzenia 1.13, więc teza wynika z Faktów 1.7 i 1.8. Druga część wynika poprzez bezpośredni rachunek z równości (\*). □

ALGORYTM (ROZSZERZONY ALGORYTM EUKLIDESA).

Wynikiem działania poniższej funkcji dla liczb całkowitych  $a$  i  $b$  jest  $\gcd(a, b)$  oraz liczby całkowite  $k$  i  $l$  takie, że  $(a, b) = k \cdot a + l \cdot b$ .

```
int Euclides (int a, int b, int & k, int & l) {
    if (b == 0) {
        l = 0;
        if (a > 0)
            k = 1;
        else
            k = -1;
    }
```

```

    return abs (a);
}
int x;
int y;
int d = Euclides (b, b mod a, x, y);
k = y;
l = x - y * (a div b);
return d;
}

```

LEMAT 1.21.

Jeśli  $a$  i  $b$  są liczbami całkowitymi, to

$$\gcd(a, b) \mid k \cdot a + l \cdot b$$

dla dowolnych liczb całkowitych  $k$  i  $l$ . W szczególności, jeśli istnieją liczby całkowite  $k$  i  $l$  takie, że

$$1 = k \cdot a + l \cdot b,$$

to  $\gcd(a, b) = 1$ .

DOWÓD.

Pierwsza część wynika z Faktów 1.7 i 1.8. Dla dowodu drugiej części zauważmy, że pierwsza część implikuje, iż  $\gcd(a, b) \mid 1$ . Ponieważ  $\gcd(a, b) \geq 0$ , więc Fakt 1.4 implikuje, że  $\gcd(a, b) = 1$ .  $\square$

WNIOSEK 1.22.

Jeśli  $a$ ,  $b$  i  $c$  są liczbami całkowitymi,  $\gcd(a, b) = 1$  i  $a \mid b \cdot c$ , to  $a \mid c$ .

DOWÓD.

Z Wniosku 1.19 wiemy, że istnieją liczby całkowite  $k$  i  $l$  takie, że

$$1 = k \cdot a + l \cdot b.$$

Ponadto, istnieje liczba całkowita  $q$  taka, że  $b \cdot c = q \cdot a$ . Wtedy

$$\begin{aligned} c &= c \cdot 1 = c \cdot (k \cdot a + l \cdot b) \\ &= c \cdot k \cdot a + l \cdot b \cdot c = c \cdot k \cdot a + l \cdot q \cdot a = (c \cdot k + l \cdot q) \cdot a, \end{aligned}$$

co kończy dowód.  $\square$

WNIOSEK 1.23.

Jeśli  $a, b_1, \dots, b_n$  są liczbami całkowitymi,  $n \in \mathbb{N}$ ,  $\gcd(a, b_i) = 1$  dla każdego  $i \in [1, n]$ , to

$$\gcd\left(a, \prod_{i \in [1, n]} b_i\right) = 1.$$

Dowód.

Udowodnimy tezę przez indukcję ze względu na  $n$ .

Dla  $n = 0$  teza jest oczywista, gdyż z definicji  $\prod_{i \in \emptyset} b_i = 1$ .

Założmy zatem, że  $n > 0$ , oraz, że

$$\gcd\left(a, \prod_{i \in [1, n-1]} b_i\right) = 1.$$

Z Wniosku 1.19 wiemy, że istnieją liczby całkowite  $x, y, k$  i  $l$  takie, że

$$x \cdot a + y \cdot \prod_{i \in [1, n-1]} b_i = 1 = k \cdot a + l \cdot b_n.$$

Wtedy

$$\begin{aligned} 1 &= x \cdot a + y \cdot \prod_{i \in [1, n-1]} b_i = x \cdot a + y \cdot \prod_{i \in [1, n-1]} b_i \cdot 1 \\ &= x \cdot a + y \cdot \prod_{i \in [1, n-1]} b_i \cdot (k \cdot a + l \cdot b_n) \\ &= \left(x + k \cdot y \cdot \prod_{i \in [1, n-1]} b_i\right) \cdot a + (l \cdot y) \cdot \prod_{i \in [1, n]} b_i, \end{aligned}$$

co kończy dowód na mocy Lematu 1.21. □

UWAGA.

Jeśli  $a, b_1, \dots, b_n$  są liczbami całkowitymi,  $n \in \mathbb{N}$ , oraz  $\gcd\left(a, \prod_{i \in [1, n]} b_i\right) = 1$ , to  $\gcd(a, b_i) = 1$  dla każdego  $i \in [1, n]$ .

WNIOSEK 1.24.

Jeśli  $a_1, \dots, a_n$  i  $b$  są liczbami całkowitymi,  $n \in \mathbb{N}$ ,  $\gcd(a_i, a_j) = 1$  dla wszystkich  $i, j \in [1, n]$  takich, że  $i \neq j$ ,  $a_i \mid b$  dla wszystkich  $i \in [1, n]$ , to

$$\prod_{i \in [1, n]} a_i \mid b.$$

Dowód.

Udowodnimy tezę przez indukcję na  $n$ .

Dla  $n = 0$  teza wynika, z Faktu 1.4, gdyż  $\prod_{i \in \emptyset} a_i = 1$ .

Założmy zatem, że  $n > 0$ , oraz wiemy już, że

$$\prod_{i \in [1, n-1]} a_i \mid b,$$

a więc istnieje liczba całkowita  $q$  taka, że

$$b = q \cdot \prod_{i \in [1, n-1]} a_i.$$

Z założenia istnieje również liczba całkowita  $q'$  taka, że  $b = q' \cdot a_n$ . Z Wniosku 1.23 wiemy, że  $\gcd(\prod_{i \in [1, n-1]} a_i, a_n) = 1$ , zatem na mocy Wniosku 1.19 istnieją liczby całkowite  $k$  i  $l$  takie, że

$$1 = k \cdot \prod_{i \in [1, n-1]} a_i + l \cdot a_n.$$

Wtedy

$$\begin{aligned} b &= b \cdot 1 = b \cdot \left( k \cdot \prod_{i \in [1, n-1]} a_i + l \cdot a_n \right) = b \cdot k \cdot \prod_{i \in [1, n-1]} a_i + b \cdot l \cdot a_n \\ &= q' \cdot a_n \cdot k \cdot \prod_{i \in [1, n-1]} a_i + q \cdot \prod_{i \in [1, n-1]} a_i \cdot l \cdot a_n \\ &= (k \cdot q' + l \cdot q) \cdot \prod_{i \in [1, n]} a_i, \end{aligned}$$

co kończy dowód. □

#### STWIERDZENIE 1.25.

Niech  $a$  i  $b$  będą liczbami całkowitymi i  $d := \gcd(a, b)$ . Jeśli  $d \neq 0$ , to

$$\gcd(a/d, b/d) = 1.$$

Dowód.

Z Wniosku 1.19 wiemy, że istnieją liczby całkowite  $k$  i  $l$  takie, że

$$d = k \cdot a + l \cdot b.$$

Wtedy

$$1 = k \cdot (a/d) + l \cdot (b/d),$$

co kończy dowód na mocy Lematu 1.21. □

### 1.3. ZASADNICZE TWIERDZENIE ARYTMETYKI

DEFINICJA.

Liczbę całkowitą  $p$  nazywamy PIERWSZĄ, jeśli  $p \geq 0$  i

$$\#\{a \in \mathbb{N} : a \mid p\} = 2.$$

OZNACZENIE.

Definiujemy

$$\mathbb{P} := \{p \in \mathbb{Z} : \text{liczba } p \text{ jest pierwsza}\}.$$

LEMAT 1.26.

Niech  $p$  będzie liczbą pierwszą.

- (1) Wtedy  $p > 1$ .
- (2) Jeśli  $a$  jest nieujemną liczbą całkowitą i  $a \mid p$ , to  $a = 1$  lub  $a = p$ .

DOWÓD.

- (1) Z Faktów 1.5 i 1.4 wiemy, że

$$\{a \in \mathbb{N} : a \mid 0\} = \mathbb{N} \quad \text{i} \quad \{a \in \mathbb{N} : a \mid 1\} = \{1\}.$$

- (2) Wiemy, że

$$\{1, p\} \subseteq \{a \in \mathbb{N} : a \mid p\}.$$

Ponieważ z definicji

$$\#\{a \in \mathbb{N} : a \mid p\} = 2$$

oraz  $p \neq 1$  na mocy części (1), więc

$$\{1, p\} = \{a \in \mathbb{N} : a \mid p\}. \quad \square$$

LEMAT 1.27.

Jeśli  $a$  jest dodatnią liczbą całkowitą, to istnieją liczby pierwsze  $p_1, \dots, p_n$ ,  $n \in \mathbb{N}$ , takie, że

$$a = \prod_{i \in [1, n]} p_i.$$

DOWÓD.

Dowód jest indukcyjny ze względu na  $a$ .

Jeśli  $a = 1$ , to teza jest oczywista ( $n := 0$ ).

Założmy teraz, że  $a > 1$ , oraz, że dla każdej dodatniej liczby całkowitej  $b$  mniejszej od  $a$  istnieją liczby pierwsze  $p_1, \dots, p_n$ ,  $n \in \mathbb{N}$ , takie, że

$$b = \prod_{i \in [1, n]} p_i.$$

## MATEMATYKA DYSKRETNA

Jeśli  $a$  jest liczbą pierwszą, to teza jest oczywista ( $n := 1$  i  $p_1 := a$ ).

Założmy zatem, że liczba  $a$  nie jest pierwsza. Wtedy istnieje nieujemna liczba całkowita  $b$  taka, że  $b \mid a$  i  $b \neq 1, a$ . W szczególności  $b < a$ . Z Faktu 1.5 wiemy, że  $b \neq 0$ . Z założenia indukcyjnego istnieją liczby pierwsze  $p_1, \dots, p_{n_1}$ ,  $n_1 \in \mathbb{N}$ , takie, że

$$b = \prod_{i \in [1, n_1]} p_i.$$

Niech  $c := a/b$ . Ponieważ  $b > 1$ , więc  $c < a$ . Oczywiście  $c > 0$ . Z założenia indukcyjnego istnieją liczby pierwsze  $p_{n_1+1}, \dots, p_{n_1+n_2}$ ,  $n_2 \in \mathbb{N}$ , takie, że

$$c = \prod_{i \in [n_1+1, n_1+n_2]} p_i.$$

Niech  $n := n_1 + n_2$ . Wtedy

$$a = b \cdot c = \prod_{i \in [1, n_1]} p_i \cdot \prod_{i \in [n_1+1, n_2]} p_i = \prod_{i \in [1, n]} p_i. \quad \square$$

### WNIOSEK 1.28.

Jeśli  $a$  jest liczbą całkowitą i  $a \neq \pm 1$ , to istnieje liczba pierwsza  $p$  taka, że  $p \mid a$ .

### DOWÓD.

Jeśli  $a = 0$ , to teza jest oczywista. Założmy zatem, że  $a \neq 0$ . Z Lematu 1.27 wiemy, że istnieją liczby pierwsze  $p_1, \dots, p_n$ ,  $n \in \mathbb{N}$ , takie, że

$$|a| = \prod_{i \in [1, n]} p_i.$$

Ponieważ  $|a| \neq 1$ , więc  $n > 0$ . W szczególności,  $p_1 \mid a$ . □

### ALGORYTM (SITO ERATOSTENESA).

Dla liczby dodatniej liczby całkowitej  $a$  algorytm zwraca wszystkie liczby pierwsze nie większe niż  $a$ .

```
int Eratostenes (int a, int * primes) {
    int num = 0;
    bool * prime = new bool [a + 1];
    for (int i = 2; i <= a; i++)
        prime [i] = true;
    for (int i = 2; i <= a; i++)
```

```

if (prime [i]) {
    primes [num] = i;
    num++;
    for (int j = i * i; j <= a; j += i)
        prime [j] = false;
}
delete [] prime;
return num;
}

```

TWIERDZENIE 1.29.

Istnieje nieskończenie wiele liczb pierwszych.

DOWÓD (EUKLIDES).

Pokażemy, że dla każdego skończonego podzbioru  $P$  zbioru liczb pierwszych istnieje liczba pierwsza  $p$  taka, że  $p \notin P$ .

Ustalmy skończony podzbiór  $P$  zbioru liczb pierwszych. Niech

$$a := \prod_{q \in P} q + 1.$$

Ponieważ  $a > 1$ , więc na mocy Lematu 1.28 istnieje liczba pierwsza  $p$  taka, że  $p \mid a$ . Zauważmy, że  $p \notin P$ . Istotnie, gdyby  $p \in P$ , to

$$p \mid a - \prod_{q \in P} q = 1$$

na mocy Faktu 1.7, gdyż oczywiście  $p \mid p \cdot \prod_{q \in P \setminus \{p\}} q = \prod_{q \in P} q$ . Fakt 1.4 prowadziłby do wniosku, że  $p = 1$ , co jest sprzeczne z Lematem 1.26 (1).  $\square$

STWIERDZENIE 1.30.

Niech  $a_1, \dots, a_n, n \in \mathbb{N}$ , będą liczbami całkowitymi. Jeśli  $p$  jest liczbą pierwszą i  $p \mid \prod_{i \in [1, n]} a_i$ , to istnieje  $i \in [1, n]$  takie, że  $p \mid a_i$ .

DOWÓD.

Udowodnimy tezę przez indukcję ze względu na  $n$ . Zauważmy, że ponieważ  $p > 1$  na mocy Lematu 1.26 (1), więc  $\prod_{i \in [1, n]} a_i \neq 1$  na mocy Faktu 1.4. W szczególności,  $n > 0$ .

Jeśli  $n = 1$ , to teza jest oczywista.

Załóżmy zatem, że  $n > 1$ . Jeśli  $p \nmid a_n$ , to  $\gcd(p, a_n) = 1$  na mocy Lematu 1.26 (2). Korzystając z Wniosku 1.22 otrzymujemy, że  $p \mid \prod_{i \in [1, n-1]} a_i$ , zatem teza wynika z założenia indukcyjnego.  $\square$



TWIERDZENIE 1.31 (ZASADNICZE TWIERDZENIE ARYTMETYKI).

Jeśli  $a$  jest dodatnią liczbą całkowitą, to istnieją jednoznacznie wyznaczone skończony podzbiór  $P$  zbioru liczb pierwszych oraz funkcja  $\alpha : P \rightarrow \mathbb{N}_+$  takie, że

$$a = \prod_{p \in P} p^{\alpha(p)}.$$

DOWÓD.

1° Istnienie.

Z Lematu 1.27 wiemy, że istnieją liczby pierwsze  $p_1, \dots, p_n$ ,  $n \in \mathbb{N}$ , takie, że

$$a = \prod_{i \in [1, n]} p_i.$$

Kładziemy  $P := \{p_1, \dots, p_n\}$  i

$$\alpha(p) := \#\{i \in [1, n] : p_i = p\} \quad (p \in P).$$

2° Jednoznaczność.

Przypuśćmy, że  $P$  i  $P'$  są skończonymi podzbiorami zbioru liczb pierwszych oraz  $\alpha : P \rightarrow \mathbb{N}_+$  i  $\alpha' : P' \rightarrow \mathbb{N}_+$  takimi, że

$$\prod_{p \in P} p^{\alpha(p)} = \prod_{p \in P'} p^{\alpha'(p)}.$$

Przez indukcję na  $\sum_{p \in P} \alpha(p)$  udowodnimy, że  $P = P'$  i  $\alpha = \alpha'$ .

Jeśli  $\sum_{p \in P} \alpha(p) = 0$ , to  $P = \emptyset$ , więc  $\prod_{p \in P} p^{\alpha(p)} = 1$ . Stąd  $\prod_{p \in P'} p^{\alpha'(p)} = 1$ , więc  $P' = \emptyset = P$ . Ponadto  $\alpha = \emptyset = \alpha'$ .

Założmy zatem, że  $\sum_{p \in P} \alpha(p) > 0$ . Wtedy  $P \neq \emptyset$ . Wybierzmy  $q \in P$ . Ze Stwierdzenia 1.30 wiemy, że istnieje  $q' \in P'$  takie, że  $q \mid q'$ , a więc  $q = q'$  na mocy Lematu 1.26. Wtedy

$$q^{\alpha(q)-1} \cdot \prod_{p \in P \setminus \{q\}} p^{\alpha(p)} = q'^{\alpha(q')-1} \cdot \prod_{p \in P' \setminus \{q'\}} p^{\alpha'(p)}.$$

więc teza wynika z założenia indukcyjnego.

FAKT 1.32.

Niech  $a$  i  $b$  będą dodatnimi liczbami całkowitymi. Jeśli

$$a = \prod_{p \in P} p^{\alpha(p)} \quad \text{i} \quad b = \prod_{p \in P} p^{\beta(p)}$$

dla pewnych zbioru skończonego  $P \subseteq \mathbb{P}$  i funkcji  $\alpha, \beta : P \rightarrow \mathbb{N}$ , to  $b \mid a$  wtedy i tylko wtedy, gdy  $\beta(p) \leq \alpha(p)$  dla każdej liczby  $p \in P$ .

Dowód.

Założmy najpierw, że  $\beta(p) \leq \alpha(p)$  dla każdej liczby  $p \in P$ . Jeśli

$$c := \prod_{p \in P} p^{\alpha(p) - \beta(p)},$$

to  $a = b \cdot c$ , więc  $b \mid a$ .

Założmy teraz, że  $b \mid a$ . Ustalmy liczbę całkowitą  $c$  taką, że  $a = b \cdot c$ . Wtedy  $c > 0$ , więc na mocy Twierdzenia 1.31 istnieją skończony podzbiór  $P'$  zbioru liczb pierwszych oraz funkcja  $\gamma : P' \rightarrow \mathbb{N}_+$  takie, że

$$c = \prod_{p \in P'} p^{\gamma(p)}.$$

Definiujemy funkcje  $\alpha', \beta', \gamma' : P \cup P' \rightarrow \mathbb{N}$  wzorami

$$\alpha'(p) := \begin{cases} \alpha(p) & \text{jeśli } p \in P, \\ 0 & \text{jeśli } p \notin P, \end{cases} \quad (p \in P \cup P'),$$

$$\beta'(p) := \begin{cases} \beta(p) & \text{jeśli } p \in P, \\ 0 & \text{jeśli } p \notin P, \end{cases} \quad (p \in P \cup P'),$$

i

$$\gamma'(p) := \begin{cases} \gamma(p) & \text{jeśli } p \in P', \\ 0 & \text{jeśli } p \notin P', \end{cases} \quad (p \in P \cup P').$$

Wtedy

$$\prod_{p \in P \cup P'} p^{\alpha'(p)} = a = b \cdot c = \prod_{p \in P \cup P'} p^{\beta'(p) + \gamma'(p)}.$$

Z Twierdzenia 1.31 otrzymujemy, że  $\alpha'(p) = \beta'(p) + \gamma'(p)$  dla każdej liczby  $p \in P \cup P'$ . W szczególności  $\alpha'(p) \geq \beta'(p)$  dla każdej liczby  $p \in P$ .

**FAKT 1.33.**

Niech  $a$  i  $b$  będą dodatnimi liczbami całkowitymi. Jeśli

$$a = \prod_{p \in P} p^{\alpha(p)} \quad \text{i} \quad b = \prod_{p \in P} p^{\beta(p)}$$

dla pewnych zbioru skończonego  $P \subseteq \mathbb{P}$  i funkcji  $\alpha, \beta : P \rightarrow \mathbb{N}$ , to

$$\gcd(a, b) = \prod_{p \in P} p^{\min\{\alpha(p), \beta(p)\}}.$$

DOWÓD.

