Grzegorz Bobiński

Matematyka Dyskretna

Wydział Matematyki i Informatyki
Uniwersytet Mikołaja Kopernika w Toruniu
2023

Spis treści

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 $x_1, \ldots, x_n \in \mathbb{Z}$, 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 $F : I \to \mathbb{C}$ jest funkcją, to definiujemy

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

gdzie $\sigma : [1, |I|] \to I$ jest ustaloną bijekcją (powyższe definicje nie zależą od wyboru bijekcji σ).
Ogólniej, jeśli I jest zbiorem i $F : I \to \mathbb{C}$ jest funkcją taką, że $|I_0| < \infty$, gdzie

$$I_0 := \{i \in I : F(i) \neq 0\}$$

(funkcje takie będziemy nazywać SUMOWALNYMI), to definiujemy

$$\sum_{i\in I} F(i) := \sum_{i\in I_0} F(i).$$

Analogicznie, jeśli I jest zbiorem i $F : I \to \mathbb{C} \setminus \{0\}$ jest funkcją taką, że $|I_1| < \infty$, gdzie

$$I_1 := \{i \in I : F(i) \neq 1\},$$

(funkcje takie będziemy nazywać WYMNAŻALNYMI), to definiujemy

$$\prod_{i \in I} F(i) := \prod_{i \in I_1} F(i).$$

Zauważmy, że jeśli I jest zbiorem, $F : I \to \mathbb{N}$, $x_i \in \mathbb{N} \setminus \{0, 1\}$, $i \in I$, oraz funkcja $G : I \to \mathbb{N}$ dana jest wzorem

$$G(i) := x_i^{F(i)} \qquad (i \in I),$$

to funkcja F jest sumowalna wtedy i tylko wtedy, gdy funkcja G jest wymnażalna.

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

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. □

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. □

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

$$|b| = |k| \cdot |a| \geq |a|.$$ □

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 $b \cdot c = (k \cdot c) \cdot a$. □

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 $b \cdot c = k \cdot (a \cdot c)$.

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 $b = k \cdot a$. □

Oznaczenie.

Jeśli a jest liczbą całkowitą, to definiujemy

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

Fakt 1.10.

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

Dowód.

Oczywiste. □

Definicja.

Niech a i b będą liczbami całkowitymi takimi, że $b \neq 0$. Ilorazem 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 1.11.

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 $\operatorname{sign} b \cdot b = |b| \geq 1$, gdyż $b \neq 0$. Stąd

$$(-\operatorname{sign} b \cdot |a|) \cdot b = -|a| \cdot (\operatorname{sign} b \cdot |b|) \leq -|a| \cdot 1 = -|a| \leq a.$$ □

Fakt 1.12.

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 $q_1 = q_2$. □

Oznaczenie.

Jeśli a i b są liczbami całkowitymi takimi, że $b \neq 0$, to przez $a \operatorname{div} b$ 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 $a - (a \operatorname{div} b) \cdot b$.

Oznaczenie.

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

Stwierdzenie 1.13.

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

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

Dowód.

Równość

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

wynika natychmiast z definicji reszty. Z definicji ilorazu całkowitego wiemy, że $(a \operatorname{div} b) \cdot b \leq a$, 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 $(a \operatorname{div} b) \cdot b \leq a - |b|$. Jeśli $q := a \operatorname{div} b + \operatorname{sign} b$, to

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

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

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

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

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

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 liczbami całkowitymi takimi, że

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

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

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

Dowód.

Ze Stwierdzenia 1.13 wiemy, że

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

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 $a \bmod b = 0$.

Dowód.

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

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

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

Wniosek 1.17 (Zapis w systemie o podstawie b).

Jeśli a i b są dodatnimi liczbami całkowitymi takimi, że $b > 1$, to istnieją jednoznacznie wyznaczone liczby całkowite nieujemne n, c_0, …, c_n takie, że

$$a = \sum_{i \in [0,n]} c_i \cdot b^i,$$

$c_0, \ldots, c_n \in [0, b-1]$ i $c_n \neq 0$.

Dowód.

Istnienie udowodnimy przez indukcję ze względu na a.

Jeśli $a < b$, to $n = 0$ i $c_0 = a$.

Załóżmy zatem, że $a \geq b$, i niech $c_0 := a \bmod b$ i $a' := a \operatorname{div} b$. Wtedy $0 < a' < a$ (gdyż $a \geq b$ i $b > 1$), więc z założenia indukcyjnego istnieją całkowite liczby nieujemne n, c_1, …, c_n takie, że $n > 0$ i

$$a' = \sum_{i \in [1,n]} c_i \cdot b^{i-1},$$

$c_1, \ldots, c_n \in [0, b-1]$ i $c_n \neq 0$. Ze Stwierdzenia 1.13 otrzymujemy, że $c_0 \in [0, b-1]$ oraz

$$a = a' \cdot b' + c_0 = \sum_{i \in [1,n]} c_i \cdot b^i + c_0 = \sum_{i \in [0,n]} c_i \cdot b^i,$$

co kończy dowód istnienia.

Jednoznaczność również udowodnimy przez indukcję ze względu na a.

Załóżmy najpierw, że $a < b$. Jeśli

$$a = \sum_{i \in [0,n]} c_i \cdot b^i,$$

$n \in \mathbb{N}$, $c_0, \ldots, c_n \in [0, b-1]$ i $c_n \neq 0$, to

$$b > a \geq c_n \cdot b^n,$$

skąd natychmiast wynika, że $n = 0$ i $c_0 = a$, gdyż $b > 1$.

Załóżmy teraz, że $a \geq b$ oraz

$$\sum_{i \in [0,n]} c_i \cdot b^i = a = \sum_{i \in [0,m]} d_i \cdot b^i$$

dla $n, m \in \mathbb{N}$, $c_0, \ldots, c_n, d_0, \ldots, d_m \in [0, b-1]$ takich, że $c_n \neq 0 \neq d_m$. Z Wniosku 1.15 wynika, że

$$c_0 = a \bmod b = d_0 \qquad \text{i} \qquad \sum_{i \in [1,n]} c_i \cdot b^{i-1} = a \operatorname{div} b = \sum_{i \in [1,m]} d_i \cdot b^{i-1}.$$

Ponieważ $a \operatorname{div} b < a$ (gdyż $b > 1$), więc z założenia indukcyjnego otrzymujemy, że $m = n$ oraz $c_i = d_i$ dla każdego $i \in [1, m]$.