Niech

$$I := \{c \in \mathbb{N}_+ : a \mid c \text{ i } b \mid c\}$$

oraz

$$I' := \{\gamma : P \rightarrow \mathbb{N} : \gamma(p) \leq \alpha(p) \text{ i } \gamma(p) \leq \beta(p) \text{ dla każdej liczby } p \in P\}.$$

W zbiorach  $I$  i  $I'$  definiujemy relacje porządku  $\preceq$  i  $\preceq'$  wzorami

$$c \preceq c' : \iff c \mid c' \quad (c, c' \in I)$$

i

$$\gamma \preceq' \gamma' : \iff \gamma(p) \leq \gamma'(p) \text{ dla każdej liczby } p \in P \quad (\gamma, \gamma' \in I').$$

Z Faktu 1.32 wynika, że funkcja  $F : I' \rightarrow I$  dana wzorem

$$F(\gamma) := \prod_{p \in P} p^{\gamma(p)} \quad (p \in P),$$

jest izomorfizmem zbiorów częściowo uporządkowanych. Ponieważ

$$(\max I')(p) = \min\{\alpha(p), \beta(p)\}$$

dla każdej liczby  $p \in P$ , więc

$$\gcd(a, b) = \max I = F(\max I') = \prod_{p \in P} p^{\min\{\alpha(p), \beta(p)\}}. \quad \square$$

UWAGA.

Niech  $\pi : \mathbb{N}_+ \rightarrow \mathbb{N}$  będzie funkcją zdefiniowaną wzorem

$$\pi(n) := \#\{p \in \mathbb{P} : p \leq n\} \quad (n \in \mathbb{N}_+).$$

Można pokazać, że

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \ln n} = 1.$$

1.4. KONGRUENCJE

DEFINICJA.

Niech  $n$  będzie niezerową liczbą całkowitą. Jeśli  $a$  i  $b$  są liczbami całkowitymi, to mówimy, że LICZBA  $a$  PRZYSTAJE DO LICZBY  $b$  MODULO  $n$  i piszemy  $a \equiv_n b$  (lub  $a \equiv b \pmod{n}$ ), jeśli  $n \mid a - b$ .

FAKT 1.34.

Niech  $n$  będzie niezerową liczbą całkowitą. Jeśli  $a$  i  $b$  są liczbami całkowitymi, to  $a \equiv_n b$  wtedy i tylko wtedy, gdy  $a \bmod n = b \bmod n$ .

DOWÓD.

Założmy najpierw, że  $a \equiv_n b$ . Wtedy istnieje liczba całkowita  $q$  taka, że  $a - b = q \cdot n$ . Korzystając ze Stwierdzenia 1.13 otrzymujemy, że

$$a = b + q \cdot n = (b \operatorname{div} n + q) \cdot n + b \bmod n.$$

Ponieważ  $0 \leq b \bmod n < |n|$  na mocy Stwierdzenia 1.13, więc Wniosek 1.15 implikuje, że  $a \bmod n = b \bmod n$ .

Założmy teraz, że  $a \bmod n = b \bmod n$ . Korzystając ze Stwierdzenia 1.13 otrzymujemy, że

$$\begin{aligned} a - b &= ((a \operatorname{div} n) \cdot n + (a \bmod n)) - ((b \operatorname{div} n) \cdot n + (b \bmod n)) \\ &= (a \operatorname{div} n - b \operatorname{div} n) \cdot n, \end{aligned}$$

a więc  $a \equiv_n b$ . □

WNIOSEK 1.35.

Niech  $n$  będzie liczbą całkowitą taką, że  $n \neq 0$ .

- (1) Jeśli  $a$  jest liczbą całkowitą, to  $a \equiv_n a$ .
- (2) Jeśli  $a$  i  $b$  są liczbami całkowitymi i  $a \equiv_n b$ , to  $b \equiv_n a$ .
- (3) Jeśli  $a$ ,  $b$  i  $c$  są liczbami całkowitymi,  $a \equiv_n b$  i  $b \equiv_n c$ , to  $a \equiv_n c$ .

DOWÓD.

Wynika natychmiast z Faktu 1.34. □

LEMAT 1.36.

Niech  $n$  będzie niezerową liczbą całkowitą.

- (1) Jeśli  $a$ ,  $b$ ,  $c$  i  $d$  są liczbami całkowitymi takimi, że  $a \equiv_n b$  oraz  $c \equiv_n d$ , to

$$a \pm c \equiv_n b \pm d \quad \text{i} \quad a \cdot c \equiv_n b \cdot d.$$

- (2) Jeśli  $a$ ,  $b$  i  $c$  są liczbami całkowitymi takimi, że  $a \cdot c \equiv_n b \cdot c$  i  $\operatorname{gcd}(c, n) = 1$ , to  $a \equiv_n b$ .

- (3) Jeśli  $a, b$  i  $m$  są liczbami całkowitymi takimi, że  $m \neq 0$ , to  $m \cdot a \equiv_{m \cdot n} m \cdot b$  wtedy i tylko wtedy, gdy  $a \equiv_n b$ .

Dowód.

- (1) Ponieważ

$$(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$$

i

$$a \cdot c - b \cdot d = (a - b) \cdot c + (c - d) \cdot b$$

więc teza wynika z Faktów 1.7 i 1.8.

- (2) Teza wynika z Wniosku 1.22.

- (3) Teza wynika z Faktu 1.9. □

STWIERDZENIE 1.37.

Niech  $a, b$  i  $n$  będą liczbami całkowitymi takimi, że  $n \neq 0$ , i  $d := \gcd(a, n)$ .

- (1) Jeśli  $d \nmid b$ , to nie istnieje liczba całkowita  $x$  taka, że  $a \cdot x \equiv_n b$ .  
 (2) Jeśli  $d \mid b$ , to istnieje liczba całkowita  $x$  taka, że  $a \cdot x \equiv_n b$ . Ponadto, jeśli  $k$  jest liczbą całkowitą taką, że  $k \cdot a \equiv_n d$ , to

$$\{x \in \mathbb{Z} : a \cdot x \equiv_n b\} = \{x \in \mathbb{Z} : x \equiv_{n/d} (b/d) \cdot k\}.$$

Dowód.

- (1) Przypuśćmy, że istnieje liczba całkowita  $x$  taka, że  $a \cdot x \equiv_n b$ . Z Faktu 1.2 wynika, że  $a \cdot x \equiv_d b$ . Ponieważ  $d \mid a$ , więc  $a \cdot x \equiv_d 0$  na mocy Lematu 1.36 (1). Stąd

$$b \equiv_d a \cdot x \equiv_d 0.$$

- (2) Zauważmy, że liczba  $k$  istnieje na mocy Wniosku 1.19. Przypuśćmy najpierw, że  $x$  jest liczbą całkowitą taką, że  $x \equiv_{n/d} (b/d) \cdot k$ . Wtedy  $d \cdot x \equiv_n b \cdot k$  na mocy Lematu 1.36 (3). Korzystając z Lematu 1.36 (1) otrzymujemy, że

$$a \cdot x = (a/d) \cdot d \cdot x \equiv_n (a/d) \cdot b \cdot k = a \cdot k \cdot (b/d) \equiv_n d \cdot (b/d) = b.$$

Niech  $c := (b/d) \cdot k$ . Z powyższego rachunku wiemy, że  $a \cdot c \equiv_n b$ . Stąd, jeśli  $x$  jest liczbą całkowitą taką, że  $a \cdot x \equiv_n b$ , to

$$d \cdot x \equiv_n k \cdot a \cdot x \equiv_n k \cdot b = d \cdot c,$$

zatem Lemat 1.36 (3) implikuje, że

$$x \equiv_{n/d} c.$$

LEMAT 1.38.

Niech  $a, b, n_1, \dots, n_k$  będą liczbami całkowitymi takimi, że  $n_i \neq 0$  dla każdego  $i \in [1, k]$ . Jeśli  $\gcd(n_i, n_j) = 1$  dla wszystkich  $i, j \in [1, k]$  takich, że  $i \neq j$ , oraz  $a \equiv_{n_i} b$  dla wszystkich  $i \in [1, k]$ , to  $a \equiv_n b$ , gdzie  $n := \prod_{i \in [1, k]} n_i$ .

DOWÓD.

Wynika z Wniosku 1.24. □

TWIERDZENIE 1.39 (CHIŃSKIE TWIERDZENIE O RESZTACH).

Założmy, że  $n_1, \dots, n_k$  są dodatnimi liczbami całkowitymi i  $\gcd(n_i, n_j) = 1$  dla wszystkich  $i, j \in [1, k]$  takich, że  $i \neq j$ . Jeśli

$$n := \prod_{i \in [1, k]} n_i,$$

to funkcja  $\Phi : [0, n - 1] \rightarrow [0, n_1 - 1] \times \dots \times [0, n_k - 1]$  dana wzorem

$$\Phi(a) := (a \bmod n_1, \dots, a \bmod n_k) \quad (a \in [0, n - 1]),$$

jest bijekcją.

DOWÓD.

Ponieważ

$$\#[0, n - 1] = n = \prod_{i \in [1, k]} n_i = \#[0, n_1 - 1] \times \dots \times [0, n_k - 1],$$

więc wystarczy pokazać, że funkcja  $\Phi$  jest różnowartościowa. W tym celu ustalmy liczby  $a, b \in [0, n - 1]$  i założmy, że  $\Phi(a) = \Phi(b)$ . Wtedy  $a \equiv_{n_i} b$  dla każdego  $i \in [1, k]$  na mocy Faktu 1.34. Korzystając z Lematu 1.38, otrzymujemy zatem, że  $a \equiv_n b$ , a więc  $a \bmod n = b \bmod n$  na mocy Faktu 1.34. Ponieważ

$$a \bmod n = a \quad \text{i} \quad b \bmod n = b$$

mocy Wniosku 1.15, więc

$$a = a \bmod n = b \bmod n = b. \quad \square$$

STWIERDZENIE 1.40.

Założmy, że  $n_1, \dots, n_k$  są dodatnimi liczbami całkowitymi i  $\gcd(n_i, n_j) = 1$  dla wszystkich  $i, j \in [1, k]$  takich, że  $i \neq j$ . Niech

$$m_i := \prod_{j \in [1, k] \setminus \{i\}} n_j \quad (i \in [1, k])$$

## MATEMATYKA DYSKRETNA

oraz  $b_1, \dots, b_k$  będą liczbami całkowitymi. Jeśli dla każdego  $i \in [1, k]$   $l_i$  jest liczbą całkowitą taką, że  $l_i \cdot m_i \equiv_{n_i} 1$ , i

$$x := \sum_{i \in [1, k]} b_i \cdot l_i \cdot m_i,$$

to

$$x \bmod n_i = b_i \bmod n_i$$

dla każdego  $i \in [1, k]$ .

**DOWÓD.**

Ustalmy  $i \in [1, k]$ . Ponieważ  $m_j \equiv_{n_i} 0$  dla każdego  $j \in [1, k] \setminus \{i\}$ , więc korzystając z Lematu 1.36 (1) otrzymujemy, że

$$x \equiv_{n_i} b_i \cdot l_i \cdot m_i \equiv_{n_i} b_i \cdot 1 = b_i.$$

Stąd  $x \bmod n_i = b_i \bmod n_i$  na mocy Faktu 1.34.  $\square$

**UWAGA.**

Niech  $n_1, \dots, n_k$  będą liczbami całkowitymi takimi, że  $n_i \neq 0$  dla każdego  $i \in [1, k]$  oraz  $\gcd(n_i, n_j) = 1$  dla wszystkich  $i, j \in [1, k]$  takich, że  $i \neq j$ . Jeśli

$$m_i := \prod_{j \in [1, k] \setminus \{i\}} n_j \quad (i \in [1, k]),$$

to dla każdego  $i \in [1, k]$  istnieje liczba całkowita  $l_i$  taka, że  $l_i \cdot m_i \equiv_{n_i} 1$ .

**DOWÓD.**

Z Wniosku 1.23 wiemy, że  $\gcd(m_i, n_i) = 1$  dla każdego  $i \in [1, k]$ , zatem teza wynika ze Stwierdzenia 1.37 (2).  $\square$

### 1.5. FUNKCJA I TWIERDZENIE EULERA

**DEFINICJA.**

FUNKCJĄ EULERA nazywamy funkcję  $\varphi : \mathbb{N}_+ \rightarrow \mathbb{N}_+$  zdefiniowaną wzorem

$$\varphi(n) := \#U_n \quad (n \in \mathbb{N}_+),$$

gdzie

$$U_n := \{a \in [0, n-1] : \gcd(a, n) = 1\} \quad (n \in \mathbb{N}_+).$$

**PRZYKŁAD.**

$$\varphi(1) = 1.$$

PRZYKŁAD.

Jeśli  $p$  jest liczbą pierwszą, to  $\varphi(p) = p - 1$ .

PRZYKŁAD.

$\varphi(12) = \#\{1, 5, 7, 11\} = 4$ .

LEMAT 1.41.

Jeśli  $p$  jest liczbą pierwszą i  $k$  jest dodatnią liczbą całkowitą, to

$$\varphi(p^k) = p^k - p^{k-1} = (p - 1) \cdot p^{k-1} = p^k \cdot \left(1 - \frac{1}{p}\right).$$

DOWÓD.

Z Faktu 1.33 wiemy, że jeśli  $a$  jest liczbą całkowitą, to  $\gcd(a, p^k) \neq 1$  wtedy i tylko wtedy, gdy  $p \mid a$ . Stąd wynika, że

$$\begin{aligned} \varphi(p^k) &= \#\{a \in [0, p^k - 1] : \gcd(a, p^k) = 1\} \\ &= \#[0, p^k - 1] - \#\{a \in [0, p^k - 1] : p \mid a\} = p^k - p^{k-1}, \end{aligned}$$

co kończy dowód. □

LEMAT 1.42.

Jeśli  $n_1, \dots, n_k$  są dodatnimi liczbami całkowitymi takimi, że  $\gcd(n_i, n_j) = 1$  dla wszystkich  $i, j \in [1, k]$  takich, że  $i \neq j$ , to

$$\varphi\left(\prod_{i \in [1, k]} n_i\right) = \prod_{i \in [1, k]} \varphi(n_i).$$

DOWÓD.

Niech

$$n := \prod_{i \in [1, k]} n_i.$$

Definiujemy funkcję  $\Phi : [0, n - 1] \rightarrow [0, n_1 - 1] \times \dots \times [0, n_k - 1]$  wzorem

$$\Phi(a) := (a \bmod n_1, \dots, a \bmod n_k) \quad (a \in [0, n - 1]).$$

Z Twierdzenia 1.39 wiemy, że funkcja ta jest bijekcją. Ponadto, jeśli  $a \in [0, n - 1]$ , to korzystając z Wniosku 1.23 i Lematu 1.20 otrzymujemy, że

$$\begin{aligned} \gcd(a, n) = 1 &\iff \forall_{i \in [1, k]} \gcd(a, n_i) = 1 \\ &\iff \forall_{i \in [1, k]} \gcd(a \bmod n_i, n_i) = 1. \end{aligned}$$

Zatem funkcja  $\Phi$  indukuje bijekcję

$$U_n \rightarrow U_{n_1} \times \dots \times U_{n_k}. \quad \square$$



WNIOSEK 1.43.

Niech  $P$  będzie skończonym podzbiorem zbioru liczb pierwszych i  $\alpha : P \rightarrow \mathbb{N}_+$ . Jeśli

$$n := \prod_{p \in P} p^{\alpha(p)},$$

to

$$\varphi(n) = \prod_{p \in P} (p^{\alpha(p)} - p^{\alpha(p)-1}) = \prod_{p \in P} (p-1) \cdot p^{\alpha(p)-1} = n \cdot \prod_{p \in P} \left(1 - \frac{1}{p}\right).$$

DOWÓD.

Dla liczby  $p \in P$  definiujemy dodatnią liczbę całkowitą  $n_p$  wzorem  $n_p := p^{\alpha(p)}$ . Z Faktu 1.33 wiemy, że  $\gcd(n_p, n_q) = 1$  dla wszystkich liczb  $p, q \in P$  takich, że  $p \neq q$ . Korzystając z Lematu 1.42 otrzymujemy, że

$$\varphi(n) = \varphi\left(\prod_{p \in P} n_p\right) = \prod_{p \in P} \varphi(n_p),$$

zatem teza wynika z Lematu 1.41. □

WNIOSEK 1.44.

Przypuśćmy, że  $p$  i  $q$  są różnymi liczbami pierwszymi. Jeśli  $n := p \cdot q$ , to znajomość liczb  $p$  i  $q$  jest równoważna znajomości liczb  $n$  i  $\varphi(n)$ .

DOWÓD.

Wystarczy zauważyć, że liczby  $p$  i  $q$  spełniają warunki

$$p \cdot q = n \quad \text{i} \quad p + q = n - \varphi(n) + 1,$$

a więc są rozwiązaniami równania

$$x^2 - (n - \varphi(n) + 1)x + n = 0. \quad \square$$

TWIERDZENIE 1.45 (EULER).

Jeśli  $a$  i  $n$  są liczbami całkowitymi takimi, że  $n > 0$  i  $\gcd(a, n) = 1$ , to

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

DOWÓD.

Definiujemy funkcję  $\Phi : U_n \rightarrow U_n$  wzorem

$$\Phi(b) := (a \cdot b) \bmod n \quad (b \in U_n).$$

Zauważmy najpierw, że funkcja  $\Phi$  jest poprawnie określona. Istotnie, jeśli  $b \in U_n$ , to  $\gcd(b, n) = 1$ , więc  $\gcd(a \cdot b, n) = 1$  na mocy Wniosek 1.23. Korzystając z Lematu 1.20 wnioskujemy, że  $\gcd(\Phi(b), n) = 1$ , a więc  $\Phi(b) \in U_n$ .

Pokażemy teraz, że funkcja  $\Phi$  jest bijekcją. W tym celu wystarczy uzasadnić, że funkcja  $\Phi$  jest różnowartościowa. Przypuśćmy więc, że  $b, c \in U_n$  i  $\Phi(b) = \Phi(c)$ . Wtedy  $a \cdot b \equiv_n a \cdot c$  na mocy Faktu 1.34, więc  $b \equiv_n c$  na mocy Lemat 1.36 (2). Korzystając ponownie z Faktu 1.34, otrzymujemy, że  $b \bmod n = c \bmod n$ . Wykorzystując dodatkowo Wniosek 1.15, wiemy, że  $b = b \bmod n$  i  $c = c \bmod n$ , gdyż  $b, c \in [0, n - 1]$ . Ostatecznie otrzymujemy, że

$$b = b \bmod n = c \bmod n = c.$$

Ponieważ funkcja  $\Phi$  jest bijekcją, więc korzystając z Lematu 1.36 (1) otrzymujemy, że

$$\prod_{b \in U_n} b = \prod_{b \in U_n} \Phi(b) \equiv_n \prod_{b \in U_n} (a \cdot b) = a^{\varphi(n)} \prod_{b \in U_n} b.$$

Ponieważ  $\gcd(\prod_{b \in U_n} b, n) = 1$  na mocy Wniosku 1.23, więc teza wynika z Lematu 1.36 (2).  $\square$

WNIOSEK 1.46.

Jeśli  $p$  jest liczbą pierwszą,  $a$  jest liczbą całkowitą i  $p \nmid a$ , to  $a^{p-1} \equiv_p 1$ .  $\square$

WNIOSEK 1.47.

Jeśli  $p$  jest liczbą pierwszą i  $a$  jest liczbą całkowitą, to  $a^p \equiv_p a$ .

DOWÓD.

Jeśli  $p \nmid a$ , to  $a^p = a \cdot a^{p-1} \equiv_p a \cdot 1 = a$  na mocy Wniosku 1.46. Gdy  $p \mid a$ , to  $a^p \equiv_p 0 \equiv_p a \pmod{p}$ .  $\square$

## 1.6. ZASTOSOWANIE TEORII LICZB W KRYPTOGRAFII

Celem kryptografii jest opracowanie metod przekazywania wiadomości, które uniemożliwią jej odczytanie osobom niepowołanym nawet w przypadku jej przechwycenia.

ZAŁOŻENIE.

Utożsamiamy symbole używane do zapisu tekstu (litery, bądź ich pary, trójki ..., itd.) z elementami zbioru  $[0, N - 1]$  dla pewnej dodatniej liczby całkowitej  $N$ .

DEFINICJA.