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 1.18.

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 $0 < |a| + |b| = \operatorname{sign} a \cdot a + \operatorname{sign} b \cdot b$, więc $I \neq \varnothing$. 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

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

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 1.19.

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 $d_1 = d_2$. □

Oznaczenie.

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

Wniosek 1.20.

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

Dowód.

Z Faktu 1.18 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 1.19 implikuje, że $k \cdot a + l \cdot b = \gcd(a, b)$. □

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

Dowód.
Ćwiczenie. □

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

Dowód.
Ćwiczenie. □

Lemat 1.21.
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

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

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 cześć 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 1.22.
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 $\gcd(a, b) = 1$. □

Wniosek 1.23.
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 1.20 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. □

Wniosek 1.24.

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

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

Dowód.

Udowodnimy tezę przez indukcję ze względu na n.

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

Załóżmy zatem, że $n > 0$, oraz, że

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

Z Wniosku 1.20 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

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

co kończy dowód na mocy Lematu 1.22. □

Uwaga.

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

Wniosek 1.25.

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 $\prod_{i \in \varnothing} a_i = 1$.

Załóżmy zatem, że $n > 0$ oraz że wiemy już, iż

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

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 1.24 wiemy, że $\gcd(\prod_{i \in [1,n-1]} a_i, a_n) = 1$, zatem na mocy Wniosku 1.20 istnieją liczby całkowite k i l takie, że

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

Wtedy

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

co kończy dowód. □

Stwierdzenie 1.26.

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 1.20 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 1.22. □

1.3. Podstawowe 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 1.27.

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

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

(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

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

Lemat 1.28.

Jeśli a jest dodatnią liczbą całkowitą, to istnieją liczby pierwsze $p_1, \ldots, p_n$, $n \in \mathbb{N}$, 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 ($n := 0$).

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

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

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

Załóżmy 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 $p_1, \ldots, p_{n_1}$, $n_1 \in \mathbb{N}$, 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 $p_{n_1+1}, \ldots, p_{n_1+n_2}$, $n_2 \in \mathbb{N}$, takie, że

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

Niech $n := n_1 + n_2$. Wtedy

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

Wniosek 1.29.

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. Załóżmy zatem, że $a \neq 0$. Z Lematu 1.28 wiemy, że istnieją liczby pierwsze $p_1, \ldots, p_n$, $n \in \mathbb{N}$, takie, że

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

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

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 1.30.
Istnieje nieskończenie wiele liczb pierwszych.

Dowód (Euklides).
Przypuśćmy przez sprzeczność, że $|\mathbb{P}| < \infty$. Niech

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

Ponieważ $a > 1$, więc na mocy Lematu 1.29 istnieje liczba pierwsza p taka, że $p \mid a$. Oczywiście $p \mid \prod_{q \in \mathbb{P}} q$. Stąd

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

na mocy Faktu 1.7. Zatem Fakt 1.4 prowadzi do wniosku, że $p = 1$, co jest sprzeczne z Lematem 1.27 (1). □

Stwierdzenie 1.31.
Niech $a_1, \ldots, a_n, n \in \mathbb{N}$, 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 $p \mid a_i$. W szczególności, $n > 0$.

Dowód.
Udowodnimy tezę przez indukcję ze względu na n. Zauważmy, że ponieważ $p > 1$ na mocy Lematu 1.27 (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 1.27 (2). Korzystając z Wniosku 1.23 otrzymujemy, że $p \mid \prod_{i\in[1,n-1]} a_i$, zatem teza wynika z założenia indukcyjnego. □

Twierdzenie 1.32 (Podstawowe Twierdzenie Arytmetyki).
Jeśli a jest dodatnią liczbą całkowitą, to istnieje jednoznacznie wyznaczona funkcja sumowalna $\alpha : P \to \mathbb{N}$ taka, że

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

Dowód.
1° Istnienie.

Z Lematu 1.28 wiemy, że istnieją liczby pierwsze $p_1, \ldots, p_n$, $n \in \mathbb{N}$, takie, że

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

Kładziemy

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

2° Jednoznaczność.

Przypuśćmy, że $\alpha, \alpha' : \mathbb{P} \to \mathbb{N}$ są funkcjami sumowalnymi takimi, że

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

Przez indukcję na a udowodnimy, że $\alpha = \alpha'$ (tzn. $\alpha(p) = \alpha'(p)$ dla każdej liczby pierwszej p).

Jeśli $a = 1$, to $\alpha(p) = 0 = \alpha'(p)$ dla każdej liczby pierwszej p

Załóżmy zatem, że $a > 1$. Wtedy istnieje liczba pierwsza q taka, że $\alpha(q) > 0$. Ze Stwierdzenia 1.31 wiemy, że istnieje liczba pierwsza q' taka, że $\alpha'(q') > 0$ i $q \mid q'$. Zauważmy, że $q = q'$ na mocy Lematu 1.27. Jeśli zdefiniujemy funkcje $\beta, \beta' : \mathbb{P} \to \mathbb{N}$ wzorami

$$\beta(p) := \begin{cases} \alpha(p) - 1 & p = q, \\ \alpha(p) & p \neq q, \end{cases} \qquad (p \in \mathbb{P})$$

i

$$\beta'(p) := \begin{cases} \alpha'(p) - 1 & p = q, \\ \alpha'(p) & p \neq q, \end{cases} \qquad (p \in \mathbb{P}),$$

to

$$q \cdot \prod_{p\in\mathbb{P}} p^{\beta(p)} = \prod_{p\in\mathbb{P}} p^{\alpha(p)} = \prod_{p\in\mathbb{P}} p^{\alpha'(p)} = q \cdot \prod_{p\in\mathbb{P}} p^{\beta'(p)}.$$

Stąd

$$\prod_{p\in\mathbb{P}} p^{\beta(p)} = \frac{a}{q} = \prod_{p\in\mathbb{P}} p^{\beta'(p)},$$

więc $\beta = \beta'$ z założenia indukcyjnego i, w konsekwencji, $\alpha = \alpha'$. □

Fakt 1.33.

Niech a i b będą dodatnimi liczbami całkowitymi. Jeśli

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

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

Dowód.

Załóżmy najpierw, że $\beta(p) \leq \alpha(p)$ dla każdej liczby pierwszej p. Zauważmy, że funkcja $\alpha - \beta$ jest sumowalna. Jeśli

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

to $c \in \mathbb{Z}$ i $a = b \cdot c$, więc $b \mid a$.

Załóżmy teraz, że $b \mid a$. Ustalmy liczbę całkowitą c taką, że $a = b \cdot c$. Wtedy $c > 0$, więc na mocy Twierdzenia 1.32 istnieje funkcja sumowalna $\gamma : \mathbb{P} \to \mathbb{N}$ taka, że

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

Wtedy

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

Z Twierdzenia 1.32 otrzymujemy, że $\alpha(p) = \beta(p) + \gamma(p)$ dla każdej liczby pierwszej p. W szczególności, $\alpha(p) \geq \beta(p)$ dla każdej liczby pierwszej p. □

Fakt 1.34.

Niech a i b będą dodatnimi liczbami całkowitymi. Jeśli

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

dla pewnych funkcji sumowalnych $\alpha, \beta : P \to \mathbb{N}$, to

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

Dowód.

Niech

$$d := \prod_{p\in\mathbb{P}} p^{\min\{\alpha(p),\beta(p)\}}.$$

Oczywiście, $d \geq 0$. Ponadto

$$\min\{\alpha(p),\beta(p)\} \leq \alpha(p) \qquad \text{i} \qquad \min\{\alpha(p),\beta(p)\} \leq \alpha(p)$$

dla każdej liczby pierwszej p, więc $d \mid a$ i $d \mid b$ na mocy Faktu 1.33. Załóżmy wreszcie, że $c \mid a$ i $c \mid b$ dla pewnej liczby całkowitej d. Z Faktu 1.5 wynika, że $c \neq 0$, gdyż $a \neq 0$ i $b \neq 0$. Z Twierdzenia 1.32 wynika, że istnieje funkcja sumowalna $\gamma\colon \mathbb{P} \to \mathbb{N}$ taka, że

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

Ponieważ $c \mid a$ i $c \mid b$, więc na mocy Faktu 1.33

$$\gamma(p) \leq \alpha(p) \qquad \text{i} \qquad \beta(p)$$

dla każdej liczby pierwszej p. Stąd $\gamma(p) \leq \min\{\alpha(p),\beta(p)\}$ dla każdej liczby pierwszej p, więc $c \mid d$ na mocy Faktu 1.33. □

Uwaga.

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

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

Można pokazać, że

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

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 1.35.

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.

Załóżmy 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 $a \bmod n = b \bmod n$.

Załóżmy 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 1.36.

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 1.35. □

Lemat 1.37.

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

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

(2) Jeśli a, b i c są liczbami całkowitymi takimi, że $a \cdot c \equiv_n b \cdot c$ i $\gcd(c, n) = 1$, 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 wyników z Faktów 1.7 i 1.8.

(2) Teza wynika z Wniosku 1.23.

(3) Teza wynika z Faktu 1.9. □

Stwierdzenie 1.38.

Niech a, b i n będą liczbami całkowitymi takimi, że $a \neq 0 \neq n$, 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

$$\{x \in \mathbb{Z} : a \cdot x \equiv_n b\} = \{x \in \mathbb{Z} : x \equiv_{n/d} c\},$$

gdzie $c := (b/d) \cdot k$.

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 1.37 (1). Stąd

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

sprzeczność.

(2) Zauważmy, że liczba k istnieje na mocy Wniosku 1.20. Przypuśćmy najpierw, że x jest liczbą całkowitą taką, że $x \equiv_{n/d} c$. Wtedy $d \cdot x \equiv_n d \cdot c = b \cdot k$ na mocy Lematu 1.37 (3). Korzystając z Lematu 1.37 (1), otrzymujemy, że

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

Z powyższego rachunku wiemy między innymi, 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 1.37 (3) implikuje, że

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

Lemat 1.39.
Niech a, b, n_1, $\ldots$, 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 $i \in [1,n]$, to $a \equiv_n b$, gdzie $n := \prod_{i\in[1,k]} n_i$.

Dowód.
Wynika z Wniosku 1.25. □

Twierdzenie 1.40 (Chińskie twierdzenie o resztach).
Załóżmy, że n_1, $\ldots$, 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 $\Phi : [0, n-1] \to [0, n_1 - 1] \times \cdots \times [0, n_k - 1]$ dana wzorem

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

jest bijekcją.

Dowód.
Ponieważ

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

więc wystarczy pokazać, że funkcja Φ jest różnowartościowa. W tym celu ustalmy liczby $a, b \in [0, n-1]$ i załóżmy, że $\Phi(a) = \Phi(b)$. Wtedy $a \equiv_{n_i} b$ dla każdego $i \in [1,k]$ na mocy Faktu 1.35. Korzystając z Lematu 1.39, otrzymujemy zatem, że $a \equiv_n b$, a więc $a \bmod n = b \bmod n$ na mocy Faktu 1.35. Ponieważ

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

mocy Wniosku 1.15, więc

$$a = a \bmod n = b \bmod n = b.$$ □

Stwierdzenie 1.41.

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

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

oraz $b_1, \ldots, b_k$ 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 1.37 (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 1.35. □

Uwaga.

Niech $n_1, \ldots, n_k$ 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

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

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 1.24 wiemy, że $\gcd(m_i, n_i) = 1$ dla każdego $i \in [1, k]$, zatem teza wynika ze Stwierdzenia 1.38 (2). □

1.5. Funkcja i twierdzenie Eulera

Definicja.

Funkcją Eulera nazywamy funkcję $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ zdefiniowaną wzorem

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

gdzie

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

Przykład.
$\varphi(1) = 1$.