SYSTEMEM KRYPTOGRAFICZNYM nazywamy każdą trójkę  $(P, C, f)$  składającą się ze zbioru  $P$  symboli używanych do zapisu tekstu jawnego, zbioru  $C$

## MATEMATYKA DYSKRETNA

symboli służących do zapisu tekstu zakodowanego oraz bijekcji  $f : P \rightarrow C$  zwanej FUNKCJĄ SZYFRUJĄCĄ. Funkcję odwrotną  $f^{-1} : C \rightarrow P$  nazywamy FUNKCJĄ DESZYFRUJĄCĄ.

PRZYKŁAD (SZYFR CEZARA).

Ustalmy dodatnią liczbę całkowitą  $N$  oraz liczbę  $k \in [0, N - 1]$ . Niech  $P := [0, N - 1] := C$ . Definiujemy funkcję  $f : P \rightarrow C$  wzorem

$$f(a) := (a + k) \bmod N \quad (a \in [0, N - 1]).$$

Funkcja odwrotna  $f^{-1} : C \rightarrow P$  dana jest wzorem

$$f^{-1}(b) := (b - k) \bmod N \quad (b \in [0, N - 1]).$$

Liczbę  $k$  nazywamy KLUCZEM SZYFRUJĄCYM.

UWAGA.

Szyfr Cezara jest przykładem SZYFRU SYMETRYCZNEGO — znajomość klucza szyfrującego oznacza możliwość odszyfrowania wiadomości.

PRZYKŁAD (SZYFR R(IVEST)S(HAMIR)A(DLEMAN)).

Niech  $p$  i  $q$  będą (dużymi) różnymi liczbami pierwszymi,  $n := p \cdot q$ , oraz wybierzmy (losowo) liczbę  $e \in [2, \varphi(n) - 1]$  taką, że  $\gcd(e, \varphi(n)) = 1$ . Definiujemy zbiory  $P$  i  $C$  wzorami

$$P := [0, n - 1] =: C$$

oraz funkcję  $f : P \rightarrow C$  wzorem

$$f(a) := a^e \bmod n \quad (a \in [0, n - 1]).$$

Parę  $(n, e)$  nazywamy KLUCZEM SZYFRUJĄCYM. KLUCZEM DESZYFRUJĄCYM nazywamy parę  $(n, d)$ , gdzie liczba  $d \in [2, \varphi(n) - 1]$  spełnia warunek  $d \cdot e \equiv_{\varphi(n)} 1$  (liczba taka istnieje na mocy Stwierdzenia 1.37 (2)).

LEMAT 1.48.

Jeśli  $p$  i  $q$  są różnymi liczbami pierwszymi,  $n := p \cdot q$ ,  $d, e \in \mathbb{N}_+$  oraz  $d \cdot e \equiv_{\varphi(n)} 1$ , to  $a^{d \cdot e} \equiv_n a$  dla dowolnej liczby całkowitej  $a$ .

DOWÓD.

Z Wniosku 1.46 wynika, że jeśli  $\gcd(a, p) = 1$ , to  $a^{p-1} \equiv_p 1$ , więc  $a^{\varphi(n)} \equiv_p 1$ , zatem również  $a^{d \cdot e - 1} \equiv_p 1$ . Stąd  $a^{d \cdot e} \equiv_p a$ . Ta kongruencja jest również prawdziwa, gdy  $\gcd(a, p) \neq 1$ , gdyż w tym przypadku  $a^{d \cdot e} \equiv_p 0 \equiv_p a$ . Analogicznie pokazujemy, że  $a^{d \cdot e} \equiv_q a$ , więc teza wynika Lematu 1.38.  $\square$

UWAGA.

Szyfr RSA jest przykładem SZYFRU ASYMETRYCZNEGO — znajomość klucza szyfrującego nie wystarcza do odszyfrowania wiadomości. Istotnie, wyliczenie liczby  $d$  wymaga znajomości liczby  $\varphi(n)$ , co jest równoważne znajomości rozkładu liczby  $n$  na czynniki pierwsze. Dzięki tej własności szyfr RSA może być stosowany jako SYSTEM Z KLUCZEM PUBLICZNYM — nie występuje problem dystrybucji kluczy.

2. ELEMENTY KOMBINATORYKI

ZAŁOŻENIE.

Rozważane zbiory są skończone.

2.1. PODSTAWOWE OBIEKTY KOMBINATORYCZNE

DEFINICJA.

Jeśli  $n$  jest nieujemną liczbą całkowitą oraz  $X$  jest zbiorem, to CIĄGIEM DŁUGOŚCI  $n$  ELEMENTÓW ZBIORU  $X$  nazywamy każdą funkcję  $a : [1, n] \rightarrow X$ . Jeśli  $a$  jest ciągiem długości  $n$ , to piszemy  $a = (a(1), \dots, a(n))$ .

UWAGA.

Jeśli  $X$  jest zbiorem, to istnieje dokładnie  $|X|^n$  ciągów długości  $n$  elementów zbioru  $X$  dla każdej nieujemnej liczby całkowitej  $n$  (gdzie  $0^0 := 1$ ). W szczególności, dla dowolnego zbioru istnieje dokładnie 1 ciąg długości 0 elementów tego zbioru — ciąg pusty. Z drugiej strony, nie ma żadnego ciągu długości  $n$  elementów zbioru pustego, jeśli  $n$  jest dodatnią liczbą całkowitą.

DEFINICJA.

Jeśli  $X$  jest zbiorem, to PERMUTACJĄ elementów zbioru  $X$  nazywamy każdy różnowartościowy ciąg długości  $|X|$  elementów zbioru  $X$ . Zbiór wszystkich permutacji elementów zbioru  $X$  oznaczamy  $P_X$ .

STWIERDZENIE 2.1.

Jeśli  $X$  jest zbiorem, to  $|P_X| = |X|!$ .

DOWÓD.

Dowód będzie indukcyjny ze względu na  $n := |X|$ . Dla  $n = 0$  teza jest oczywista. Przypuśćmy teraz, że  $n > 0$ . Definiujemy funkcję  $f : P_X \rightarrow \bigcup_{x \in X} P_{X \setminus \{x\}}$  wzorem

$$f(a) := (a(1), \dots, a(n-1)) \quad (a \in P_X).$$

Funkcja  $f$  jest bijekcją. Z założenie indukcyjnego wiemy, że  $|P_{X \setminus \{x\}}| = (n-1)!$  dla każdego elementu  $x$  zbioru  $X$ , więc

$$|P_X| = \sum_{x \in X} |P_{X \setminus \{x\}}| = \sum_{x \in X} (n-1)! = n \cdot (n-1)! = n!. \quad \square$$

STWIERDZENIE 2.2.

Jeśli  $n$  jest dodatnią liczbą całkowitą, to

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{n^{n+1}}{e^{n-1}}.$$

Dowód.

Przypomnijmy, że dla dowolnej dodatniej liczby całkowitej  $k$  mamy nierówności

$$\left(\frac{k+1}{k}\right)^k \leq e \leq \left(\frac{k+1}{k}\right)^{k+1}.$$

Wykorzystując te nierówności otrzymujemy, że

$$\begin{aligned} e^{n-1} &\geq \prod_{k \in [1, n-1]} \left(\frac{k+1}{k}\right)^k = \prod_{k \in [1, n-1]} \frac{1}{k^k} \cdot \prod_{k \in [1, n-1]} (k+1)^k \\ &= \prod_{k \in [1, n-1]} \frac{1}{k^k} \cdot \prod_{k \in [2, n]} k^{k-1} = \prod_{k \in [1, n-1]} \frac{1}{k^k} \cdot \prod_{k \in [1, n]} k^{k-1} \\ &= \left(\prod_{k \in [1, n-1]} \frac{1}{k}\right) \cdot n^{n-1} = \frac{n^{n-1}}{(n-1)!} = \frac{n^n}{n!} \end{aligned}$$

i

$$\begin{aligned} e^{n-1} &\leq \prod_{k \in [1, n-1]} \left(\frac{k+1}{k}\right)^{k+1} = \prod_{k \in [1, n-1]} \frac{1}{k^{k+1}} \cdot \prod_{k \in [1, n-1]} (k+1)^{k+1} \\ &= \prod_{k \in [1, n-1]} \frac{1}{k^{k+1}} \cdot \prod_{k \in [2, n]} k^k = \prod_{k \in [1, n-1]} \frac{1}{k^{k+1}} \cdot \prod_{k \in [1, n]} k^k \\ &= \prod_{k \in [1, n-1]} \frac{1}{k} \cdot n^n = \frac{n^n}{(n-1)!} = \frac{n^{n+1}}{n!}, \end{aligned}$$

co kończy dowód. □

UWAGA.

Stirling udowodnił, że

$$\lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2 \cdot \pi \cdot n} \cdot \left(\frac{n}{e}\right)^n} = 1.$$

DEFINICJA.

Jeśli  $k$  jest nieujemną liczbą całkowitą oraz  $X$  jest zbiorem, to KOMBINACJĄ DŁUGOŚCI  $k$  ( $k$ -ELEMENTOWĄ) ELEMENTÓW ZBIORU  $X$  nazywamy każdy  $k$ -elementowy podzbiór zbioru  $X$ . Zbiór wszystkich kombinacji długości  $k$  elementów zbioru  $X$  oznaczamy  $C_{X,k}$ .

OZNACZENIE.

Jeśli  $n$  i  $k$  są nieujemnymi liczbami całkowitymi, to  $C_{n,k} := C_{[1,n],k}$ .

DEFINICJA.

Jeśli  $n$  i  $k$  są nieujemnymi liczbami całkowitymi, to SYMBOLEM NEWTONA  $n$  NAD  $k$  nazywamy

$$\binom{n}{k} := \begin{cases} \frac{n!}{(n-k)!k!} & \text{jeśli } k \in [0, n], \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

STWIERDZENIE 2.3.

Jeśli  $k$  jest nieujemną liczbą całkowitą oraz  $X$  jest zbiorem, to  $|C_{X,k}| = \binom{|X|}{k}$ .

DOWÓD.

Oczywiście  $C_{X,k} = \emptyset$ , gdy  $k > |X|$ . Dla  $k \leq |X|$  rozważmy funkcję  $f : P_X \rightarrow C_{X,k}$  daną wzorem

$$f(a) := a([1, k]) \quad (a \in P_X).$$

Wtedy

$$f^{-1}(A) = \{a \in P_X : (a(1), \dots, a(k)) \in P_A, (a(k+1), \dots, a(n)) \in P_{X \setminus A}\},$$

a więc  $|f^{-1}(A)| = k! \cdot (n-k)!$ , dla każdej kombinacji  $A \in C_{X,k}$ , co kończy dowód.  $\square$

UWAGA.

Przypomnijmy, że jeśli  $x_i$  i  $y_i$ ,  $i \in J$ , są elementami pierścienia przemiennego  $R$  oraz  $|J| < \infty$ , to

$$\prod_{i \in J} (x_i + y_i) = \sum_{I \subseteq J} \left( \prod_{i \in I} x_i \cdot \prod_{i \in J \setminus I} y_i \right).$$

WNIOSEK 2.4.

Jeśli  $x$  i  $y$  są elementami pierścienia przemiennego  $R$  oraz  $n \in \mathbb{N}$ , to

$$(x + y)^n = \sum_{k \in [0, n]} \binom{n}{k} \cdot x^k \cdot y^{n-k}.$$

DOWÓD.

Z powyższej uwagi otrzymujemy, że

$$(x + y)^n = \prod_{k \in [1, n]} (x + y) = \sum_{I \subseteq [1, n]} \left( \prod_{i \in I} x \cdot \prod_{i \in [1, n] \setminus I} y \right)$$

$$\begin{aligned}
 &= \sum_{I \subseteq [1, n]} \left( x^{|I|} \cdot y^{n-|I|} \right) = \sum_{k \in [0, n]} \sum_{I \in C_{n, k}} x^k \cdot y^{n-k} \\
 &= \sum_{k \in [0, n]} \binom{n}{k} \cdot x^k \cdot y^{n-k},
 \end{aligned}$$

co kończy dowód. □

## 2.2. METODA BIJEKTYWNA

UWAGA.

Zauważmy, że w dowodach Stwierżeń 2.1 i 2.3 liczyliśmy ilość obiektów kombinatorycznych konstruując funkcję pomiędzy rozważanym zbiorem oraz zbiorem, którego ilość elementów była znana. W „najlepszych” sytuacjach funkcja ta jest bijekcją, stąd tę metodę zliczania obiektów kombinatorycznych nazywamy METODĄ BIJEKTYWNA. Zilustrujemy teraz tę metodą kilkoma innymi przykładami.

STWIERDZENIE 2.5.

Jeśli  $n$  i  $k$  są dodatnimi liczbami całkowitymi, to

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

DOWÓD.

Lewa strona powyższej równości to liczba  $k$ -elementowych kombinacji zbioru  $[1, n]$ . Pierwszy wyraz po prawej stronie to liczba tych kombinacji, do których nie należy  $n$ , natomiast drugi wyraz po prawej stronie to liczba tych kombinacji, do których należy  $n$ .

Bardziej formalnie rozważmy funkcję  $f : C_{n, k} \rightarrow C_{n-1, k} \cup C_{n-1, k-1}$  daną wzorem

$$f(X) := \begin{cases} X & \text{jeśli } n \notin X, \\ X \setminus \{n\} & \text{jeśli } n \in X, \end{cases} \quad (X \in C_{n, k}).$$

Funkcja  $f$  jest poprawnie określona i jest bijekcją — funkcja odwrotna  $f^{-1} : C_{n-1, k} \cup C_{n-1, k-1} \rightarrow C_{n, k}$  dana jest wzorem

$$f^{-1}(Y) := \begin{cases} Y & \text{jeśli } Y \in C_{n-1, k}, \\ Y \cup \{n\} & \text{jeśli } Y \in C_{n-1, k-1}, \end{cases} \quad (Y \in C_{n-1, k} \cup C_{n-1, k-1}). \quad \square$$



UWAGA.

Powyższa równość pozwala wyliczać wartości  $\binom{n}{k}$  dla nieujemnych liczb całkowitych  $n$  i  $k$  rekurencyjnie z warunkami początkowymi:  $\binom{n}{0} = 1$  dla każdej nieujemnej liczby całkowitej  $n$  oraz  $\binom{0}{k} = 0$  dla każdej dodatniej liczby całkowitej  $k$  (lub  $\binom{n}{n} = 1$  dla każdej nieujemnej liczby całkowitej  $n$ ). Metoda ta nosi nazwę TRÓJKĄTA PASCALA.

DEFINICJA.

Dla nieujemnej liczby całkowitej  $k$  definiujemy wielomian  $\binom{T}{k} \in \mathbb{C}[T]$  wzorem

$$\binom{T}{k} := \frac{1}{k!} \cdot \prod_{i \in [0, k-1]} (T - i).$$

W szczególności  $\binom{T}{0} = 1$ .

UWAGA.

Jeśli  $k$  jest nieujemną liczbą całkowitą, to  $\deg \binom{T}{k} = k$  oraz pierwiastkami (jednokrotnymi) wielomianu  $\binom{T}{k}$  są liczby  $0, \dots, k - 1$ .

WNIOSEK 2.6.

Jeśli  $k$  jest dodatnią liczbą całkowitą, to

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

W szczególności, jeśli  $x$  jest liczbą zespoloną, to

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

DOWÓD.

Niech

$$F := \binom{T}{k} \quad \text{i} \quad G := \binom{T-1}{k} + \binom{T-1}{k-1}.$$

Stwierdzenie 2.5 implikuje, że  $F(n) = G(n)$  dla każdej dodatniej liczby całkowitej  $n$ , więc  $F = G$ .  $\square$

STWIERDZENIE 2.7.

Jeśli  $n$  jest nieujemną liczbą całkowitą oraz  $k \in [0, n]$ , to

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

Dowód.

Definiujemy funkcję  $f : C_{n,k} \rightarrow C_{n,n-k}$  wzorem

$$f(X) := [1, n] \setminus X \quad (X \in C_{n,k}).$$

Funkcja  $f$  jest poprawnie określona i jest bijekcją — funkcja odwrotna  $f^{-1} : C_{n,n-k} \rightarrow C_{n,k}$  dana jest wzorem

$$f^{-1}(Y) := [1, n] \setminus Y \quad (Y \in C_{n,n-k}). \quad \square$$

OZNACZENIE.

Jeśli  $X$  jest zbiorem, to

$$2^X := \{A : A \subseteq X\}.$$

STWIERDZENIE 2.8.

Jeśli  $X$  jest zbiorem, to  $|2^X| = 2^{|X|}$ .

Dowód.

Teza wynika z tego, że każdy podzbiór zbioru  $X$  jest wyznaczony przez swoją funkcję charakterystyczną.

Bardziej formalnie bez straty ogólności możemy założyć, że  $X = [1, n]$  dla pewnej nieujemnej liczby całkowitej  $n$ . Niech  $\mathcal{X}$  będzie zbiorem ciągów długości  $n$  elementów zbioru  $\{0, 1\}$ . Wiemy, że  $|\mathcal{X}| = 2^n$ . Definiujemy funkcję  $f : 2^X \rightarrow \mathcal{X}$  wzorem

$$(f(A))(i) := \begin{cases} 1 & \text{jeśli } i \in A, \\ 0 & \text{jeśli } i \notin A, \end{cases} \quad (i \in [1, n]).$$

Funkcja  $f$  jest bijekcją — funkcja odwrotna  $f^{-1} : \mathcal{X} \rightarrow 2^X$  dana jest wzorem

$$f^{-1}(a) := \{i \in [1, n] : a(i) = 1\} \quad (a \in \mathcal{X}). \quad \square$$

WNIOSEK 2.9.

Jeśli  $n$  jest nieujemną liczbą całkowitą, to

$$\sum_{k \in [0, n]} \binom{n}{k} = 2^n.$$

Dowód.

Obie strony odpowiadają dwóm różnym sposobów zliczenia podzbiorów zbioru  $n$ -elementowego.

Bardziej formalnie niech  $X := 2^{[1,n]}$ . Wtedy  $|X| = 2^n$  na mocy Stwierdzenia 2.8. Z drugiej strony  $X = \bigcup_{k \in [0,n]} C_{n,k}$  oraz  $C_{n,k} \cap C_{n,l} = \emptyset$  dla wszystkich indeksów  $k, l \in [0, n]$  takich, że  $k \neq l$ . Stąd

$$|X| = \sum_{k \in [0,n]} |C_{n,k}| = \sum_{k \in [0,n]} \binom{n}{k}$$

na mocy Stwierdzenia 2.3. □

**STWIERDZENIE 2.10 (WZÓR CHU–VANDERMONDE’A).**

Jeśli  $k, l$  i  $n$  są nieujemnymi liczbami całkowitymi, to

$$\sum_{i \in [0,n]} \binom{k}{i} \cdot \binom{l}{n-i} = \binom{k+l}{n}.$$

**Dowód.**

Prawa strona powyższej równości, to liczba  $n$ -elementowych kombinacji zbioru  $[1, k+l]$ . Lewa strona odpowiada takiemu sposobowi wyboru tych kombinacji, w których najpierw wybieramy część pochodzącą ze zbioru  $[1, k]$ , a potem tę pochodzącą ze zbioru  $[k+1, k+l]$ .

Bardziej formalnie niech

$$X := \{(A_1, A_2) \in 2^{[1,k]} \times 2^{[k+1, k+l]} : |A_1| + |A_2| = n\}$$

oraz

$$Y := \{B \in 2^{[1, k+l]} : |B| = n\}.$$

Ze Stwierdzenia 2.3 wiemy, że  $|Y| = \binom{k+l}{n}$ . Z drugiej strony  $X = \bigcup_{i \in [0,n]} X_i$ , gdzie

$$X_i := \{(A_1, A_2) \in X : |A_1| = i\} \quad (i \in [0, n]).$$

Ponieważ  $X_i \cap X_j = \emptyset$  dla wszystkich indeksów  $i, j \in [0, n]$  takich, że  $i \neq j$ , więc

$$|X| = \sum_{i \in [0,n]} |X_i| = \sum_{i \in [0,n]} \binom{k}{i} \cdot \binom{l}{n-i}$$

na mocy Stwierdzenia 2.3.

Rozważmy funkcję  $f : X \rightarrow Y$  daną wzorem

$$f(A_1, A_2) := A_1 \cup A_2 \quad ((A_1, A_2) \in X).$$

MATEMATYKA DYSKRETNA

Funkcja  $f$  jest poprawnie określona i jest bijekcją — funkcja odwrotna  $f^{-1} : Y \rightarrow X$  dana jest wzorem

$$f^{-1}(B) := (B \cap [1, k], B \cap [k + 1, k + l]) \quad (B \in Y). \quad \square$$

UWAGA.

Jeśli  $F, G \in \mathbb{C}[S, T]$  oraz  $F(k, l) = G(k, l)$  dla wszystkich liczb nieujemnych liczb całkowitych  $k$  i  $l$ , to  $F = G$ .

Dowód.

Wiemy, że

$$F = \sum_{i \in \mathbb{N}} F_i \cdot Y^i \quad \text{i} \quad G = \sum_{i \in \mathbb{N}} G_i \cdot Y^i$$

dla wielomianów  $F_i, G_i \in \mathbb{C}[X]$ ,  $i \in \mathbb{N}$ . Definiujemy wielomiany  $F^{(k)}, G^{(k)} \in \mathbb{C}[Y]$ ,  $k \in \mathbb{N}$ , wzorami

$$F^{(k)} := F(k, Y) := \sum_{i \in \mathbb{N}} F_i(k) \cdot Y^i$$

i

$$G^{(k)} := G(k, Y) := \sum_{i \in \mathbb{N}} G_i(k) \cdot Y^i.$$

Wtedy

$$F^{(k)}(l) = F(k, l) = G(k, l) = G^{(k)}(l)$$

dla wszystkich nieujemnych liczb całkowitych  $k$  i  $l$ , więc

$$F^{(k)} = G^{(k)}$$

dla wszystkich nieujemnych liczb całkowitych  $k$ . Innymi słowy

$$F_i(k) = G_i(k)$$

dla wszystkich nieujemnych liczb całkowitych  $k$  i  $i$ , więc

$$F_i = G_i$$

dla wszystkich nieujemnych liczb całkowitych  $i$ . Ostatecznie

$$F = \sum_{i \in \mathbb{N}} F_i \cdot Y^i = \sum_{i \in \mathbb{N}} G_i \cdot Y^i = G. \quad \square \square$$

WNIOSEK 2.11.

Jeśli  $x$  i  $y$  są liczbami zespolonymi oraz  $n$  jest nieujemną liczbą całkowitą, to

$$\sum_{i \in [0, n]} \binom{x}{i} \cdot \binom{y}{n-i} = \binom{x+y}{n}.$$

DOWÓD.

Definiujemy wielomiany  $F, G \in \mathbb{C}[X, Y]$  wzorami

$$F := \sum_{i \in [0, n]} \binom{X}{i} \cdot \binom{Y}{n-i} \quad \text{i} \quad G := \binom{X+Y}{n}.$$

Ze Stwierdzenia 2.10 wiemy, że  $F(k, l) = G(k, l)$  dla wszystkich nieujemnych liczb całkowitych  $k$  i  $l$ , skąd na mocy powyższej uwagi otrzymujemy tezę.  $\square$

DEFINICJA.

Niech  $m$  i  $n$  będą nieujemnymi liczbami całkowitymi. DROGĄ Z PUNKTU  $(0, 0)$  DO PUNKTU  $(m, n)$  nazywamy każdy ciąg  $a : [0, m+n] \rightarrow \mathbb{R}^2$  taki, że

- $a(0) = (0, 0)$ ,  $a(m+n) = (m, n)$ , oraz
- $a(i) = a(i-1) + \mathbf{x}$  lub  $a(i) = a(i-1) + \mathbf{y}$  dla każdego  $i \in [1, m+n]$ ,

gdzie  $\mathbf{x} := (1, 0)$  oraz  $\mathbf{y} := (0, 1)$ .

STWIERDZENIE 2.12.

Jeśli  $m$  i  $n$  są nieujemnymi liczbami całkowitymi, to dróg z punktu  $(0, 0)$  do punktu  $(m, n)$  jest  $\binom{m+n}{m}$ .

DOWÓD.

Zauważmy, że każda droga składa się ze  $m+n$  kroków:  $m$  kroków w prawo i  $n$  kroków w górę. Ponadto droga jest wyznaczona jednoznacznie przez wybór  $m$  kroków, które wykonamy w prawo.

Bardziej formalnie niech  $X$  będzie zbiorem wszystkich dróg z punktu  $(0, 0)$  do punktu  $(m, n)$ . Definiujemy funkcję  $f : C_{m+n, m} \rightarrow X$  wzorem

$$(f(A))(i) := |[1, i] \cap A| \cdot \mathbf{x} + |[1, i] \setminus A| \cdot \mathbf{y} \quad (A \in C_{m+n, m}, i \in [0, m+n]).$$

Innymi słowy,  $i$ -ty krok na drodze  $f(A)$  wykonujemy w kierunku  $\mathbf{x}$  wtedy i tylko wtedy, gdy  $i \in A$ . Funkcja  $f$  jest poprawnie określona oraz jest bijekcją — funkcja odwrotna  $f^{-1} : X \rightarrow C_{m+n, m}$  dana jest wzorem

$$f^{-1}(a) := \{i \in [1, m+n] : a(i) - a(i-1) = \mathbf{x}\} \quad (a \in X). \quad \square$$

WNIOSEK 2.13.

Jeśli  $n$  jest nieujemną liczbą całkowitą i  $k$  jest dodatnią liczbą całkowitą, to

$$\#\left\{x : [1, k] \rightarrow \mathbb{N} : \sum_{j \in [1, k]} x(j) = n\right\} = \binom{n+k-1}{n}.$$

DOWÓD.

Niech  $X$  będzie zbiorem dróg z punktu  $(0, 0)$  do punktu  $(k-1, n)$  oraz

$$Y := \left\{x : [1, k] \rightarrow \mathbb{N} : \sum_{j \in [1, k]} x(j) = n\right\}.$$

Ze Stwierdzenia 2.12 wiemy, że

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

Definiujemy funkcję  $f : X \rightarrow Y$  wzorem

$$(f(a))(j) := \#\{i \in [1, n+k-1] : \pi_1(a(i)) = j-1 = \pi_1(a(i-1))\} \\ (a \in X),$$

gdzie  $\pi_1 : \mathbb{R}^2 \rightarrow \mathbb{R}$  jest rzutowaniem na pierwszą współrzędną. Innymi słowy,  $j$ -ta współrzędna ciągu  $f(a)$  jest ilością kroków na drodze  $a$  w kierunku  $\mathbf{y}$  wykonanych „nad” liczbą  $j-1$ . Funkcja  $f$  jest poprawnie określona oraz jest bijekcją — funkcja odwrotna  $f^{-1} : Y \rightarrow X$  dana jest wzorem

$$(f^{-1}(x))(i) := (p_i(x), i - p_i(x)) \quad (x \in Y),$$

gdzie dla każdego indeksu  $i \in [0, n+k-1]$  definiujemy funkcję  $p_i : Y \rightarrow \mathbb{R}$  wzorem

$$p_i(x) := \max\left\{l \in [0, k] : l + \sum_{j \in [1, l]} x(j) \leq i\right\} \quad (x \in Y).$$

Innymi słowy, wykonujemy najpierw  $x(1)$  kroków („nad” 0) w kierunku  $\mathbf{y}$ , potem jeden krok w kierunku  $\mathbf{x}$ , następnie  $x(2)$  kroków („nad” 1) w kierunku  $\mathbf{y}$ , potem jeden krok w kierunku  $\mathbf{x}$ , itd. Zauważmy, że liczbę  $l + \sum_{j \in [1, l]} x(j)$  można interpretować jako numer kroku, w którym znajdziemy się nad liczbą  $l$ .  $\square$

2.3. REGUŁA WŁĄCZANIA I WYŁĄCZANIA

TWIERDZENIE 2.14 (REGUŁA WŁĄCZANIA I WYŁĄCZANIA).

Jeśli  $X_i, i \in J$ , są zbiorami i  $|J| < \infty$ , to

$$\left| \bigcup_{i \in J} X_i \right| = \sum_{\substack{I \subseteq J \\ I \neq \emptyset}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} X_i \right| = \sum_{k \in [1, |J|]} (-1)^{k-1} \cdot \sum_{I \in \mathcal{C}_{J,k}} \left| \bigcap_{i \in I} X_i \right|.$$

Dowód.

Tezę udowodnimy przez indukcję ze względu na  $|J|$ . Gdy  $|J| = 0$  lub  $|J| = 1$ , to teza jest oczywista. Podobnie łatwo udowodnić powyższy wzór, gdy  $|J| = 2$ . Załóżmy teraz, że  $|J| > 2$ . Ustalmy element  $j \in J$  i niech  $J' := J \setminus \{j\}$ . Korzystając z założenia indukcyjnego otrzymujemy, że

$$\begin{aligned} \left| \bigcup_{i \in J} X_i \right| &= \left| \left( \bigcup_{i \in J'} X_i \right) \cup X_j \right| = \left| \bigcup_{i \in J'} X_i \right| + |X_j| - \left| \left( \bigcup_{i \in J'} X_i \right) \cap X_j \right| \\ &= \left| \bigcup_{i \in J'} X_i \right| + |X_j| - \left| \bigcup_{i \in J'} (X_i \cap X_j) \right| = \\ &= \sum_{\substack{I \subseteq J' \\ I \neq \emptyset}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} X_i \right| + |X_j| - \sum_{\substack{I \subseteq J' \\ I \neq \emptyset}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} (X_i \cap X_j) \right| \\ &= \sum_{\substack{I \subseteq J' \\ I \neq \emptyset}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} X_i \right| + |X_j| + \sum_{\substack{I \subseteq J' \\ I \neq \emptyset}} (-1)^{|I|} \cdot \left| \left( \bigcap_{i \in I} X_i \right) \cap X_j \right| \\ &= \sum_{\substack{I \subseteq J \\ I \neq \emptyset, j \notin I}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} X_i \right| + \sum_{\substack{I \subseteq J \\ j \in I}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} X_i \right| \\ &= \sum_{\substack{I \subseteq J \\ I \neq \emptyset}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} X_i \right|, \end{aligned}$$

co kończy dowód. □

PRZYKŁAD.

Niech  $P$  będzie skończonym podzbiorem zbioru  $\mathbb{P}$  oraz  $\alpha : P \rightarrow \mathbb{N}_+$ . Jeśli  $n := \prod_{p \in P} p^{\alpha(p)}$ , to

$$\varphi(n) = n \cdot \prod_{p \in P} \left( 1 - \frac{1}{p} \right).$$

Dowód.

Dla liczby  $p \in P$  definiujemy zbiór  $X_p$  wzorem

$$X_p := \{m \in [0, n-1] : p \mid m\}$$

Zauważmy, że

$$\left| \bigcap_{p \in I} X_p \right| = \frac{n}{\prod_{p \in I} p}$$

dla dowolnego niepustego podzbioru  $I$  zbioru  $P$ . Stąd

$$\begin{aligned} \varphi(n) &= \left| [0, n-1] \setminus \bigcup_{p \in P} X_p \right| = n - \left| \bigcup_{p \in P} X_p \right| \\ &= n - \sum_{\substack{I \subseteq P \\ I \neq \emptyset}} (-1)^{|I|-1} \cdot \left| \bigcap_{p \in I} X_p \right| = n + \sum_{\substack{I \subseteq P \\ I \neq \emptyset}} (-1)^{|I|} \cdot \frac{n}{\prod_{p \in I} p} \\ &= n \cdot \sum_{I \subseteq P} \prod_{p \in I} \frac{(-1)^{|I|}}{p} = n \cdot \prod_{p \in P} \left( 1 - \frac{1}{p} \right), \end{aligned}$$

co kończy dowód. □

**OZNACZENIE.**

Dla  $n$  nieujemnej liczby całkowitej definiujemy zbiory  $P_n$  i  $P'_n$  wzorami  $P_n := P_{[1,n]}$  i

$$P'_n := \{a \in P_n : a(i) \neq i \text{ dla wszystkich liczb } i \in [1, n]\}.$$

**LEMAT 2.15.**

Jeśli  $n$  jest nieujemną liczbą całkowitą, to

$$|P'_n| = n! \cdot \sum_{k \in [0, n]} \frac{(-1)^k}{k!}.$$

**DOWÓD.**

Dla indeksu  $i \in [1, n]$  niech

$$X_i := \{a \in P_n : a(i) = i\}.$$

Korzystając ze Stwierdzenia 2.1, zauważmy, że

$$\left| \bigcap_{i \in I} X_i \right| = |P_{[1,n] \setminus I}| = (n - |I|)!$$

dla każdego niepustego podzbioru  $I$  zbioru  $[1, n]$ . Ponieważ  $|C_{n,k}| = \binom{n}{k}$  na mocy Stwierdzenia 2.3, więc

$$|P'_n| = \left| P_n \setminus \bigcup_{i \in [1, n]} X_i \right| = |P_n| - \left| \bigcup_{i \in [1, n]} X_i \right| =$$



$$\begin{aligned}
 &= n! - \sum_{k \in [1, n]} (-1)^{k-1} \cdot \sum_{I \in C_{n,k}} \left| \bigcap_{i \in I} X_i \right| \\
 &= n! + \sum_{k \in [1, n]} (-1)^k \cdot \sum_{I \in C_{n,k}} (n-k)! \\
 &= n! + \sum_{k \in [1, n]} (-1)^k \cdot \binom{n}{k} \cdot (n-k)! = (-1)^0 \cdot \frac{n!}{0!} + \sum_{k \in [1, n]} (-1)^k \cdot \frac{n!}{k!} \\
 &= n! \cdot \sum_{k \in [0, n]} \frac{(-1)^k}{k!},
 \end{aligned}$$

co kończy rozwiązanie. □

**OZNACZENIE.**

Dla liczby rzeczywistej  $x$  definiujemy liczbę całkowitą  $[x]$  wzorem

$$[x] := \begin{cases} [x] & \text{jeśli } x - [x] \leq \frac{1}{2}, \\ [x] + 1 & \text{jeśli } x - [x] > \frac{1}{2}. \end{cases}$$

**UWAGA.**

Jeśli  $x$  jest liczbą rzeczywistą,  $k$  jest liczbą całkowitą i  $|x - k| < \frac{1}{2}$ , to  $[x] = k$ .

**WNIOSEK 2.16.**

- (1) Jeśli  $n$  jest dodatnią całkowitą, to  $|P'_n| = \lfloor \frac{n!}{e} \rfloor$ .
- (2)  $\lim_{n \rightarrow \infty} \frac{|P'_n|}{|P_n|} = \frac{1}{e}$ .

**DOWÓD.**

Wiadomo, że

$$\left| \frac{1}{e} - \sum_{k \in [0, n]} \frac{(-1)^k}{k!} \right| < \frac{1}{(n+1)!},$$

i w szczególności

$$\lim_{n \rightarrow \infty} \sum_{k \in [0, n]} \frac{(-1)^k}{k!} = \frac{1}{e}.$$

To natychmiast implikuje drugą część wniosku. Ponadto,

$$\left| \frac{n!}{e} - |P'_n| \right| = \left| \frac{n!}{e} - n! \cdot \sum_{k \in [0, n]} \frac{(-1)^k}{k!} \right| < \frac{n!}{(n+1)!} = \frac{1}{n+1} \leq \frac{1}{2},$$

co kończy dowód. □

3. FUNKCJE TWORZĄCE

3.1. SZEREGI FORMALNE

DEFINICJA.

SZEREGIEM FORMALNYM nazywamy każdy ciąg  $\mathcal{A} : \mathbb{N} \rightarrow \mathbb{C}$ , który zapisujemy

$$\mathcal{A} = \sum_{n \in \mathbb{N}} \mathcal{A}(n) \cdot T^n.$$

Jeśli istnieje nieujemna liczba całkowita  $m$  taka, że  $\mathcal{A}(n) = 0$  dla wszystkich liczb całkowitych  $n$  takich, że  $n > m$ , to piszemy również

$$\mathcal{A} = \sum_{n \in [0, m]} \mathcal{A}(n) \cdot T^n.$$

Zbiór szeregów formalnych oznaczamy symbolem  $\mathbb{C}[[T]]$ . W zbiorze  $\mathbb{C}[[T]]$  wprowadzamy działania dodawania i mnożenia wzorami

$$(\mathcal{A} + \mathcal{B})(n) := \mathcal{A}(n) + \mathcal{B}(n) \quad (\mathcal{A}, \mathcal{B} \in \mathbb{C}[[T]], n \in \mathbb{N})$$

i

$$(\mathcal{A} \cdot \mathcal{B})(n) := \sum_{k \in [0, n]} \mathcal{A}(k) \cdot \mathcal{B}(n - k) \quad (\mathcal{A}, \mathcal{B} \in \mathbb{C}[[T]], n \in \mathbb{N}),$$

tzn.

$$\left( \sum_{n \in \mathbb{N}} a_n \cdot T^n \right) + \left( \sum_{n \in \mathbb{N}} b_n \cdot T^n \right) := \sum_{n \in \mathbb{N}} (a_n + b_n) \cdot T^n,$$

i

$$\left( \sum_{n \in \mathbb{N}} a_n \cdot T^n \right) \cdot \left( \sum_{n \in \mathbb{N}} b_n \cdot T^n \right) := \sum_{n \in \mathbb{N}} \left( \sum_{k \in [0, n]} a_k \cdot b_{n-k} \right) \cdot T^n.$$

Zbiór  $\mathbb{C}[[T]]$  wraz z powyższymi działaniami jest pierścieniem.

OZNACZENIE.

Zauważmy, że każdy wielomian jest szeregiem. Aby odróżnić wartości wielomianu od jego współczynników,  $n$ -ty współczynnik szeregu  $\mathcal{A}$  będziemy oznaczać  $[T^n]\mathcal{A}$ , zamiast  $\mathcal{A}(n)$ .

LEMAT 3.1.

Szereg  $\mathcal{A} \in \mathbb{C}[[T]]$  jest odwracalny wtedy i tylko wtedy, gdy  $[T^0]\mathcal{A} \neq 0$ .

DOWÓD.

Jeśli szereg  $\mathcal{A}$  jest odwracalny, to istnieje szereg  $\mathcal{B}$  taki, że  $\mathcal{A} \cdot \mathcal{B} = 1$ . W szczególności,  $[T^0]\mathcal{A} \cdot [T^0]\mathcal{B} = [T^0](\mathcal{A} \cdot \mathcal{B}) = 1$ , skąd  $[T^0]\mathcal{A} \neq 0$ .

Przypuśćmy teraz, że  $\mathcal{A}[T^0] \neq 0$ . Definiujemy szereg  $\mathcal{B}$  wzorem

$$[T^n]\mathcal{B} := \begin{cases} \frac{1}{[T^0]\mathcal{A}} & \text{jeśli } n = 0, \\ -\frac{1}{[T^0]\mathcal{A}} \cdot \left( \sum_{k \in [1, n]} [T^k]\mathcal{A} \cdot [T^{n-k}]\mathcal{B} \right) & \text{jeśli } n > 0, \end{cases} \quad (n \in \mathbb{N}).$$

Łatwo sprawdzić, że  $\mathcal{A} \cdot \mathcal{B} = 1$ , co kończy dowód.

OZNACZENIE.

Jeśli  $\mathcal{A}$  i  $\mathcal{B}$  są szeregami oraz szereg  $\mathcal{B}$  jest odwracalny, to symbolem  $\frac{\mathcal{A}}{\mathcal{B}}$  oznaczamy iloczyn szeregu  $\mathcal{A}$  i szeregu odwrotnego do szeregu  $\mathcal{B}$ .

PRZYKŁAD.