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

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

Lemat 1.42.
Jeśli p jest liczbą pierwszą i k jest dodatnią liczbą całkowitą, to

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

Dowód.
Z Faktu 1.34 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 1.43.
Jeśli $n_1, \ldots, n_k$ 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

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

Dowód.
Niech

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

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

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

Z Twierdzenia 1.40 wiemy, że funkcja ta jest bijekcją. Ponadto, jeśli $a \in [0, n-1]$, to, korzystając z Wniosku 1.24 i Lematu 1.21, otrzymujemy, że

$$\gcd(a, n) = 1 \iff \forall_{i \in [1,k]}\ \gcd(a, n_i) = 1$$

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

Zatem funkcja Φ indukuje bijekcję

$$U_n \to U_{n_1} \times \ldots \times U_{n_k}. \qquad \square$$

Wniosek 1.44.
Niech P będzie skończonym podzbiorem zbioru liczb pierwszych i $\alpha : P \to \mathbb{N}_+$. Jeśli

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

to

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

Dowód.
Dla liczby $p \in P$ definiujemy dodatnią liczbę całkowitą n_p wzorem $n_p := p^{\alpha(p)}$. Z Faktu 1.34 wiemy, że $\gcd(n_p, n_q) = 1$ dla wszystkich liczb $p, q \in P$ takich, że $p \neq q$. Korzystając z Lematu 1.43, otrzymujemy, że

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

zatem teza wynika z Lematu 1.42. $\square$

Wniosek 1.45.
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

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

a więc są rozwiązaniami równania

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

Twierdzenie 1.46 (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 $\Phi : U_n \to U_n$ wzorem

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

Zauważmy najpierw, że funkcja Φ jest poprawnie określona. Istotnie, jeśli $b \in U_n$, to $\gcd(b, n) = 1$, więc $\gcd(a \cdot b, n) = 1$ na mocy Wniosku 1.24. Korzystając z Lematu 1.21, wnioskujemy, że $\gcd(\Phi(b), n) = 1$, a więc $\Phi(b) \in U_n$.

Pokażemy teraz, że funkcja Φ jest bijekcją. W tym celu wystarczy uzasadnić, że funkcja Φ 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 1.35, więc $b \equiv_n c$ na mocy Lemat 1.37 (2). Korzystając ponownie z Faktu 1.35, 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 Φ jest bijekcją, więc, korzystając z Lematu 1.37 (1), otrzymujemy, że

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

Ponieważ $\gcd(\prod_{b \in U_n} b, n) = 1$ na mocy Wniosku 1.24, więc teza wynika z Lematu 1.37 (2). □

Wniosek 1.47.

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

Wniosek 1.48.

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 1.47. Gdy $p \mid a$, to $a^p \equiv_p 0 \equiv_p a \pmod{p}$. □

1.6. Zastosowanie teorii liczb w kryptografii

Celem kryptografii jest opracowanie metod przekazywania wiadomości, które uniemożliwią jej odczytanie osobom niepowołanym nawet w przepadku 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 symboli służących do zapisu tekstu zakodowanego oraz bijekcji $f : P \to C$ zwanej funkcją szyfrującą. Funkcję odwrotną $f^{-1} : C \to P$ 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 $f : P \to C$ wzorem

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

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

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

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 $f : P \to C$ wzorem

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

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 1.38 (2)).

Lemat 1.49.

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 1.47 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 $a^{de} \equiv_q a$, więc teza wynika Lematu 1.39. □

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 $a : [1, n] \to X$. Jeśli a jest ciągiem długości n, to piszemy $a = (a(1), \ldots, a(n))$.

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.

Definicja.

Jeśli n jest nieujemnymą liczbami całkowitymi, to definiujemy n silnia wzorem

$$n! := \begin{cases} 1 & \text{jeśli } n = 0, \\ n \cdot (n-1)! & \text{jeśli } n > 0. \end{cases}$$

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 $f : P_X \to \bigcup_{x \in X} P_{X \setminus \{x\}}$ wzorem

$$f(a) := (a(1), \ldots, a(n-1)) \qquad (a \in P_X).$$

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

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

Stwierdzenie 2.2.

Jeśli $n > 1$ jest liczbą całkowitą, to

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

Dowód.

Przypomnijmy, że dla dowolnej dodatniej liczby całkowitej k mamy nierówności

$$\Big(\frac{k+1}{k}\Big)^k < e < \Big(\frac{k+1}{k}\Big)^{k+1}.$$

Wykorzystując te nierówności, otrzymujemy, że

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

i

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

co kończy dowód. □

Uwaga.

Stirling udowodnił, że

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

Definicja.

Jeśli k jest nieujemną liczbą całkowitą oraz X jest zbiorem, to k-elementową kombinacją 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

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

Stwierdzenie 2.3.
Jeśli k jest nieujemną liczbą całkowitą oraz X jest zbiorem, to $|C_{X,k}| = \binom{|X|}{k}$.

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

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

Wtedy

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

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

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

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

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

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

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

co kończy dowód. □

2.2. Metoda bijektywna

Uwaga.

Zauważmy, że w dowodach Stwierdzeń 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 bijektywną. 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 $f : C_{n,k} \to C_{n-1,k} \cup C_{n-1,k-1}$ daną wzorem

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

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

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

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 $0, \ldots, k-1$.

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

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

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

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 $f : C_{n,k} \to C_{n,n-k}$ wzorem

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

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

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

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 $f : 2^X \to \mathcal{X}$ wzorem

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

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

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

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 $C_{n,k} \cap C_{n,l} = \varnothing$ 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 cześć pochodzącą ze zbioru $[1, k]$, a potem tę pochodząca 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

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

Ponieważ $X_i \cap X_j = \varnothing$ 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 $f : X \to Y$ daną wzorem

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

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

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

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

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

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 liczba 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

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

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 $F, G \in \mathbb{C}[S,T]$ wzorami

$$F := \sum_{i\in[0,n]} \binom{S}{i} \cdot \binom{T}{n-i} \qquad \text{i} \qquad G := \binom{S+T}{n}.$$

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. □

Definicja.

Niech m i n będą nieujemnymi liczbami całkowitymi. Drogą z punktu $(0,0)$ do punktu (m,n) nazywamy każdy ciąg $a : [0, m+n] \to \mathbb{N}^2$ 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 $f : C_{m+n,m} \to X$ wzorem

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

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 $f^{-1} : X \to C_{m+n,m}$ dana jest wzorem

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

Wniosek 2.13.

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

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

Dowód.

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

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

Ze Stwierdzenia 2.12 wiemy, że

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

Definiujemy funkcję $f : X \to Y$ wzorem

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

gdzie $\pi_1 : \mathbb{R}^2 \to \mathbb{R}$ 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 $f^{-1} : Y \to X$ dana jest wzorem

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

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

$$p_i(x) := \max\Big\{l \in [0,k] : l + \sum_{j\in[1,l]} x(j) \le i\Big\} \qquad (x \in Y).$$

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. □

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

$$\Big|\bigcup_{i\in J} X_i\Big| = \sum_{\substack{I\subset J\\ I\neq\varnothing}} (-1)^{|I|-1} \cdot \Big|\bigcap_{i\in I} X_i\Big| = \sum_{k\in[1,|J|]} (-1)^{k-1} \cdot \sum_{I\in C_{J,k}} \Big|\bigcap_{i\in I} X_i\Big|.$$

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

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

co kończy dowód. □

Przykład.

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

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

Dowód.

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

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

Zauważmy, że

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

dla dowolnego niepustego podzbioru I zbioru P. Stąd

$$\varphi(n) = \Big|[0, n-1] \setminus \bigcup_{p\in P} X_p\Big| = n - \Big|\bigcup_{p\in P} X_p\Big|$$

$$= n - \sum_{\substack{I\subseteq P\\ I\neq\varnothing}} (-1)^{|I|-1} \cdot \Big|\bigcap_{p\in I} X_p\Big| = n + \sum_{\substack{I\subseteq P\\ I\neq\varnothing}} (-1)^{|I|} \cdot \frac{n}{\prod_{p\in I} p}$$

$$= n \cdot \sum_{I\subseteq P} \prod_{p\in I} \frac{(-1)^{|I|}}{p} = n \cdot \prod_{p\in P} \Big(1 - \frac{1}{p}\Big),$$

co kończy dowód. □

Oznaczenie.

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

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

Elementy zbioru P'_n nazywamy permutacjami bez punktów stałych.

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

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

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

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

$$= n! - \sum_{k\in[1,n]} (-1)^{k-1} \cdot \sum_{I\in C_{n,k}} \Big|\bigcap_{i\in I} X_i\Big|$$

$$= n! + \sum_{k\in[1,n]} (-1)^k \cdot \sum_{I\in C_{n,k}} (n-k)!$$

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

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

co kończy rozwiązanie. □

Oznaczenie.

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

$$[x] := \begin{cases} \lfloor x \rfloor & \text{jeśli } x - \lfloor x \rfloor < \frac{1}{2}, \\ \lfloor x \rfloor + 1 & \text{jeśli } x - \lfloor x \rfloor \geq \frac{1}{2}. \end{cases}$$

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 $|P'_n| = [\frac{n!}{e}]$.

(2) $\lim_{n\to\infty} \frac{|P'_n|}{|P_n|} = \frac{1}{e}$.

Dowód.

Wiadomo, że

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

i, w szczególności,

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

To natychmiast implikuje drugą część wniosku. Ponadto,

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

co kończy dowód. □

3. Funkcje tworzące

3.1. Szeregi formalne

Definicja.

Szeregiem formalnym nazywamy każdy ciąg $\mathcal{A} : \mathbb{N} \to \mathbb{C}$, 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

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

i

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

tzn.

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

i

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

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

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

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 λ 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 zepoloną, to przez $\mathcal{A}_x$ oznaczamy funkcję tworzącą ciągu $\binom{x}{n}_{n\in\mathbb{N}}$, tzn.

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

Lemat 3.2.

Jeśli x i y są liczbami zespoloną, 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 $\mathcal{A}_0$. □

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 λ 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 $k \in \mathbb{N}_+$ i $\mathcal{A}^k = 1+T$ dla szeregu $\mathcal{A} \in \mathbb{C}[[T]]$, to istnieje pierwiastek zespolony ε stopnia k z jedynki taki, że

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

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 $\lambda_1, \ldots, \lambda_n$ są wszystkimi parami różnymi pierwiastkami zespolonymi wielomianu G krotności $m_1, \ldots, m_n$ odpowiednio, to istnieją liczby zespolone $A_{i,j}$, $j \in [1, m_n]$, $i \in [1, n]$, 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 ciągu a. Zauważmy, że

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

Stąd

$$\begin{aligned}
\mathcal{A} &= \Big(\sum_{n\in\mathbb{N}} T^n\Big) \cdot \Big(\sum_{n\in\mathbb{N}} T^{2\cdot n}\Big) \cdot \Big(\sum_{n\in\mathbb{N}} T^{5\cdot n}\Big) \\
&= \frac{1}{(1-T)\cdot(1-T^2)\cdot(1-T^5)} \\
&= \frac{1}{(1-T)^3\cdot(1+T)\cdot\prod_{i\in[1,4]}(1-\varepsilon^i\cdot T)}
\end{aligned}$$

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

więc, korzystając z Wniosku 3.4, otrzymujemy równość

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

dla każdej nieujemnej liczby całkowitej n, gdzie ε 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

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

3.3. Rekurencje

Przykład.

Definiujemy ciąg Fibonacciego F wzorem

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

Policzymy 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

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

skąd

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

dla każdej nieujemnej liczby całkowitej n.

Definicja.

Rekurencją (liniową o stałych współczynnikach) rzędu r, $r \in \mathbb{N}_+$, nazywamy każdy układ równań postaci

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

gdzie $u_{r-1}, \ldots, u_0$ 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

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

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

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

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

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

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 zepolonych jest przestrzenią liniową nad ciałem liczb zespolonych z działaniami dodawania ciągów po współrzędnych oraz mnożeniem ciągów przez skalary po współrzędnych.

Twierdzenie 3.6.