Jeśli  $\lambda$  jest liczbą zespoloną, to

$$\frac{1}{1 - \lambda \cdot T} = \sum_{n \in \mathbb{N}} \lambda^n \cdot T^n.$$

### 3.2. FUNKCJE TWORZĄCE

DEFINICJA.

FUNKCJĄ TWORZĄCĄ ciągu  $a$  nazywamy szereg  $\sum_{n \in \mathbb{N}} a(n) \cdot T^n$ .

OZNACZENIE.

Jeśli  $x$  jest liczbą rzeczywistą, to przez  $\mathcal{A}_x$  oznaczamy funkcję tworzącą ciągu  $\left( \binom{x}{n} \right)_{n \in \mathbb{N}}$ , tzn.

$$\mathcal{A}_x = \sum_{n \in \mathbb{N}} \binom{x}{n} \cdot T^n.$$

LEMAT 3.2.

Jeśli  $x$  i  $y$  są liczbami rzeczywistymi, to

$$\mathcal{A}_{x+y} = \mathcal{A}_x \cdot \mathcal{A}_y.$$

Ponadto  $\mathcal{A}_0 = 1$ .

DOWÓD.

Pierwsza część wynika natychmiast z Wniosku 2.11, natomiast druga wynika bezpośrednio z definicji szeregu  $\mathcal{A}_0$ .  $\square$

**STWIERDZENIE 3.3.**

Jeśli  $k$  jest dodatnią liczbą całkowitą, to

$$\frac{1}{(1+T)^k} = \sum_{n \in \mathbb{N}} (-1)^n \cdot \binom{k+n-1}{k-1} \cdot T^n.$$

**DOWÓD.**

Korzystając Wniosku 2.4 otrzymujemy, że

$$(1+T)^k = \sum_{n \in [0, k]} \binom{k}{n} \cdot T^n = \sum_{n \in \mathbb{N}} \binom{k}{n} \cdot T^n = \mathcal{A}_k.$$

Ponieważ  $\mathcal{A}_{-k} \cdot \mathcal{A}_k = \mathcal{A}_0 = 1$  na mocy Lematu 3.2, więc otrzymujemy, że

$$\begin{aligned} \frac{1}{(1+T)^k} &= \frac{1}{\mathcal{A}_k} = \mathcal{A}_{-k} = \sum_{n \in \mathbb{N}} \binom{-k}{n} \cdot T^n = \sum_{n \in \mathbb{N}} \frac{\prod_{i \in [0, n-1]} (-k-i)}{n!} \cdot T^n \\ &= \sum_{n \in \mathbb{N}} (-1)^n \cdot \frac{\prod_{i \in [0, n-1]} (k+i)}{n!} \cdot T^n \\ &= \sum_{n \in \mathbb{N}} (-1)^n \cdot \frac{\prod_{i \in [0, n-1]} (k+n-1-i)}{n!} \cdot T^n \\ &= \sum_{n \in \mathbb{N}} (-1)^n \cdot \binom{k+n-1}{n} \cdot T^n \\ &= \sum_{n \in \mathbb{N}} (-1)^n \cdot \binom{k+n-1}{k-1} \cdot T^n, \end{aligned}$$

co kończy dowód. □

**WNIOSEK 3.4.**

Jeśli  $k$  i  $m$  są dodatnimi liczbami całkowitymi i  $\lambda$  jest liczbą zespoloną, to

$$\frac{1}{(1-\lambda \cdot T^m)^k} = \sum_{n \in \mathbb{N}} \binom{k+n-1}{k-1} \cdot \lambda^n \cdot T^{n \cdot m}.$$

**DOWÓD.**

Wystarczy we wzorze ze Stwierdzenia 3.3 podstawić  $-\lambda \cdot T^m$  w miejsce  $T$ . □

**FAKT 3.5.**

Jeśli  $\mathcal{A}^k = 1 + T$  dla szeregu  $\mathcal{A}$ , to istnieje pierwiastek zespolony  $\varepsilon$  stopnia  $k$  z jedynek taki, że

$$\mathcal{A} = \varepsilon \cdot \mathcal{A}_{\frac{1}{k}} = \varepsilon \cdot \left( 1 + \sum_{n \in \mathbb{N}_+} (-1)^{n-1} \cdot \frac{\prod_{i \in [1, n-1]} (i \cdot k - 1)}{k^n \cdot n!} \cdot T^n \right).$$

DOWÓD.

Z Lematu 3.2 natychmiast wynika, że  $(\mathcal{A}_{\frac{1}{k}})^k = \mathcal{A}_1 = 1 + T$ . □

UWAGA.

Jeśli  $F$  i  $G$  są wielomianami o współczynnikach zespolonych i  $G \neq 0$ , to istnieją wielomiany  $Q$  i  $R$  takie, że  $\deg R < \deg G$  oraz

$$\frac{F}{G} = Q + \frac{R}{G}.$$

UWAGA.

Niech  $F$  i  $G$  będą wielomianami o współczynnikach zespolonych takimi, że  $\deg F < \deg G$  oraz  $G(0) = 1$ . Jeśli  $\lambda_1, \dots, \lambda_n$  są wszystkimi parami różnymi pierwiastkami zespolonymi wielomianu  $G$  krotności  $m_1, \dots, m_n$  odpowiednio, to istnieją liczby zespolone  $A_{i,j}$ ,  $j \in [1, m_i]$ ,  $i \in [1, n]$ , takie, że

$$\frac{F}{G} = \sum_{i \in [1, n]} \sum_{j \in [1, m_i]} \frac{A_{i,j}}{(1 - \lambda_i^{-1} \cdot T)^j}.$$

PRZYKŁAD.

Na ile sposobów można wypłacić kwotę  $n$  złotych przy pomocy monet jedno-, dwu- i pięciozłotowych?

ROZWIĄZANIE.

Dla każdej nieujemnej liczby całkowitej  $n$  niech  $a(n)$  będzie szukaną wielkością i  $\mathcal{A}$  funkcją tworzącą ciąg  $a$ . Zauważmy, że

$$\begin{aligned} & \left( \sum_{n \in \mathbb{N}} T^n \right) \cdot \left( \sum_{n \in \mathbb{N}} T^{2 \cdot n} \right) \cdot \left( \sum_{n \in \mathbb{N}} T^{5 \cdot n} \right) \\ &= \sum_{n \in \mathbb{N}} \left( \sum_{\substack{(i_1, i_2, i_3) \in \mathbb{N}^3 \\ i_1 + 2 \cdot i_2 + 5 \cdot i_3 = n}} 1 \right) \cdot T^n \\ &= \sum_{n \in \mathbb{N}} \#\{(i_1, i_2, i_3) \in \mathbb{N}^3 : i_1 + 2 \cdot i_2 + 5 \cdot i_3 = n\} \cdot T^n \\ &= \sum_{n \in \mathbb{N}} a(n) \cdot T^n = \mathcal{A}. \end{aligned}$$

Stąd

$$\begin{aligned} \mathcal{A} &= \left( \sum_{n \in \mathbb{N}} T^n \right) \cdot \left( \sum_{n \in \mathbb{N}} T^{2 \cdot n} \right) \cdot \left( \sum_{n \in \mathbb{N}} T^{5 \cdot n} \right) \\ &= \frac{1}{(1 - T) \cdot (1 - T^2) \cdot (1 - T^5)} \end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{(1-T)^3 \cdot (1+T) \cdot \prod_{i \in [1,4]} (1 - \varepsilon^i \cdot T)} \\
 &= \frac{13}{40} \cdot \frac{1}{1-T} + \frac{1}{4} \cdot \frac{1}{(1-T)^2} + \frac{1}{10} \cdot \frac{1}{(1-T)^3} + \frac{1}{8} \cdot \frac{1}{1+T} \\
 &\quad + \frac{1}{25} \cdot \sum_{i \in [1,4]} \frac{1 - \varepsilon^i - \varepsilon^{2 \cdot i} + \varepsilon^{3 \cdot i}}{1 - \varepsilon^i \cdot T},
 \end{aligned}$$

więc korzystając z Wniosku 3.4 otrzymujemy, że

$$\begin{aligned}
 a(n) = \frac{13}{40} + \frac{1}{4} \cdot (n+1) + \frac{1}{10} \cdot \binom{n+2}{n} + (-1)^n \cdot \frac{1}{8} \\
 + \frac{1}{25} \cdot \sum_{i \in [1,4]} (1 - \varepsilon^i - \varepsilon^{2 \cdot i} + \varepsilon^{3 \cdot i}) \cdot \varepsilon^{n \cdot i}
 \end{aligned}$$

dla każdej nieujemnej liczby całkowitej  $n$ , gdzie  $\varepsilon$  jest pierwiastkiem pierwotnym 5-tego stopnia z 1. Ostatecznie

$$a(n) = \frac{1}{20} \cdot n^2 + \frac{2}{5} \cdot n + \begin{cases} 1 & \text{jeśli } n \equiv_{10} 0, 2, \\ \frac{11}{20} & \text{jeśli } n \equiv_{10} 1, \\ \frac{7}{20} & \text{jeśli } n \equiv_{10} 3, 9, \\ \frac{3}{5} & \text{jeśli } n \equiv_{10} 4, 8, \\ \frac{3}{4} & \text{jeśli } n \equiv_{10} 5, 7, \\ \frac{4}{5} & \text{jeśli } n \equiv_{10} 6, \end{cases}$$

dla każdej nieujemnej liczby całkowitej  $n$ , co kończy rozwiązanie.

Ten sam wynik otrzymujemy stosując przedstawienie

$$\begin{aligned}
 \mathcal{A} &= \frac{1}{(1-T) \cdot (1-T^2) \cdot (1-T^5)} \\
 &= \frac{(\sum_{i \in [0,9]} T^i) \cdot (\sum_{i \in [0,4]} T^{2 \cdot i}) \cdot (1+T^5)}{(1-T^{10})^3} \\
 &= \left( \sum_{i \in [0,9]} T^i \right) \cdot \left( \sum_{i \in [0,4]} T^{2 \cdot i} \right) \cdot (1+T^5) \cdot \left( \sum_{n \in \mathbb{N}} \binom{n+2}{2} \cdot T^{10 \cdot n} \right).
 \end{aligned}$$

### 3.3. REKURENCJA

PRZYKŁAD.

Definiujemy ciąg Fibonacciego  $F$  wzorem

$$F(n) := \begin{cases} 0 & \text{jeśli } n = 0, \\ 1 & \text{jeśli } n = 1, \\ F(n-1) + F(n-2) & \text{jeśli } n \geq 2, \end{cases} \quad (n \in \mathbb{N}).$$

MATEMATYKA DYSKRETNA

Policzmy funkcję tworzącą  $\mathcal{F}$  ciągu  $F$ . Zauważmy, że dla każdej liczby całkowitej  $n$  takiej, że  $n \geq 2$ , mamy

$$F(n) \cdot T^n = F(n-1) \cdot T^n + F(n-2) \cdot T^n$$

skąd

$$\begin{aligned} \mathcal{F} &= \sum_{n \in \mathbb{N}} F(n) \cdot T^n = T + \sum_{n \geq 2} (F(n-1) \cdot T^n + F(n-2) \cdot T^n) \\ &= T + T \cdot \sum_{n \geq 2} F(n-1) \cdot T^{n-1} + T^2 \cdot \sum_{n \geq 2} F(n-2) \cdot T^{n-2} \\ &= T + T \cdot \mathcal{F} + T^2 \cdot \mathcal{F}, \end{aligned}$$

więc

$$\begin{aligned} \mathcal{F} &= \frac{T}{1-T-T^2} = \frac{\sqrt{5}}{5} \cdot \frac{1}{1 - \frac{1+\sqrt{5}}{2} \cdot T} - \frac{\sqrt{5}}{5} \cdot \frac{1}{1 - \frac{1-\sqrt{5}}{2} \cdot T} \\ &= \frac{\sqrt{5}}{5} \cdot \sum_{n \in \mathbb{N}} \left(\frac{1+\sqrt{5}}{2}\right)^n \cdot T^n - \frac{\sqrt{5}}{5} \cdot \sum_{n \in \mathbb{N}} \left(\frac{1-\sqrt{5}}{2}\right)^n \cdot T^n, \end{aligned}$$

skąd

$$F(n) = \frac{\sqrt{5}}{5} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{\sqrt{5}}{5} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

dla każdej nieujemnej liczby całkowitej  $n$ .

DEFINICJA.

REKURENCJĄ (LINIOWĄ O STAŁYCH WSPÓŁCZYNNIKACH) RZĘDU  $r$ ,  $r \in \mathbb{N}_+$ , nazywamy każdy układ równań postaci

$$(*) \quad X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \dots + u_0 \cdot X_n = f(n), \quad n \in \mathbb{N},$$

gdzie  $u_{r-1}, \dots, u_0$  są liczbami zespolonymi takimi, że  $u_0 \neq 0$ , oraz  $f$  jest ciągiem liczb zespolonych. Rekurencję  $(*)$  nazywamy JEDNORODNĄ, jeśli  $f = 0$  (tzn.  $f(n) = 0$  dla wszystkich nieujemnych liczb całkowitych  $n$ ). REKURENCJĄ JEDNORODNĄ STOWARZYSZONĄ Z REKURENCJĄ  $(*)$  nazywamy rekurencję

$$X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \dots + u_0 \cdot X_n = 0, \quad n \in \mathbb{N}.$$

WIELOMIANEM CHARAKTERYSTYCZNYM REKURENCJI  $(*)$  nazywamy wielomian

$$\sum_{i \in [0, r]} u_i \cdot T^i \in \mathbb{C}[T],$$

gdzie  $u_r := 1$ . Mówimy, że ciąg  $a$  JEST ROZWIĄZANIEM REKURENCJI (\*), jeśli

$$\sum_{i \in [0, r]} u_i \cdot a(n + i) = f(n)$$

dla każdej nieujemnej liczb całkowitej  $n$ .

UWAGA.

Jeśli

$$(*) \quad X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \dots + u_0 \cdot X_n = f(n), \quad n \in \mathbb{N},$$

jest rekurencją rzędu  $r$  oraz  $x_0, \dots, x_{r-1}$  są liczbami zespolonymi, to ciąg  $a$  dany wzorem

$$a(n) := \begin{cases} x_n & \text{jeśli } n \in [0, r-1], \\ f(n-r) - (\sum_{i \in [0, r-1]} u_i \cdot a(n-r+i)) & \text{jeśli } n \geq r, \end{cases} \quad (n \in \mathbb{N}),$$

jest rozwiązaniem rekurencji (\*). Ponadto, każde rozwiązanie rekurencji (\*) jest tej postaci. W szczególności, zbiór rozwiązań rekurencji (\*) ma wymiar  $r$ .

UWAGA.

Zbiór  $\mathbb{C}^{\mathbb{N}}$  ciągów o współczynnikach zespolonych jest przestrzenią liniową nad ciałem liczb zespolonych z działaniami dodawania ciągów po współrzędnych oraz mnożeniem ciągów przez skalary po współrzędnych.

TWIERDZENIE 3.6.

Niech

$$(*) \quad X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \dots + u_0 \cdot X_n = f(n), \quad n \in \mathbb{N},$$

będzie rekurencją.

- (1) Jeśli rekurencja (\*) jest jednorodna, to zbiór rozwiązań rekurencji (\*) jest podprzestrzenią liniową przestrzeni  $\mathbb{C}^{\mathbb{N}}$ .
- (2) Jeśli ciągi  $a$  i  $b$  są rozwiązaniami rekurencji (\*), to ciąg  $a - b$  jest rozwiązaniem stowarzyszonej rekurencji jednorodnej.
- (3) Jeśli ciągi  $a$  i  $b$  są rozwiązaniami rekurencji (\*) oraz stowarzyszonej rekurencji jednorodnej, odpowiednio, to ciąg  $a + b$  jest rozwiązaniem rekurencji (\*).



Dowód.

Ćwiczenie. □

UWAGA.

Jeśli

$$(*) \quad X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \cdots + u_0 \cdot X_n = f(n), \quad n \in \mathbb{N},$$

jest rekurencją, to zbiór  $A$  rozwiązań tej rekurencji możemy znajdować następująco:

- (1) znajdujemy zbiór  $A'$  rozwiązań stowarzyszonej rekurencji jednorodnej,
- (2) znajdujemy jedno rozwiązanie  $a$  rekurencji (\*),
- (3)  $A = a + A'$ , tzn. rozwiązaniami rekurencji (\*) są ciągi postaci  $a + a'$ , gdzie  $a' \in A'$ .

TWIERDZENIE 3.7.

Jeśli  $\lambda_1, \dots, \lambda_l$  są wszystkimi parami różnymi pierwiastkami krotności  $k_1, \dots, k_l$ , odpowiednio, wielomianu charakterystycznego  $F$  rekurencji jednorodnej

$$(*) \quad X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \cdots + u_0 \cdot X_n = 0, \quad n \in \mathbb{N},$$

rzędu  $r$ , to ciągi  $(n^j \cdot \lambda_i^n)_{n \in \mathbb{N}}$ ,  $i \in [1, l]$ ,  $j \in [0, k_i - 1]$ , tworzą bazę przestrzeni rozwiązań rekurencji (\*). W szczególności, dla każdego rozwiązania  $a$  rekurencji (\*) istnieją liczby zespolone  $\mu_{i,j}$ ,  $i \in [1, l]$ ,  $j \in [0, k_i - 1]$ , takie, że

$$a(n) = \sum_{i \in [1, l]} \sum_{j \in [0, k_i - 1]} \mu_{i,j} \cdot n^j \cdot \lambda_i^n.$$

Dowód.

Ponieważ zbiór rozwiązań rekurencji (\*) ma wymiar  $r$ , więc wystarczy udowodnić, że każde rozwiązanie rekurencji (\*) jest kombinacją liniową powyższych ciągów. Niech ciąg  $a$  będzie rozwiązaniem rekurencji (\*). Policzmy funkcję tworzącą  $\mathcal{A}$  ciągu  $a$ :

$$\begin{aligned} & \left( \sum_{i \in [0, r]} u_i \cdot T^{r-i} \right) \cdot \mathcal{A} \\ &= \left( \sum_{j \in [0, r]} u_{r-j} \cdot T^j \right) \cdot \left( \sum_{n \in \mathbb{N}} a(n) \cdot T^n \right) \\ &= \sum_{\substack{j \in [0, r] \\ n \in \mathbb{N}}} u_{r-j} \cdot a(n) \cdot T^{n+j} \\ &= \sum_{m \in [0, r-1]} \sum_{j \in [0, m]} u_{r-j} \cdot a(m-j) \cdot T^m \end{aligned}$$

$$\begin{aligned}
 & + \sum_{m \geq r} \sum_{j \in [0, r]} u_{r-j} \cdot a(m-j) \cdot T^m \\
 = & \sum_{m \in [0, r-1]} \sum_{j \in [0, m]} u_{r-j} \cdot a(m-j) \cdot T^m \\
 & + \sum_{n \in \mathbb{N}} \sum_{i \in [0, r]} u_i \cdot a(n+i) \cdot T^{n+r} \\
 = & \sum_{m \in [0, r-1]} \sum_{j \in [0, m]} u_{r-j} \cdot a(m-j) \cdot T^m,
 \end{aligned}$$

gdzie  $u_r := 1$ , więc

$$\mathcal{A} = \frac{\sum_{m \in [0, r-1]} \sum_{j \in [0, m]} u_{r-j} \cdot a(m-j) \cdot T^m}{\sum_{i \in [0, r]} u_i \cdot T^{r-i}}.$$

Zauważmy, że

$$\deg \sum_{m \in [0, r-1]} \sum_{j \in [0, m]} u_{r-j} \cdot a(m-j) \cdot T^m < r = \deg \left( \sum_{i \in [0, r]} u_i \cdot T^{r-i} \right).$$

Ponieważ  $\sum_{i \in [0, r]} u_i \cdot T^{r-i} = T^r \cdot F(\frac{1}{T})$ , więc liczby  $\lambda_1^{-1}, \dots, \lambda_l^{-1}$  są parami różnymi pierwiastkami wielomianu  $\sum_{i \in [0, r]} u_i \cdot T^{r-i}$  krotności  $k_1, \dots, k_l$ , odpowiednio. Stąd istnieją liczby zespolone  $A_{i,j}$ ,  $i \in [1, l]$ ,  $j \in [1, k_i]$ , takie, że

$$\mathcal{A} = \sum_{i \in [1, l]} \sum_{j \in [1, k_i]} \frac{A_{i,j}}{(1 - \lambda_i \cdot T)^j}.$$

Z Wniosku 3.4 wynika, że

$$\mathcal{A} = \sum_{n \in \mathbb{N}} \left( \sum_{i \in [1, l]} \sum_{j \in [1, k_i]} A_{i,j} \cdot \binom{j+n-1}{j-1} \cdot \lambda_i^n \right) \cdot T^n$$

tzn.

$$a(n) = \sum_{i \in [1, l]} \sum_{j \in [1, k_i]} A_{i,j} \cdot \binom{j+n-1}{n} \cdot \lambda_i^n$$

dla każdej nieujemnej liczby całkowitej  $n$ . Na zakończenie ustalmy dodatnią liczbę całkowitą  $j$ . Wtedy istnieją liczby zespolone  $B_{j,p}$ ,  $p \in [0, j-1]$ , takie, że

$$\binom{j+n-1}{j-1} = \sum_{p \in [0, j-1]} B_{j,p} \cdot n^p.$$

Stąd

$$a(n) = \sum_{i \in [1, l]} \sum_{p \in [0, k_i - 1]} \left( \sum_{j \in [l, k_i - 1]} A_{i,j} \cdot B_{j,p} \right) \cdot n^p \cdot \lambda_i^n$$

dla każdej nieujemnej liczby całkowitej  $n$ , co kończy dowód.  $\square$

PRZYKŁAD (WIEŻE Z HANOI).