Niech

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

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

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

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

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

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 $(*)$. Policzymy funkcję tworzącą $\mathcal{A}$ ciągu a:

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

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

gdzie $u_r := 1$, więc

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

Zauważmy, że

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

Ponieważ $\sum_{i\in[0,r]} u_i\cdot T^{r-i} = T^r\cdot F(\frac{1}{T})$, więc liczby λ_1^{-1}, …, λ_l^{-1} są parami różnymi pierwiastkami wielomianu $\sum_{i\in[0,r]} u_i\cdot T^{r-i}$ krotności k_1, …, 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

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

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

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

dla każdej nieujemnej liczby całkowitej n, co kończy dowód. □

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

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

Wielomianem charakterystycznym tej rekurencji jest wielomian $T^2 - 3 \cdot T + 2$, którego pierwiastkami (jednokrotnymi) są 1 i 2. Zatem istnieją liczby zespolone μ_1 i μ_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

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

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

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

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 rekruencję

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

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 $\lambda_0 = 1$, λ_1, $\ldots$, λ_l będą pierwiastkami wielomianu G krotności $k_0 = k + m + 1$, k_1, $\ldots$, k_l, odpowiednio. Ustalmy rozwiązanie a rekurencji $(*)$. Z Twierdzenia 3.7 wiemy, że istnieją liczby zespolone $A_{i,j}$, $i \in [0, l]$, $j \in [0, k_l - 1]$, 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 $\lambda_0, \lambda_1, \ldots, \lambda_l$, a ich krotności to $k = k_0 - m - 1, k_1, \ldots, k_l$, odpowiednio, więc korzystając ponownie z poprzedniego twierdzenia otrzymujemy, że ciąg a' dany wzorem

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

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

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

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

Zauważmy, że ciąg s jest rozwiązaniem rekurencji

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

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

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

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

$$\begin{cases} 4 \cdot \mu'_3 = 1 \\ 3 \cdot \mu'_2 + 6 \cdot \mu'_3 = 3 \\ 2 \cdot \mu'_1 + 3 \cdot \mu'_2 + 4 \cdot \mu'_3 = 3 \\ \mu'_0 + \mu'_1 + \mu'_2 + \mu'_3 = 1 \end{cases},$$

którego rozwiązaniem są liczby

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

Na mocy Twierdzenie 3.7 istnieje liczba zespolona μ 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 tworzącą ciągu a. Jeśli

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

dla pewnych liczb zespolonych $u_0, \ldots, u_r$ 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

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

Dowód.

Zauważmy, że powyższa równość oznacza, że

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

zatem

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

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

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 $k_x = n$ ($x = (1, 0, \ldots, 0, 1)$. 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

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

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 $\varnothing$, 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

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

Korzystając z Faktu 3.5, otrzymujemy, że

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

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

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

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

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

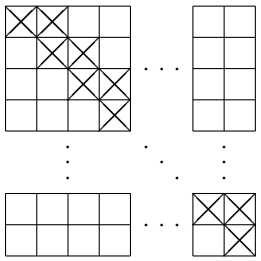
dla wszystkich indeksów $i \in I$ i $j \in J$. Liczbę rozstawień k wież na szachownicy B oznaczamy przez $r^B(k)$.

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 $k > |I|$ lub $k > |J|$.

Przykład.

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

$B :=$ 

o n wierszach i n kolumnach.

Definicja.

Wielomianem wieżowym szachownicy B nazywamy funkcję tworzącą ciągu r^B. Wielomian wieżowy szachownicy B oznaczamy symbolem R_B.

Przykład.

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

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

Przykład.

Jeśli $B = (I, J, \varnothing)$, to

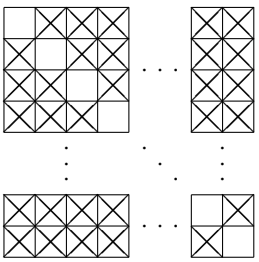
$$R_B = \sum_{k\in\mathbb{N}} \binom{|I|}{k} \cdot \binom{|J|}{k} \cdot k! \cdot T^k.$$

Przykład.

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

Przykład.

Jeśli n jest nieujemną liczbą całkowitą i

$B_n :=$ 

jest szachownicą o n wierszach i n kolumnach, to

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

Oznaczenie.

Jeśli $B = (I, J, F)$ jest szachownicą, $\sigma \in P_I$ i $\tau \in P_J$, to definiujemy szachownice B_σ i B^τ 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_σ i B^τ są otrzymane z szachownicy B przez permutację wierszy i kolumn, odpowiednio. Zauważmy, że $(B_\sigma)^\tau = (B^\tau)_\sigma$ i tę szachownicę oznaczamy B^τ_σ.

Uwaga.

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

Stwierdzenie 3.10.

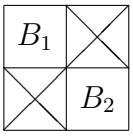
Niech $B = (I, J, F)$ będzie szachownicą. Jeśli $I = I_1 \cup I_2$ i $J = J_1 \cup J_2$, przy czym $I_1 \cap I_2 = \varnothing$ i $J_1 \cap J_2 = \varnothing$ oraz

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

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

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

Innymi słowy, jeśli

$B =$ 

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 $f : X \to \bigcup_{l\in[0,k]} Y_l \times Z_{k-l}$ dana wzorem

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

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

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

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. □

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 $B^{j_0}_{i_0}$.

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 $R_{B^{j_0}} = R_B$.

Twierdzenie 3.11.

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

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

gdzie $B' := (I, J, F \cup \{(i_0, j_0)\})$, tzn. szachownica B' powstaje z szachownicy B przez zamianę pola (i_0, j_0) na pole zabronione.

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 $X_1 \cap X_2 = \varnothing$. Ponadto $|X_1| = r^{B'}(k)$ oraz $|X_2| = r^{B^{j_0}_{i_0}}(k-1)$, zatem

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

Oczywiście

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

co kończy dowód. □

Definicja.

Negatywem szachownicy $B = (I, J, F)$ nazywamy szachownicę $\overline{B}$ daną wzorem

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

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

Twierdzenie 3.12.

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

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

Dowód.