Dane są trzy pionowe pręty. Na pierwszym z tych prętów jest nałożonych  $n$ ,  $n \in \mathbb{N}$ , krążków różnego rozmiaru w ten sposób, że krążki mniejsze znajdują się nad krążkami większymi. Ilu ruchów potrzeba, aby przełożyć wszystkie krążki na pręt trzeci, jeśli w jednym ruchu możemy przełożyć jeden krążek pomiędzy dowolnymi dwoma prętami, przy czym w żadnym momencie nie wolno kłaść krążka większego na mniejszego?

ROZWIĄZANIE.

Dla każdej liczby całkowitej nieujemnej  $n$  oznaczmy przez  $a(n)$  szukaną wielkość. Łatwo zauważyć, że  $a(0) = 0$  oraz  $a(n) = 2 \cdot a(n-1) + 1$  dla każdej dodatniej liczby całkowitej  $n$ . W szczególności,  $a(1) = 1$ . Ponadto

$$\begin{aligned} a(n+2) - a(n+1) &= (2 \cdot a(n+1) + 1) - (2 \cdot a(n) + 1) \\ &= 2 \cdot a(n+1) - 2 \cdot a(n) \end{aligned}$$

dla każdej nieujemnej liczby całkowitej  $n$ . Zatem ciąg  $a$  jest rozwiązaniem rekurencji jednorodnej

$$X_{n+2} - 3 \cdot X_{n+1} + 2 \cdot X_n = 0, \quad n \in \mathbb{N}.$$

Wielomianem charakterystycznym tej rekurencji jest wielomian  $T^2 - 3 \cdot T + 2$ , którego pierwiastkami (jednokrotnymi) są 1 i 2. Zatem istnieją liczby zespolone  $\mu_1$  i  $\mu_2$  takie, że

$$a(n) = \mu_1 \cdot 2^n + \mu_2$$

dla każdej nieujemnej liczby całkowitej  $n$ . Podstawiając  $n = 0$  i  $n = 1$ , wyliczamy, że  $\mu_1 = 1$  oraz  $\mu_2 = -1$ , zatem ostatecznie

$$a(n) = 2^n - 1$$

dla każdej nieujemnej liczby całkowitej  $n$ .

TWIERDZENIE 3.8.

Jeśli  $f \in \mathbb{C}[T]$ , to istnieje rozwiązanie rekurencji

$$(*) \quad X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \cdots + u_0 \cdot X_n = f(n), \quad n \in \mathbb{N},$$

rzędu  $r$  postaci  $(n^k \cdot g(n))_{n \in \mathbb{N}}$ , gdzie  $k$  jest krotnością 1 jako pierwiastka wielomianu charakterystycznego rekurencji  $(*)$ , zaś  $g \in \mathbb{C}[T]$  jest wielomianem stopnia co najwyżej  $\deg f$ .

**Dowód.**

Niech  $m := \deg f$  ( $m := -1$ , gdy  $f = 0$ ). Pokażemy najpierw, że istnieje rekurencja jednorodna

$$(**) \quad X_{n+r+m+1} + u'_{r+m} \cdot X_{n+r+m} + \cdots + u'_0 \cdot X_n = 0, \quad n \in \mathbb{N},$$

rzędu  $r + m + 1$  taka, że spełnione są następujące warunki:

1. jeśli ciąg  $a$  jest rozwiązaniem rekurencji  $(*)$ , to ciąg  $a$  jest rozwiązaniem rekurencji  $(**)$ ,
2. jeśli  $F$  i  $G$  są wielomianami charakterystycznymi rekurencji  $(*)$  i  $(**)$ , odpowiednio, to  $G = (T - 1)^{m+1} \cdot F$ .

Dowód powyżej tezy będzie indukcyjny ze względu  $m$ . Dla  $m = -1$  teza jest oczywista. Dla  $m \geq 0$  rozważmy rekurencję

$$(***) \quad X_{n+r+1} + (u_{r-1} - u_r) \cdot X_{n+r} + \cdots + (u_0 - u_1) \cdot X_{n+1} - u_0 \cdot X_n = h(n), \quad n \in \mathbb{N},$$

gdzie  $u_r := 1$  i  $h := f(T + 1) - f(T)$ . Zauważmy, że jeśli ciąg  $a$  jest rozwiązaniem rekurencji  $(*)$ , to ciąg  $a$  jest rozwiązaniem rekurencji  $(***)$ . Ponadto wielomian charakterystyczny rekurencji  $(***)$  jest postaci  $(T - 1) \cdot F$ . Wreszcie rząd rekurencji  $(***)$  jest równy  $r + 1$  i  $\deg h = m - 1$ , zatem teza wynika z założenia indukcyjnego.

Niech  $\lambda_0 = 1, \lambda_1, \dots, \lambda_l$  będą pierwiastkami wielomianu  $G$  krotności  $k_0 = k + m + 1, k_1, \dots, k_l$ , odpowiednio. Ustalmy rozwiązanie  $a$  rekurencji  $(*)$ . Z Twierdzenia 3.7 wiemy, że istnieją liczby zespolone  $A_{i,j}$ ,  $i \in [0, l], j \in [0, k_i - 1]$ , takie, że

$$a(n) := \sum_{i \in [0, l]} \sum_{j \in [0, k_i - 1]} A_{i,j} \cdot n^j \cdot \lambda_i^n$$

dla każdej nieujemnej liczby całkowitej  $n$ . Ponieważ pierwiastkami wielomianu  $F$  są  $\lambda_0, \lambda_1, \dots, \lambda_l$ , a ich krotności to  $k = k_0 - m - 1, k_1, \dots, k_l$ , odpowiednio, więc korzystając ponownie z poprzedniego twierdzenia otrzymujemy, że ciąg  $a'$  dany wzorem

$$a'(n) := \sum_{j \in [0, k-1]} A_{0,j} \cdot n^j + \sum_{i \in [1, l]} \sum_{j \in [0, k_i - 1]} A_{i,j} \cdot n^j \cdot \lambda_i^n \quad (n \in \mathbb{N})$$

jest rozwiązaniem rekurencji jednorodnej stowarzyszonej z rekurencją (\*). Wobec Twierdzenia 3.6 (3) oznacza to, że ciąg  $a - a'$  jest rozwiązaniem rekurencji (\*). Ponieważ

$$(a - a')(n) = \sum_{j \in [k, k+m]} A_{0,j} \cdot n^j = n^k \cdot \sum_{j \in [0, m]} A_{0, k+j} \cdot n^j$$

dla każdej nieujemnej liczby całkowitej  $n$ , to kończy dowód.  $\square$

UWAGA.

Podobne, bardziej ogólne, twierdzenie można sformułować w sytuacji, gdy ciąg  $f$  jest kombinacją liniową ciągów postaci  $(\lambda^n \cdot n^k)$  dla liczb  $\lambda \in \mathbb{C}$  oraz  $k \in \mathbb{N}$ .

PRZYKŁAD.

Definiujemy ciąg  $s$  wzorem

$$s(n) := \sum_{k \in [1, n]} k^3 \quad (n \in \mathbb{N}).$$

Zauważmy, że ciąg  $s$  jest rozwiązaniem rekurencji

$$X_{n+1} - X_n = n^3 + 3 \cdot n^2 + 3 \cdot n + 1, \quad n \in \mathbb{N}.$$

Wielomianem charakterystycznym powyższej rekurencji jest wielomian  $T - 1$ , którego jedynym pierwiastkiem (jednokrotnym) jest 1. Z Twierdzenia 3.8 wynika zatem, że istnieją liczby zespolone  $\mu'_0, \mu'_1, \mu'_2$  i  $\mu'_3$  takie, że

$$(*) \quad s'(n+1) - s'(n) = n^3 + 3 \cdot n^2 + 3 \cdot n + 1$$

dla każdej nieujemnej liczby całkowitej  $n$ , gdzie ciąg  $s'$  zdefiniowany jest wzorem

$$s'(n) := n \cdot (\mu'_3 \cdot n^3 + \mu'_2 \cdot n^2 + \mu'_1 \cdot n + \mu'_0) \quad (n \in \mathbb{N}).$$

Podstawiając powyższy wzór do równości (\*) i porównując współczynniki przy poszczególnych potęgach liczby  $n$ , otrzymujemy układ równań

$$\left\{ \begin{array}{rcl} & & 4 \cdot \mu'_3 = 1 \\ & & 3 \cdot \mu'_2 + 6 \cdot \mu'_3 = 3 \\ & 2 \cdot \mu'_1 + 3 \cdot \mu'_2 + 4 \cdot \mu'_3 = 3 \\ \mu'_0 + \mu'_1 + \mu'_2 + \mu'_3 = 1 \end{array} \right. ,$$

którego rozwiązaniem są liczby

$$\mu'_0 = 0, \quad \mu'_1 = \frac{1}{4}, \quad \mu'_2 = \frac{1}{2}, \quad \mu'_3 = \frac{1}{4}.$$

## MATEMATYKA DYSKRETNA

Na mocy Twierdzenie 3.7 istnieje liczba zespolona  $\mu$  taka, że

$$s(n) = \frac{1}{4} \cdot n^4 + \frac{1}{2} \cdot n^3 + \frac{1}{4} \cdot n^2 + \mu$$

dla każdej nieujemnej liczby całkowitej  $n$ . Podstawiając  $n = 0$ , otrzymujemy, że  $\mu = 0$ , zatem ostatecznie

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

dla każdej nieujemnej liczby całkowitej  $n$ .

### Twierdzenie 3.9.

Niech  $\mathcal{A}$  będzie funkcją generującą ciągu  $a$ . Jeśli

$$\mathcal{A} = \frac{F}{\sum_{i \in [0, r]} u_i \cdot T^{r-i}}$$

dla pewnych liczb zespolonych  $u_0, \dots, u_r$  takich, że  $u_0 \neq 0$  i  $u_r = 1$ , oraz wielomianu  $F \in \mathbb{C}[T]$  takiego, że  $\deg F < r$ , to ciąg  $a$  jest rozwiązaniem rekurencji

$$X_{n+r} + u_{r-1} \cdot X_{n+r-1} + \dots + u_0 \cdot X_n = 0, \quad n \in \mathbb{N}.$$

### Dowód.

Zauważmy, że powyższa równość oznacza, że

$$\left( \sum_{i \in [0, r]} u_i \cdot T^{r-i} \right) \cdot \mathcal{A} = F,$$

zatem

$$0 = [T^{n+r}]F = [T^{n+r}] \left( \left( \sum_{i \in [0, r]} u_i \cdot T^{r-i} \right) \cdot \mathcal{A} \right) = \sum_{i \in [0, r]} u_i \cdot a(n+i)$$

dla wszystkich nieujemnych liczb całkowitych  $n$ , co kończy dowód. □

### Przykład.

Dla nieujemnej liczby całkowitej  $n$  niech  $a(n)$  oznacza ilość ciągów binarnych długości  $n$ , w których występuje parzysta liczba jedynek oraz każde dwie jedynki rozdzielone są co najmniej jednym zerem.

Niech  $n$  będzie dodatnią liczbą całkowitą. Zauważmy, że ciągów długości  $n$  spełniających powyższy warunek zaczynających się od 0 jest  $a(n-1)$ . Z

MATEMATYKA DYSKRETNA

drugiej strony, jeśli mamy ciąg  $x$  długości  $n$  spełniający powyższe warunki taki, że  $x(1) = 1$ , to definiujemy liczbę  $k_x$  wzorem

$$k_x := \min\{i \in [2, n] : x(i) = 1\}.$$

Zauważmy, że  $k_x \in [3, n]$ . Dla ustalonej liczby  $k \in [3, n-1]$  ciągów  $x$ , dla których  $k_x = k$ , jest  $a(n-k-1)$ . Ponadto, jeśli  $n \geq 3$ , to mamy dokładnie jeden ciąg  $x$ , dla którego  $k_x = n$  ( $x = (1, 0, \dots, 0, 1)$ ). Otrzymujemy zatem, że

$$a(n) = \begin{cases} a(n-1) & \text{jeśli } n = 1, 2, \\ a(n-1) + \sum_{k \in [3, n-1]} a(n-k-1) + 1 & \text{jeśli } n \geq 3. \end{cases}$$

Zauważmy też, że  $a(0) = 1$ . Z powyższej równości wynika, że

$$\begin{aligned} \mathcal{A} &= \sum_{n \in \mathbb{N}} a(n) \cdot T^n \\ &= 1 + \sum_{n \geq 1} a(n-1) \cdot T^{n-1} \cdot T \\ &\quad + \sum_{n \geq 3} \sum_{k \in [3, n-1]} a(n-k-1) \cdot T^{n-k-1} \cdot T^{k+1} + \sum_{n \geq 3} T^n \\ &= 1 + T \cdot \mathcal{A} + \sum_{k \geq 3} \sum_{n \geq k+1} a(n-k-1) \cdot T^{n-k-1} \cdot T^{k+1} + \frac{T^3}{1-T} \\ &= 1 + T \cdot \mathcal{A} + \sum_{k \geq 3} \sum_{n \in \mathbb{N}} a(n) \cdot T^n \cdot T^{k+1} + \frac{T^3}{1-T} \\ &= 1 + T \cdot \mathcal{A} + \sum_{k \geq 3} \mathcal{A} \cdot T^{k+1} + \frac{T^3}{1-T} \\ &= 1 + T \cdot \mathcal{A} + \frac{T^4}{1-T} \cdot \mathcal{A} + \frac{T^3}{1-T}, \end{aligned}$$

skąd

$$\mathcal{A} = \frac{1 - T + T^3}{1 - 2 \cdot T + T^2 - T^4},$$

a więc ciąg  $a$  jest rozwiązaniem rekurencji

$$X_{n+4} - 2 \cdot X_{n+3} + X_{n+2} - X_n = 0, \quad n \in \mathbb{N}.$$

Zauważmy, że  $a(0) = a(1) = a(2) = 1$  oraz  $a(3) = 2$ .

PRZYKŁAD (LICZBY CATALANA).

Dla nieujemnej liczby całkowitej  $n$  niech  $c(n)$  oznacza liczbę drzew binarnych o  $n$  wierzchołkach. Przypomnijmy, że drzewem binarnym o  $n$  wierzchołkach nazywamy drzewo puste  $\emptyset$ , gdy  $n = 0$ , oraz parę  $(L, R)$  drzew binarnych o  $k$  i  $(n - 1) - k$  wierzchołkach dla pewnej liczby  $k \in [0, n - 1]$ , gdy  $n > 0$ . Zauważmy, że  $c(0) = 1$  oraz

$$c(n) = \sum_{j \in [0, n-1]} c(j) \cdot c(n - 1 - j)$$

dla każdej dodatniej liczby całkowitej  $n$ . Niech  $\mathcal{C}$  będzie funkcją tworzącą ciągu  $c$ . Wtedy

$$\begin{aligned} \mathcal{C} &= \sum_{n \in \mathbb{N}} c(n) \cdot T^n \\ &= 1 + \sum_{n \geq 1} \sum_{j \in [0, n-1]} c(j) \cdot T^j \cdot c(n - 1 - j) \cdot T^{n-1-j} \cdot T \\ &= 1 + T \cdot \sum_{j \in \mathbb{N}} c_j \cdot T^j \cdot \sum_{n \geq j+1} c(n - (j + 1)) \cdot T^{n-(j+1)} \\ &= 1 + T \cdot \sum_{j \in \mathbb{N}} c_j \cdot T^j \cdot \sum_{n \in \mathbb{N}} c_n \cdot T^n = 1 + T \cdot \mathcal{C}^2, \end{aligned}$$

skąd

$$T \cdot \mathcal{C} = \frac{1 - \sqrt{1 - 4 \cdot T}}{2} \quad \text{lub} \quad T \cdot \mathcal{C} = \frac{1 + \sqrt{1 - 4 \cdot T}}{2}.$$

Korzystając z Faktu 3.5 otrzymujemy, że

$$\begin{aligned} \sqrt{1 - 4 \cdot T} &= 1 - \sum_{n \geq 1} \frac{\prod_{i \in [1, n-1]} (2 \cdot i - 1)}{2^n \cdot n!} \cdot 4^n \cdot T^n \\ &= 1 - \sum_{n \geq 1} \frac{2}{n} \cdot \frac{\prod_{i \in [1, n-1]} (2 \cdot i - 1) \cdot (n - 1)! \cdot 2^{n-1}}{(n - 1)! \cdot (n - 1)!} \cdot T^n \\ &= 1 - \sum_{n \in \mathbb{N}_{\geq 1}} \frac{2}{n} \cdot \binom{2n - 2}{n - 1} \cdot T^n. \end{aligned}$$

Stąd

$$\frac{1 - \sqrt{1 - 4 \cdot T}}{2} = \sum_{n \geq 1} \frac{1}{n} \cdot \binom{2n - 2}{n - 1} \cdot T^n$$



i

$$\frac{1 + \sqrt{1 - 4 \cdot T}}{2} = 1 - \sum_{n \geq 1} \frac{1}{n} \cdot \binom{2n-2}{n-1} \cdot T^n,$$

zatem

$$C = \sum_{n \geq 1} \frac{1}{n} \cdot \binom{2n-2}{n-1} \cdot T^{n-1} = \sum_{n \in \mathbb{N}} \frac{1}{n+1} \cdot \binom{2n}{n} \cdot T^n,$$

a więc  $c(n) = \frac{1}{n+1} \cdot \binom{2n}{n}$  dla wszystkich nieujemnych liczb całkowitych  $n$ .

### 3.4. WIELOMIANY WIEŻOWE

DEFINICJA.

Niech  $n$  i  $m$  będą nieujemnymi liczbami całkowitymi. SZACHOWNICĄ O  $n$  WIERSZACH I  $m$  KOLUMNACH nazywamy każdą trójkę  $B = (I, J, F)$ , gdzie  $I$  i  $J$  są zbiorami takimi, że  $|I| = n$  i  $|J| = m$ , oraz  $F \subseteq I \times J$ . Zbiór  $F$  nazywamy zbiorem PÓL ZABRONIONYCH. Innymi słowy, szachownica to tablica o  $n$  wierszach i  $m$  kolumnach, w której część pól jest polami zabronionymi.

DEFINICJA.

Niech  $B = (I, J, F)$  będzie szachownicą oraz  $k$  nieujemną liczbą całkowitą. ROZSTAWIENIEM  $k$  WIEŻ NA SZACHOWNICY  $B$  nazywamy każdy podzbiór  $A \subseteq (I \times J) \setminus F$  taki, że  $|A| = k$  oraz

$$|A \cap (\{i\} \times J)| \leq 1 \quad \text{i} \quad |A \cap (I \times \{j\})| \leq 1$$

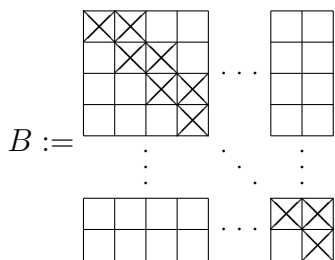
dla wszystkich indeksów  $i \in I$  i  $j \in J$ . Liczbę rozstawień  $k$  wież na szachownicy  $B$  oznaczamy przez  $r^B(k)$ .

PRZYKŁAD.

Jeśli  $B = (I, J, F)$  jest szachownicą, to  $r^B(0) = 1$ ,  $r^B(1) = |I| \cdot |J| - |F|$  i  $r^B(k) = 0$  dla każdej liczby całkowitej  $k$  takiej, że  $k > |I|$  i  $k > |J|$ .

PRZYKŁAD.

Dla dodatniej liczby całkowitej  $n$  liczba permutacji  $\sigma$  zbioru  $[1, n]$  takich, że  $\sigma(i) \neq i, i+1$  dla wszystkich liczby  $i \in [1, n]$ , jest równa liczbie  $r^B(n)$  dla szachownicy



o  $n$  wierszach i  $n$  kolumnach.

DEFINICJA.

WIELOMIANEM WIEŻOWYM SZACHOWNICY  $B$  nazywamy funkcję tworzącą ciąg  $r^B$ . Wielomian wieżowy szachownicy  $B$  oznaczamy symbolem  $R_B$ .

PRZYKŁAD.

Jeśli  $B = (I, J, F)$ , to  $R_{B^{\text{tr}}} = R_B$ , gdzie  $B^{\text{tr}} := (J, I, F^{\text{tr}})$  oraz

$$F^{\text{tr}} := \{(j, i) : (i, j) \in F\}.$$

PRZYKŁAD.

Jeśli  $B = (I, J, \emptyset)$ , to

$$R_B = \sum_{k \in \mathbb{N}} \binom{|I|}{k} \cdot \binom{|J|}{k} \cdot k! \cdot T^k.$$

PRZYKŁAD.

Jeśli  $B = (I, J, I \times J)$ , to  $R_B = 1$ .

PRZYKŁAD.

Jeśli  $n$  jest nieujemną liczbą całkowitą i

$$B_n := \begin{array}{ccc} \begin{array}{|c|c|c|c|} \hline \square & \times & \times & \times \\ \hline \times & \square & \times & \times \\ \hline \times & \times & \square & \times \\ \hline \times & \times & \times & \square \\ \hline \end{array} & \cdots & \begin{array}{|c|c|} \hline \times & \times \\ \hline \times & \times \\ \hline \end{array} \\ \vdots & \ddots & \vdots \\ \begin{array}{|c|c|c|c|} \hline \times & \times & \times & \times \\ \hline \times & \times & \times & \times \\ \hline \end{array} & \cdots & \begin{array}{|c|c|} \hline \times & \times \\ \hline \square & \square \\ \hline \end{array} \end{array}$$

jest szachownicą o  $n$  wierszach i  $n$  kolumnach, to

$$R_{B_n} = \sum_{k \in \mathbb{N}} \binom{n}{k} \cdot T^k = (1 + T)^n = R_{B_1}^n.$$

OZNACZENIE.

Jeśli  $B = (I, J, F)$  jest szachownicą,  $\sigma \in P_I$  i  $\tau \in P_J$ , to definiujemy szachownice  $B_\sigma$  i  $B^\tau$  wzorami  $B_\sigma := (I, J, F_\sigma)$ , gdzie

$$F_\sigma := \{(\sigma(i), j) : (i, j) \in F\},$$

oraz  $B^\tau := (I, J, F^\tau)$ , gdzie

$$F^\tau := \{(i, \tau(j)) : (i, j) \in F\}.$$

Mówimy, że szachownice  $B_\sigma$  i  $B^\tau$  są otrzymane z szachownicy  $B$  przez PERMUTACJĘ WIERSZY I KOLUMN, odpowiednio. Zauważmy, że  $(B_\sigma)^\tau = (B^\tau)_\sigma$  i tę szachownicę oznaczamy  $B_\sigma^\tau$ .

UWAGA.

Jeśli  $B = (I, J, F)$  jest szachownicą,  $\sigma \in P_I$  i  $\tau \in P_J$ , to  $R_{B_\sigma} = R_B = R_{B^\tau}$ .

OZNACZENIE.

Jeśli  $B = (I, J, F)$  jest szachownicą,  $i_0 \in I$  i  $j_0 \in J$ , to definiujemy szachownice  $B_{i_0}$  i  $B^{j_0}$  wzorami  $B_{i_0} := (I \setminus \{i_0\}, J, F_{i_0})$ , gdzie

$$F_{i_0} := \{(i, j) \in F : i \neq i_0\},$$

oraz  $B^{j_0} := (I, J \setminus \{j_0\}, F^{j_0})$ , gdzie

$$F^{j_0} := \{(i, j) \in F : j \neq j_0\}.$$

Mówimy, że szachownice  $B_{i_0}$  i  $B^{j_0}$  są otrzymane z szachownicy  $B$  przez USUNIĘCIE WIERSZA  $i_0$  ORAZ KOLUMNY  $j_0$ , odpowiednio. Zauważmy, że  $(B_{i_0})^{j_0} = (B^{j_0})_{i_0}$  i tę szachownicę oznaczamy  $B_{i_0}^{j_0}$ .

UWAGA.

Niech  $B = (I, J, F)$  będzie szachownicą,  $i_0 \in I$  i  $j_0 \in J$ . Jeśli  $(i_0, j) \in F$  dla każdego indeksu  $j \in J$ , to  $R_{B_{i_0}} = R_B$ . Podobnie, jeśli  $(i, j_0) \in F$  dla każdego indeksu  $i \in I$ , to  $R_{B^{j_0}} = R_B$ .

STWIERDZENIE 3.10.

Niech  $B = (I, J, F)$  będzie szachownicą. Jeśli  $I = I_1 \cup I_2$  i  $J = J_1 \cup J_2$ , przy czym  $I_1 \cap I_2 = \emptyset$  i  $J_1 \cap J_2 = \emptyset$  oraz

$$(I_1 \times J_2) \cup (I_2 \times J_1) \subseteq F,$$

to  $R_B = R_{B_1} \cdot R_{B_2}$ , gdzie

$$B_1 := (I_1, J_1, F \cap (I_1 \times J_1)) \quad \text{i} \quad B_2 := (I_2, J_2, F \cap (I_2 \times J_2)).$$

Innymi słowy, jeśli

$$B = \begin{array}{|c|c|} \hline B_1 & \diagup \diagdown \\ \hline \diagdown \diagup & B_2 \\ \hline \end{array}$$

to  $R_B = R_{B_1} \cdot R_{B_2}$ .

DOWÓD.

Ustalmy nieujemną liczbę całkowitą  $k$  i niech  $X$  będzie zbiorem wszystkich rozstawień  $k$  wież na szachownicy  $B$ . Jeśli dla nieujemnej liczby całkowitej  $l$  przez  $Y_l$  i  $Z_l$  oznaczymy zbiory wszystkich rozstawień  $l$  wież na szachownicach  $B_1$  i  $B_2$ , odpowiednio, to funkcja  $f : X \rightarrow \bigcup_{l \in [0, k]} Y_l \times Z_{k-l}$  dana wzorem

$$f(A) := (A \cap (I_1 \times J_1), A \cap (I_2 \times J_2)) \quad (A \in X),$$

MATEMATYKA DYSKRETNA

jest dobrze określona i jest bijekcją – funkcja odwrotna  $f^{-1} : \bigcup_{l \in [0, k]} Y_l \times Z_{k-l} \rightarrow X$  dana jest wzorem

$$f(A_1, A_2) := A_1 \cup A_2 \quad (A_1 \in Y_l, A_2 \in Z_{k-l}, l \in [0, k]).$$

Stąd

$$\begin{aligned} [T^k]R_B &= r^B(k) = |X| = \sum_{l \in [0, k]} |Y_l| \cdot |Z_{k-l}| \\ &= \sum_{l \in [0, k]} r^{B_1}(l) \cdot r^{B_2}(k-l) = [T^k](R_{B_1} \cdot R_{B_2}), \end{aligned}$$

co kończy dowód. □

**TWIERDZENIE 3.11.**

Jeśli  $B = (I, J, F)$  jest szachownicą oraz  $(i_0, j_0) \in (I \times J) \setminus F$ , to

$$R_B = R_{B'} + T \cdot R_{B_{i_0}^{j_0}},$$

gdzie  $B' := (I, J, F \cup \{(i_0, j_0)\})$ .

**DOWÓD.**

Ustalmy dodatnią liczbę całkowitą  $k$ . Niech  $X$  będzie zbiorem wszystkich rozstawień  $k$  wież na szachownicy  $B$ . Zauważmy, że  $X = X_1 \cup X_2$ , gdzie  $X_1$  jest zbiorem tych rozstawień  $A$ , dla których  $(i_0, j_0) \notin A$ , zaś  $X_2$  jest zbiorem tych rozstawień  $A$ , dla których  $(i_0, j_0) \in A$ . Oczywiście  $X_1 \cap X_2 = \emptyset$ . Ponadto  $|X_1| = r^{B'}(k)$  oraz  $|X_2| = r^{B_{i_0}^{j_0}}(k-1)$ , zatem

$$\begin{aligned} [T^k]R_B &= r^B(k) = |X| = |X_1| + |X_2| = r^{B'}(k) + r^{B_{i_0}^{j_0}}(k-1) \\ &= [T^k]R_{B'} + [T^{k-1}]R_{B_{i_0}^{j_0}} = [T^k]R_{B'} + [T^k](T \cdot R_{B_{i_0}^{j_0}}). \end{aligned}$$

Oczywiście

$$[T^0]R_B = 1 = 1 + 0 = [T^0]R_{B'} + [T^0](T \cdot R_{B_{i_0}^{j_0}}),$$

co kończy dowód. □

**DEFINICJA.**

NEGATYWEM SZACHOWNICY  $B = (I, J, F)$  nazywamy szachownicę  $\bar{B}$  daną wzorem

$$\bar{B} := (I, J, \bar{F}),$$

gdzie  $\bar{F} := (I \times J) \setminus F$ .

**TWIERDZENIE 3.12.**

Jeśli  $n$  jest nieujemną liczbą całkowitą oraz  $B = (I, J, F)$  jest szachownicą taką, że  $|I| = n = |J|$ , to

$$r^{\overline{B}}(n) = \sum_{k \in [0, n]} (-1)^k \cdot r_k^B \cdot (n - k)!.$$

**Dowód.**

Bez straty ogólności możemy założyć, że  $I = [1, n] = J$ . Niech  $B' := (I, J, \emptyset)$  oraz niech  $X$  i  $Y$  będą zbiorami wszystkich rozstawień  $n$  wież na szachownicach  $\overline{B}$  i  $B'$ , odpowiednio. Zauważmy, że

$$X = Y \setminus \bigcup_{i \in [1, n]} Y_i,$$

gdzie

$$Y_i := \{A \in Y : A \cap (\{i\} \times J) \cap F = \emptyset\} \quad (i \in [1, n]),$$

tzn.  $Y_i$  jest zbiorem tych rozstawień  $A$ , dla których wieża stojąca w wierszu  $i$  stoi na polu dozwolonym w szachownicy  $B$ . Ustalmy liczbę  $k \in [0, n]$ . Zbiór  $Z_k$  rozstawień  $k$  wież na szachownicy  $B$  możemy przedstawić w postaci

$$Z_k = \bigcup_{I' \in C_{I, k}} Z_{I'},$$

gdzie

$$Z_{I'} := \{A \in Z_k : A \subseteq I' \times J\} \quad (I' \in C_{I, k}),$$

tzn.  $Z_{I'}$  jest zbiorem tych rozstawień  $A$   $k$  wież na szachownicy  $B$ , w których stoją one we wierszach o indeksach należących do zbioru  $I'$ . Zauważmy, że

$$\left| \bigcap_{i \in I'} Y_i \right| = (n - k)! \cdot |Z_{I'}|$$

dla dowolnego podzbioru  $I' \in C_{I, k}$ , zatem

$$\sum_{I' \in C_{I, k}} \left| \bigcap_{i \in I'} Y_i \right| = \sum_{I' \in C_{I, k}} (n - k)! \cdot |Z_{I'}| = (n - k)! \cdot |Z_k| = (n - k)! \cdot r^B(k),$$

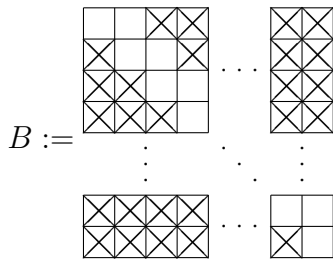
zatem teza wynika ze wzoru włączeń i wyłączeń (zauważmy, że  $|Y| = n! = 1 \cdot n! = r^B(0) \cdot n!$ ).  $\square$

PRZYKŁAD.

Ustalmy nieujemną liczbę całkowitą  $n$ . Niech  $a(n)$  oznacza liczbę permutacji  $\sigma \in P_n$  takich, że  $\sigma(i) \neq i, i + 1$  dla wszystkich liczb  $i \in [1, n]$ . Z powyższego twierdzenia wynika, że

$$a(n) = \sum_{k \in [0, n]} (-1)^k \cdot r^B(k) \cdot (n - k)!,$$

gdzie



jest szachownicą o  $n$  wierszach i  $n$  kolumnach. Ponumerujemy pola dozwolone powyższej szachownicy liczbami całkowitymi ze zbioru  $[1, 2n - 1]$  poczynając od lewego górnego rogu. Dla ustalonej liczby  $k \in [1, n]$  rozstawienia  $k$  wież na szachownicy  $B$  są parametryzowane za pomocą  $k$ -elementowych podzbiorów zbioru  $[1, 2 \cdot n - k]$ . Istotnie, rozstawieniu wież na polach o numerach  $i_1 < \dots < i_k$  możemy przyporządkować podzbiór  $\{i_1, i_2 - 1, \dots, i_k - (k - 1)\}$ . Stąd

$$r_B = \sum_{k \in [0, n]} \binom{2 \cdot n - k}{k} \cdot T^k,$$

więc

$$a(n) = \sum_{k \in [0, n]} (-1)^k \cdot \binom{2 \cdot n - k}{k} \cdot (n - k)!.$$

4. SYSTEMY REPREZENTANTÓW I TWIERDZENIE HALLA

DEFINICJA.

SYSTEMEM REPREZENTANTÓW ciągu  $(A_1, \dots, A_n)$  podzbiorów zbioru  $X$  nazywamy każdy ciąg  $(a_1, \dots, a_n)$  elementów zbioru  $X$  taki, że  $a_i \in A_i$  dla każdego indeksu  $i \in [1, n]$  oraz  $a_i \neq a_j$  dla wszystkich indeksów  $i, j \in [1, n]$  takich, że  $i \neq j$ .

UWAGA.

Niech  $(A_1, \dots, A_n)$  będzie ciągiem podzbiorów zbioru  $X$  oraz niech  $B := ([1, n], X, F)$ , gdzie

$$F := \{(i, a) \in [1, n] \times X : a \notin A_i\}.$$

Wtedy ciąg  $(A_1, \dots, A_n)$  posiada system reprezentantów wtedy i tylko wtedy, gdy  $\deg R_B = n$ . Ponadto ilość systemów reprezentantów jest równa  $[T^n]R_B$ .

DEFINICJA.

Mówimy, że ciąg  $(A_1, \dots, A_n)$  podzbiorów zbioru  $X$  spełnia WARUNEK HALLA, jeśli

$$\left| \bigcup_{i \in I} A_i \right| \geq |I|$$

dla każdego podzbioru  $I \subseteq [1, n]$ .

TWIERDZENIE 4.1 (HALL).

Ciąg  $(A_1, \dots, A_n)$  podzbiorów zbioru  $X$  posiada system reprezentantów wtedy i tylko wtedy, gdy spełnia warunek Halla.

DOWÓD.

Jest oczywiste, że jeśli ciąg  $(A_1, \dots, A_n)$  posiada system reprezentantów, to spełnia warunek Halla. Pokażemy teraz, że jeśli ciąg  $(A_1, \dots, A_n)$  spełnia warunek Halla, to posiada system reprezentantów. Jeśli  $|A_i| = 1$  dla każdego indeksu  $i \in [1, n]$ , to z warunku Halla wynika, że  $A_i \cap A_j = \emptyset$  dla wszystkich indeksów  $i, j \in [1, n]$  takich, że  $i \neq j$ , więc teza jest oczywista. Załóżmy zatem, że istnieje indeks  $i \in [1, n]$  taki, że  $|A_i| > 1$ . Bez straty ogólności możemy przyjąć, że  $|A_1| > 1$ . Ustalmy elementy  $a', a'' \in A_1$  takie, że  $a' \neq a''$ . Niech  $A'_1 := A_1 \setminus \{a'\}$  oraz  $A''_1 := A_1 \setminus \{a''\}$ . Dla zakończenia dowodu wystarczy pokazać, że jeden z ciągów  $(A'_1, A_2, \dots, A_n)$  i  $(A''_1, A_2, \dots, A_n)$  spełnia warunek Halla oraz skorzystać z założenia indukcyjnego.

Przypuśćmy, że ciąg  $(A'_1, A_2, \dots, A_n)$  nie spełnia warunku Halla. Wtedy istnieje podzbiór  $I \subseteq [2, n]$  taki, że  $|B| \leq |I|$ , gdzie

$$B := A'_1 \cup \bigcup_{i \in I} A_i.$$

Aby pokazać, że ciąg  $(A_1'', A_2, \dots, A_n)$  spełnia warunek Halla wystarczy pokazać, że

$$\left| A_1'' \cup \bigcup_{i \in J} A_i \right| > |J|$$

dla dowolnego podzbioru  $J \subseteq [2, n]$ . Ustalmy podzbiór  $J \subseteq [2, n]$  oraz niech

$$C := A_1'' \cup \bigcup_{i \in J} A_i.$$

Zauważmy, że

$$B \cup C = A_1 \cup \bigcup_{i \in I \cup J} A_i,$$

skąd  $|B \cup C| > |I \cup J|$ . Z drugiej strony

$$B \cap C \supseteq \bigcup_{i \in I \cap J} A_i,$$

więc  $|B \cap C| \geq |I \cap J|$ . W efekcie

$$|B| + |C| = |B \cup C| + |B \cap C| > |I \cup J| + |I \cap J| = |I| + |J|,$$

co kończy dowód wobec nierówności  $|B| \leq |I|$ . □

#### STWIERDZENIE 4.2.

Niech  $(A_1, \dots, A_n)$  będzie ciągiem podzbiorów zbioru  $X$ . Jeśli istnieje liczba  $d \in \mathbb{N}_+$  taka, że  $|A_i| \geq d$  dla każdego indeksu  $i \in [1, n]$  oraz

$$|\{i \in [1, n] : x \in A_i\}| \leq d$$

dla każdego elementu  $x \in X$ , to ciąg  $(A_1, \dots, A_n)$  spełnia warunek Halla.

#### Dowód.

Ustalmy podzbiór  $I \subseteq [1, n]$  oraz niech  $B := \bigcup_{i \in I} A_i$ . Niech

$$M := \{(i, x) \in I \times X : x \in A_i\}.$$

Wtedy  $|M| \geq d \cdot |I|$ , gdyż  $|A_i| \geq d$  dla każdego indeksu  $i \in I$ . Zarazem z drugiego warunku wynika, że  $|M| \leq |B| \cdot d$ , co oznacza, że  $|B| \geq |I|$  i kończy dowód. □



DEFINICJA.