Bez straty ogólności możemy założyć, że $I = [1, n] = J$. Niech $B' := (I, J, \varnothing)$ 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

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

tzn. Y_i jest zbiorem tych rozstawień A n wież, w 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

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

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 $I' \in C_{I,k}$, skąd

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

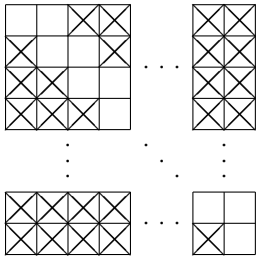
zatem teza wynika ze wzoru włączeń i wyłączeń (zauważmy, że $|Y| = n! = 1 \cdot n! = r^B(0) \cdot n!$). □

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

$B :=$ 

jest szachownicą o n wierszch i n kolumnach. Ponumerujmy 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 $i_1 < \cdots < i_k$ możemy przyporządkować podzbiór $\{i_1, i_2 - 1, \ldots, i_k - (k-1)\}$. 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 $(A_1, \ldots, A_n)$ podzbiorów zbioru X nazywamy każdy ciąg $(a_1, \ldots, a_n)$ 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 $(A_1, \ldots, A_n)$ 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 $(A_1, \ldots, A_n)$ 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 $(A_1, \ldots, A_n)$ 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 $(A_1, \ldots, A_n)$ podzbiorów zbioru X posiada system reprezentantów wtedy i tylko wtedy, gdy spełnia warunek Halla.

Dowód.

Jest oczywiste, że jeśli ciąg $(A_1, \ldots, A_n)$ posiada system reprezentantów, to spełnia warunek Halla. Pokażemy teraz, że jeśli ciąg $(A_1, \ldots, A_n)$ spełnia warunek Halla, to posiada system reprezentantów. Jeśli $|A_i| = 1$ dla każdego indeksu $i \in [1, n]$, to z warunku Halla wynika, że $A_i \cap A_j = \varnothing$ 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 zakończenie dowodu wystarczy pokazać, że jeden z ciągów $(A_1', A_2, \ldots, A_n)$ i $(A_1'', A_2, \ldots, A_n)$ spełnia warunek Halla oraz skorzystać z założenia indukcyjnego.

Przypuśćmy, że ciąg $(A_1', A_2, \ldots, A_n)$ 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 $(A_1'', A_2, \ldots, A_n)$ 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 $(A_1, \ldots, A_n)$ będzie ciągiem podzbiorów zbioru X. Jeśli istnieje dodatnia liczba naturalna d 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 $(A_1, \ldots, A_n)$ 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 $a_{i_1,j_2} \neq a_{i_2,j_2}$ 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

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

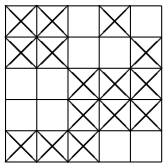
jest prostokątem łacińskim.

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.

Liczba sposobów, na które można rozszerzyć prostokąt A z poprzedniego przykładu do prostokąta 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 $(A_1, \ldots, A_n)$ posiada system reprezentantów $(a_1, \ldots, a_n)$. Wtedy macierz B o $m+1$ wierszach i n kolumnach dana wzorem

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

jest prostokątem łacińskim, który jest rozszerzeniem prostokąta A. □

Definicja.

Niech n będzie nieujemna liczba całkowitą. Macierz P o n wierszach i n kolumnach oraz 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 $(A_1, \ldots, A_n)$ 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 $(a_1, \ldots, a_n)$ będzie system reprezentantów dla ciągu $(A_1, \ldots, A_n)$. Wtedy macierz P dana wzorem

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

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

5. Ważne ciągi liczbowe

5.1. Liczby Stirlinga

Definicja.

Niech $k \in \mathbb{N}$. Rozkładem zbioru X na k części nazywamy każdą rodzinę $\mathcal{A} \subseteq 2^X \setminus \{\varnothing\}$ taką, że $|\mathcal{A}| = k$, $X = \bigcup_{A \in \mathcal{A}} A$ oraz $A \cap B = \varnothing$ dla wszystkich zbiorów $A, B \in \mathcal{A}$ takich, że $A \neq B$. .

Oznaczenie.

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

Przykład.

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

Przykład.

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

Przykład.

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

Przykład.

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

Przykład.

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

Przykład.

$\left\{ {4 \atop 2} \right\} = 7$.

Twierdzenie 5.1.

Jeśli $n, k \in \mathbb{N}_+$, to

$$\left\{ {n \atop k} \right\} = k \cdot \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}.$$

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 $f : X \to Y_1 \cup Y_2$ 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

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

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

Oznaczenie.
Dla liczby $k \in \mathbb{N}$ niech $\mathcal{S}_k$ będzie funkcją tworzącą ciągu $(\left\{{n \atop k}\right\})_{n\in\mathbb{N}}$.

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

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

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 $\varphi : A \to B$ jest równa $k! \cdot \left\{{n \atop k}\right\}$, 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 $\varphi : A \to B$, zaś niech Y będzie zbiorem

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

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

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 $\mathcal{A} = \{A_1, \ldots, A_k\} \in Y$, to

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

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

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

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

$$|X| = |P_k| \cdot |Y| = k! \cdot \left\{ {n \atop k} \right\},$$

co kończy dowód. □

Wniosek 5.4.
Jeśli $n, k \in \mathbb{N}$, to

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

Dowód.
Niech X będzie zbiorem wszystkich funkcji $\varphi : [1, n] \to [1, k]$. 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

$$|X_i| = \binom{k}{i} \cdot i! \cdot \left\{ {n \atop i} \right\}$$

dla wszystkich liczb $i \in [0, k]$. Ponieważ, $X_i \cap X_j = \varnothing$ 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

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

Dowód.

Wystarczy zauważyć, że

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

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

5.2. Liczby Bella

Definicja.

Jeśli $n \in \mathbb{N}$, to n-tą liczbą Bella nazywamy ilość rozkładów zbioru $[1,n]$, tzn.

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

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

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

co kończy dowód. □

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

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

Oczywiście $X_i \cap X_j = \varnothing$ 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. □

Stwierdzenie 5.8.

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

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

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. □

Definicja.

Powyższy sposób liczenia liczb Bella nazywamy trójkątem Bella.

Przykład.

Z następującej tablicy

$$\begin{array}{ccccc} 1 & 1 & 2 & 5 & 15 \\ & 2 & 3 & 7 & 20 \\ & & 5 & 10 & 27 \\ & & & 15 & 37 \\ & & & & 52 \end{array}$$

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

6. Elementy teorii grafów

6.1. Podstawowe definicje

Oznaczenie.

Jeśli V jest zbiorem, to

$$\mathcal{P}_2(V) := \{e \subseteq V : |e| = 2\}$$

(we Rozdziale 2 oznaczaliśmy ten zbiór $C_{V,2}$).

Definicja.