Niech  $m$  i  $n$  będą nieujemnymi liczbami całkowitymi. PROSTOKĄTEM ŁACIŃSKIM o  $m$  wierszach i  $n$  kolumnach nazywamy każdą  $m \times n$ -macierz  $A = [a_{i,j}]$  o współczynnikach w zbiorze  $[1, n]$  taką, że  $a_{i_1, j_1} \neq a_{i_2, j_2}$  dla wszystkich indeksów  $i_1, i_2 \in [1, m]$  oraz  $j_1, j_2 \in [1, n]$  takich, że  $i_1 = i_2$  i  $j_1 \neq j_2$  lub  $j_1 = j_2$  i  $i_1 \neq i_2$ .

PRZYKŁAD.

Macierz

$$\begin{bmatrix} 4 & 1 & 5 & 3 & 2 \\ 1 & 2 & 4 & 5 & 3 \\ 2 & 5 & 3 & 4 & 1 \end{bmatrix}$$

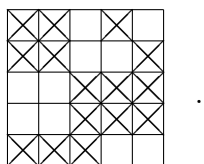
jest prostokątem łacińskim.

DEFINICJA.

Niech  $A$  będzie prostokątem łacińskim o  $m$  wierszach i  $n$  kolumnach. Mówimy, że prostokąt łaciński  $B$  o  $p$  wierszach i  $q$  kolumnach jest ROZSZERZENIEM PROSTOKĄTA  $A$ , jeśli  $p \geq m$ ,  $q = n$ , oraz  $b_{i,j} = a_{i,j}$  dla wszystkich indeksów  $i \in [1, m]$  i  $j \in [1, n]$ .

PRZYKŁAD.

Ilość sposobów na które można rozszerzyć prostokąt  $A$  z poprzedniego przykładu do prostokątu o 4 wierszach jest równa ilości rozstawień 5 wież na następującej szachownicy



TWIERDZENIE 4.3.

Jeśli  $m$  i  $n$  są nieujemnymi liczbami całkowitymi, to każdy prostokąt łaciński o  $m$  wierszach i  $n$  kolumnach można rozszerzyć do kwadratu łacińskiego.

DOWÓD.

Bez straty ogólności możemy założyć, że  $m \leq n$ .

Jeśli  $m = n$ , to nie ma co dowodzić, załóżmy zatem, że  $m < n$ .

Niech  $A$  będzie prostokątem łacińskim o  $m$  wierszach i  $n$  kolumnach. Wystarczy udowodnić, że prostokąt  $A$  można rozszerzyć do prostokąta łacińskiego o  $m + 1$  wierszach. Niech

$$A_j := [1, n] \setminus \{a_{i,j} : i \in [1, m]\}$$

dla indeksu  $j \in [1, n]$ . Zauważmy, że  $|A_j| = n - m$ . Podobnie,

$$|\{j \in [1, n] : i \in A_j\}| = n - m$$

dla każdego indeksu  $i \in [1, n]$ . Korzystając z poprzedniego stwierdzenia wiemy, że ciąg  $(A_1, \dots, A_n)$  posiada system reprezentantów  $(a_1, \dots, a_n)$ . Wtedy macierz  $B$  o  $m + 1$  wierszach i  $n$  kolumnach dana wzorem

$$b_{i,j} := \begin{cases} a_{i,j} & \text{jeśli } i \in [1, m] \text{ i } j \in [1, n], \\ a_i & \text{jeśli } i = m + 1 \text{ i } j \in [1, n], \end{cases} \quad (i \in [1, m + 1], j \in [1, n]),$$

jest prostokątem łańcuskim, który jest rozszerzeniem prostokąta  $A$ .  $\square$

DEFINICJA.

Niech  $n$  będzie nieujemna liczba całkowita. Macierz  $P$  o  $n$  wierszach i  $n$  kolumnach o współczynnikach w zbiorze  $\mathbb{N}$  nazywamy MACIERZĄ PERMUTACJI, jeśli  $\sum_{j \in [1, n]} p_{i,j} = 1$  dla każdego indeksu  $i \in [1, n]$  oraz  $\sum_{i \in [1, n]} p_{i,j} = 1$  dla każdego indeksu  $j \in [1, n]$ .

TWIERDZENIE 4.4 (BIRKHOFF).

Niech  $A$  będzie macierzą o  $n$  wierszach i  $n$  kolumnach oraz współczynnikach w zbiorze  $\mathbb{N}$ . Jeśli istnieje  $l \in \mathbb{N}$  takie, że  $\sum_{j \in [1, n]} a_{i,j} = l$  dla każdego indeksu  $i \in [1, n]$  oraz  $\sum_{i \in [1, n]} a_{i,j} = l$  dla każdego indeksu  $j \in [1, n]$ , to macierz  $A$  jest sumą  $l$  macierzy permutacji.

DOWÓD.

Dla indeksu  $i \in [1, n]$  niech

$$A_i := \{j \in [1, n] : a_{i,j} \neq 0\}.$$

Pokażemy, że ciąg  $(A_1, \dots, A_n)$  spełnia warunek Halla. Istotnie, jeśli  $I \subseteq [1, n]$ , to

$$\begin{aligned} |I| \cdot l &= \sum_{i \in I} \sum_{j \in [1, n]} a_{i,j} = \sum_{i \in I} \sum_{j \in \bigcup_{p \in I} A_p} a_{i,j} \\ &= \sum_{j \in \bigcup_{p \in I} A_p} \sum_{i \in I} a_{i,j} \leq \left| \bigcup_{p \in I} A_p \right| \cdot l. \end{aligned}$$

Niech  $(a_1, \dots, a_n)$  będzie system reprezentantów dla ciągu  $(A_1, \dots, A_n)$ . Wtedy macierz  $P$  dana wzorem

$$p_{i,j} := \begin{cases} 1 & \text{jeśli } j = a_i \text{ i } i \in [1, n], \\ 0 & \text{w przeciwnym wypadku,} \end{cases} \quad (i, j \in [1, n]),$$

## MATEMATYKA DYSKRETNA

V jest macierzą permutacji i teza wynika z założenia indukcyjnego zastosowanego do macierzy  $A - P$ .  $\square$

5. WAŻNE CIĄGI LICZBOWE

5.1. LICZBY STIRLINGA

DEFINICJA.

Niech  $k \in \mathbb{N}$ . ROZKŁADEM ZBIORU  $X$  NA  $k$  CZĘŚCI nazywamy każdą rodzinę  $\mathcal{A} \subseteq 2^X \setminus \{\emptyset\}$  taką, że  $|\mathcal{A}| = k$ ,  $X = \bigcup_{A \in \mathcal{A}} A$  oraz  $A \cap B = \emptyset$  dla wszystkich zbiorów  $A, B \in \mathcal{A}$  takich, że  $A \neq B$ .

OZNACZENIE.

Jeśli  $n, k \in \mathbb{N}$ , to przez  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$  oznaczamy liczbę rozkładów zbioru  $[1, n]$  na  $k$  części.

PRZYKŁAD.

$\left\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right\} = 1$  oraz  $\left\{ \begin{smallmatrix} n \\ 0 \end{smallmatrix} \right\} = 0$  dla wszystkich liczb  $n \in \mathbb{N}_+$ .

PRZYKŁAD.

$\left\{ \begin{smallmatrix} 0 \\ 1 \end{smallmatrix} \right\} = 0$  oraz  $\left\{ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \right\} = 1$  dla wszystkich liczb  $n \in \mathbb{N}_+$ .

PRZYKŁAD.

$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = 0$  dla wszystkich liczb  $n, k \in \mathbb{N}$  takich, że  $n < k$ .

PRZYKŁAD.

$\left\{ \begin{smallmatrix} n \\ n \end{smallmatrix} \right\} = 1$  dla wszystkich liczb  $n \in \mathbb{N}$ .

PRZYKŁAD.

$\left\{ \begin{smallmatrix} n \\ n-1 \end{smallmatrix} \right\} = \binom{n}{2}$  dla wszystkich liczb  $n \in \mathbb{N}$ .

PRZYKŁAD.

$\left\{ \begin{smallmatrix} 4 \\ 2 \end{smallmatrix} \right\} = 7$ .

TWIERDZENIE 5.1.

Jeśli  $n, k \in \mathbb{N}_+$ , to

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = k \cdot \left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\} + \left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\}.$$

DOWÓD.

Niech  $X$  będzie zbiorem wszystkich rozkładów zbioru  $[1, n]$  na  $k$  części. Podobnie, niech  $Y_1$  będzie zbiorem wszystkich rozkładów zbioru  $[1, n-1]$  na  $k-1$  części i niech  $Y_2$  będzie zbiorem wszystkich rozkładów zbioru  $[1, n-1]$  na  $k$  części. Rozważmy funkcję  $f : X \rightarrow Y_1 \cup Y_2$  daną wzorem

$$f(\mathcal{A}) := \{A \setminus \{n\} : A \in \mathcal{A}\}$$

dla rodziny  $\mathcal{A} \in X$ . Funkcja ta jest poprawnie określona. Istotnie, jeśli  $\{n\} \in \mathcal{A}$ , to  $f(\mathcal{A}) \in Y_1$ . W przeciwnym wypadku,  $f(\mathcal{A}) \in Y_2$ . Ponadto, jeśli  $\mathcal{B} \in Y_1$ ,

to  $|f^{-1}(\mathcal{B})| = 1$ , podczas gdy  $|f^{-1}(\mathcal{B})| = k$  dla rodziny  $\mathcal{B} \in Y_2$ , co kończy dowód. Istotnie,

$$f^{-1}(\mathcal{B}) = \{\mathcal{B} \cup \{\{n\}\}\}$$

jeśli  $\mathcal{B} \in Y_1$ , oraz

$$f^{-1}(\mathcal{B}) = \{\{B_1 \cup \{n\}, \dots, B_k\}, \dots, \{B_1, \dots, B_k \cup \{n\}\}\}$$

jeśli  $\mathcal{B} = \{B_1, \dots, B_k\} \in Y_2$ . □

**OZNACZENIE.**

Dla liczby  $k \in \mathbb{N}$  niech  $\mathcal{S}_k$  będzie funkcją tworzącą ciąg  $(\binom{n}{k})_{n \in \mathbb{N}}$ .

**WNIOSEK 5.2.**

Jeśli  $k \in \mathbb{N}$ , to

$$\mathcal{S}_k = \frac{T^k}{\prod_{i \in [1, k]} (1 - i \cdot T)}.$$

**DOWÓD.**

Dla  $k = 0$  teza jest oczywista, załóżmy zatem, że  $k > 0$ . Wtedy

$$\begin{aligned} \mathcal{S}_k &= \sum_{n \in \mathbb{N}} \binom{n}{k} \cdot T^n = \sum_{n \in \mathbb{N}_+} \left( \binom{n-1}{k-1} + k \cdot \binom{n-1}{k} \right) \cdot T^n \\ &= T \cdot \sum_{n \in \mathbb{N}} \binom{n}{k-1} \cdot T^n + k \cdot T \cdot \sum_{n \in \mathbb{N}} \binom{n}{k} \cdot T^n \\ &= T \cdot \mathcal{S}_{k-1} + k \cdot T \cdot \mathcal{S}_k, \end{aligned}$$

skąd

$$\mathcal{S}_k = \frac{T}{1 - k \cdot T} \cdot \mathcal{S}_{k-1},$$

więc teza wynika przez prostą indukcję. □

**STWIERDZENIE 5.3.**

Jeśli  $A$  i  $B$  są zbiorami, to liczba surjekcji  $\varphi : A \rightarrow B$  jest równa  $k! \cdot \binom{n}{k}$ , gdzie  $n := |A|$  i  $k := |B|$ .

**DOWÓD.**

Bez straty ogólności możemy założyć, że  $A = [1, n]$  oraz  $B = [1, k]$ . Niech  $X$  będzie zbiorem wszystkich surjekcji  $\varphi : A \rightarrow B$ , zaś niech  $Y$  będzie zbiorem

wszystkich podziałów zbioru  $A$  na  $k$  części. Wtedy  $|Y| = \binom{n}{k}$ . Rozważmy funkcję  $f : X \rightarrow Y$  daną wzorem

$$f(\varphi) := \{\varphi^{-1}(1), \dots, \varphi^{-1}(k)\}$$

dla funkcji  $\varphi \in X$ . Wtedy funkcja  $f$  jest poprawnie określona. Ponadto dla podziału  $\mathcal{A} \in Y$  mamy  $|f^{-1}(\mathcal{A})| = k!$ . Istotnie, jeśli  $\mathcal{A} = \{A_1, \dots, A_k\} \in Y$ , to

$$f^{-1}(\mathcal{A}) = \{\varphi_\sigma : \sigma \in P_k\},$$

gdzie dla permutacji  $\sigma \in P_k$  funkcja  $\varphi_\sigma : [1, n] \rightarrow [1, k]$  dana jest wzorem:

$$\varphi_\sigma(a) := \sigma(i),$$

jeśli  $a \in A_i$  dla liczby  $i \in [1, k]$ . Stąd

$$|X| = |P_k| \cdot |Y| = k! \cdot \binom{n}{k},$$

co kończy dowód. □

**WNIOSEK 5.4.**

Jeśli  $n, k \in \mathbb{N}$ , to

$$k^n = \sum_{i \in [0, k]} i! \cdot \binom{k}{i} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\} = \sum_{i \in [0, k]} \prod_{j \in [0, i]} (k - j + 1) \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\}.$$

**Dowód.**

Niech  $X$  będzie zbiorem wszystkich funkcji  $\varphi : [1, n] \rightarrow [1, k]$ . Wiemy, że  $|X| = k^n$ . Z drugiej strony  $X = \bigcup_{i \in [0, k]} X_i$ , gdzie

$$X_i := \{\varphi \in X : |\varphi([1, n])| = i\}$$

dla liczby  $i \in [0, k]$ . Z poprzedniego stwierdzenia wiemy, że

$$|X_i| = \binom{k}{i} \cdot i! \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\}$$

dla wszystkich liczb  $i \in [0, k]$ . Ponieważ,  $X_i \cap X_j = \emptyset$  dla wszystkich liczb  $i, j \in [0, k]$  takich, że  $i \neq j$ , więc to kończy dowód. □

**WNIOSEK 5.5.**

Jeśli  $n \in \mathbb{N}$  i  $x \in \mathbb{C}$ , to

$$x^n = \sum_{i \in [0, n]} i! \cdot \binom{x}{i} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\} = \sum_{i \in [0, n]} \prod_{j \in [0, i]} (x - j + 1) \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\}.$$

Dowód.

Wystarczy zauważyć, że

$$\sum_{i \in [0, k]} i! \cdot \binom{k}{i} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\} = \sum_{i \in [0, n]} i! \cdot \binom{k}{i} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\}$$

dla każdej liczby  $k \in \mathbb{N}$  (gdyż  $\binom{k}{i} = 0$  dla każdej liczby  $i \in [k + 1, \infty[$  oraz  $\left\{ \begin{matrix} n \\ i \end{matrix} \right\} = 0$  dla każdej liczby  $i \in [n + 1, \infty[$ ) i skorzystać z poprzedniego wniosku.  $\square$

## 5.2. LICZBY BELLA

DEFINICJA.

Jeśli  $n \in \mathbb{N}$ , to  $n$ -TĄ LICZBĄ BELLA nazywamy ilość rozkładów zbioru  $[1, n]$ , tzn.

$$B_n := \sum_{k \in \mathbb{N}} \left\{ \begin{matrix} n \\ k \end{matrix} \right\}.$$

STWIERDZENIE 5.6.

Jeśli  $n \in \mathbb{N}$ , to

$$B_n = \frac{1}{e} \cdot \sum_{k \in \mathbb{N}} \frac{k^n}{k!}.$$

Dowód.

Korzystając z Wniosku 5.4 otrzymujemy, że

$$\begin{aligned} \sum_{k \in \mathbb{N}} \frac{k^n}{k!} &= \sum_{k \in \mathbb{N}} \sum_{i \in [0, k]} \frac{i!}{k!} \cdot \binom{k}{i} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\} = \sum_{i \in \mathbb{N}} \sum_{k \in [i, \infty[} \frac{1}{(k - i)!} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\} \\ &= \sum_{i \in \mathbb{N}} \sum_{k \in \mathbb{N}} \frac{1}{k!} \cdot \left\{ \begin{matrix} n \\ i \end{matrix} \right\} = e \cdot B_n, \end{aligned}$$

co kończy dowód.  $\square$

STWIERDZENIE 5.7.

Jeśli  $n \in \mathbb{N}$ , to

$$B_{n+1} = \sum_{k \in [0, n]} \binom{n}{k} \cdot B_{n-k}.$$

Dowód.

Niech  $X$  będzie zbiorem wszystkich rozkładów zbioru  $[1, n + 1]$ . Ponadto, dla liczby  $k \in [0, n]$  definiujemy zbiór  $X_k$  wzorem

$$X_k := \{A \in X : |A| = k + 1 \text{ dla zbioru } A \in \mathcal{A} \text{ takiego, że } n + 1 \in A\}.$$

Oczywiście  $X_i \cap X_j = \emptyset$  dla wszystkich indeksów  $i, j \in [0, k]$  takich, że  $i \neq j$ . Ponadto

$$X_k = \binom{n}{k} \cdot B_{n-k}$$

dla wszystkich indeksów  $k \in [0, n]$ , co kończy dowód.  $\square$

STWIERDZENIE 5.8.

Jeśli liczby  $b_{n,m}$ ,  $m \in \mathbb{N}$ ,  $n \in [0, m]$ , są zdefiniowane następująco:

$$b_{0,0} := 1,$$

$$b_{0,m} := b_{m-1,m-1}, \quad m \in \mathbb{N}_+,$$

$$b_{n,m} := b_{n-1,m-1} + b_{n-1,m}, \quad m \in \mathbb{N}_+, \quad n \in [1, m],$$

to  $b_{n,n} = B_{n+1}$  dla wszystkich liczb  $n \in \mathbb{N}$ .

DOWÓD.

Udowodnimy indukcyjnie, że

$$b_{n,m} = \sum_{k \in [0, n]} \binom{n}{k} \cdot B_{m-k}$$

dla wszystkich liczb  $m \in \mathbb{N}$  oraz  $n \in [0, m]$ . W szczególności,

$$b_{n,n} = b_{0,n+1} = B_{n+1}$$

dla wszystkich liczb  $n \in \mathbb{N}$ , co zakończy dowód.

Jeśli  $n = 0 = m$ , to teza jest oczywista. Załóżmy zatem, że  $m > 0$ . Jeśli  $n = 0$ , to na mocy założenia indukcyjnego i poprzedniego stwierdzenia

$$b_{0,m} = b_{m-1,m-1} = B_m = \sum_{k \in [0, m]} \binom{m}{k} \cdot B_{m-k},$$

załóżmy zatem, że  $n \in [1, m]$ . Wtedy z założenia indukcyjnego wynika, że

$$\begin{aligned} b_{n,m} &= b_{n-1,m-1} + b_{n-1,m} \\ &= \sum_{k \in [0, n-1]} \binom{n-1}{k} \cdot B_{m-1-k} + \sum_{k \in [0, n-1]} \binom{n-1}{k} \cdot B_{m-k} \\ &= B_m + \sum_{k \in [1, n-1]} \left( \binom{n-1}{k-1} + \binom{n-1}{k} \right) \cdot B_{m-k} + B_{m-n} \\ &= \sum_{k \in [0, n]} \binom{n}{k} \cdot B_{m-k}, \end{aligned}$$

co kończy dowód.  $\square$



## MATEMATYKA DYSKRETNA

DEFINICJA.

Powyższy sposób liczenia liczb Bella nazywamy TRÓJKĄTEM BELLA.

PRZYKŁAD.

Z następującej tablicy

1	1	2	5	15
	2	3	7	20
		5	10	27
			15	37
				52

wynika, że  $B_1 = 1$ ,  $B_2 = 2$ ,  $B_3 = 5$ ,  $B_4 = 15$  i  $B_5 = 52$ .