Grafem (prostym nieskierowanym bez pętli) nazywamy parę $G = (V_G, E_G)$, gdzie V_G jest skończonym zbiorem (który nazywamy zbiorem wierzchołków, a jego elementy wierzchołkami) oraz $E_G \subseteq \mathcal{P}_2(V_G)$ (elementy zbioru E_G nazywamy krawędziami, a zbiór E_G zbiorem krawędzi).

Jeśli $e \in E_G$ i $e = \{x, y\}$, to mówimy, że krawędź e łączy wierzchołki x i y, krawędź e jest incydentna w wierzchołkami x i y, wierzchołki x i y są końcami krawędzi e, oraz nazywamy wierzchołek y sąsiadem wierzchołka x.

Graf o pustym zbiorze wierzchołków (a więc także o pustym zbiorze krawędzi) nazywamy grafem pustym.

Uwaga.

Grafy zwykle przedstawiamy w postaci graficznej: wierzchołki reprezentowane są przez punkty, natomiast krawędzie przez łuki, przy czym łuk odpowiadający krawędzi $\{x, y\}$ łączy punkty odpowiadające wierzchołkom x i y.

Przykład.

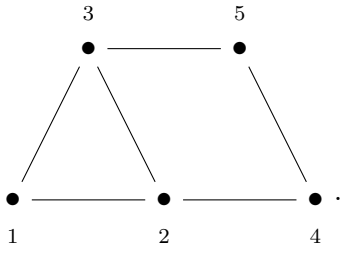
Jeśli

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

i

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

to graf G możemy przedstawić za pomocą następującego rysunku:

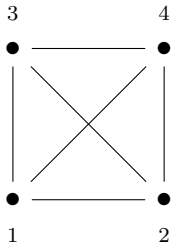


Definicja.

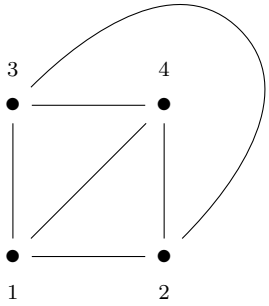
Niepusty graf G nazywamy PLANARNYM, jeśli można go przedstawić na płaszczyźnie w ten sposób, aby łuki odpowiadające krawędziom nie przecinały się (z wyjątkiem wierzchołków będących wspólnymi końcami danych krawędzi).

Przykład.

Graf z poprzedniego przykłady jest planarny. Również graf



jest planarny, gdyż można go narysować następująco:



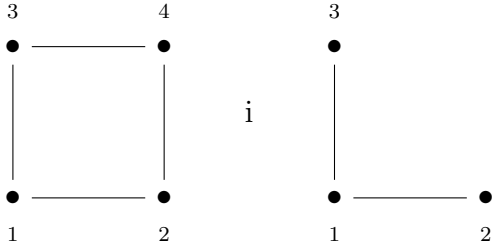
Przykłady grafów, które nie są planarne, zostaną przedstawione w podrozdziale 6.2.

Definicja.

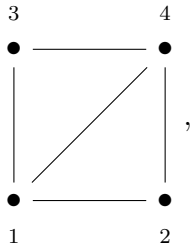
Graf H nazywamy PODGRAFEM grafu G, jeśli $V_H \subseteq V_G$ oraz $E_H \subseteq E_G$. Jeśli dodatkowo $E_H := \mathcal{P}_2(V_H) \cap E_G$, to graf H nazywamy PODGRAFEM INDUKOWANYM przez zbiór V_H i piszemy $H = \langle V_H \rangle_G$.

Przykład.

Grafy



są podgrafami grafu



,

ale tylko drugi z tych grafów jest podgrafem indukowanym.

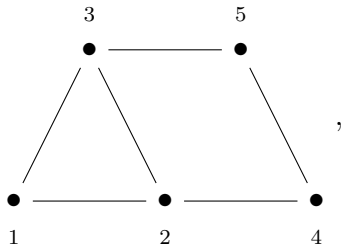
Definicja.

Jeśli x jest wierzchołkiem grafu G, to stopniem $\deg_G x$ wierzchołka x w grafie G nazywamy liczbę krawędzi incydentych z wierzchołkiem x (równoważnie, liczbę sąsiadów wierzchołka x), tzn.

$$\deg_G x := \#\{e \in E_G : x \in e\} = \#\{y \in V_G : \{x, y\} \in E_G\}.$$

Przykład.

Jeśli G jest grafem



,

to

$$\deg_G 1 = 2,\ \deg_G 2 = 3,\ \deg_G 3 = 3,\ \deg_G 4 = 2 \text{ i } \deg_G 5 = 2.$$

Stwierdzenie 6.1.

Jeśli G jest grafem, to

$$\sum_{x \in V_G} \deg_G x = 2 \cdot |E_G|.$$

Dowód.

Obie strony równości są liczbą par $(x, y) \in V_G^2$ takich, że $\{x, y\}$ jest krawędzią w grafie G. □

Definicja.

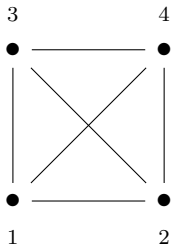
Graf G nazywamy spójnym, jeśli nie istnieje podział zbioru V_G na niepuste zbiory U i W (tzn. $V_G = U \cup W$ i $U \cap W = \varnothing$) taki, że $E_G \subseteq \mathcal{P}_2(U) \cup \mathcal{P}_2(W)$ (tzn. każda krawędź w grafie G łączy albo dwa wierzchołki ze zbioru U albo dwa wierzchołki ze zbioru W).

Maksymalne podgrafy spójne grafu G nazywamy składowymi (spójności) grafu G. Innymi słowy, podgraf H grafu G jest składową grafu G, jeśli graf H jest spójny G oraz jeśli H' jest podgrafem spójnym grafu takim, że $H \subseteq H'$ (tzn. $V_H \subseteq V_{H'}$ oraz $E_H \subseteq E_{H'}$), to $H' = H$ (tzn. $V_{H'} = V_H$ oraz $E_{H'} = E_H$).

Przykład.

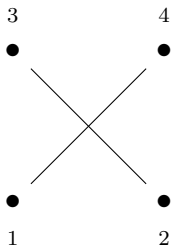
Graf pusty jest grafem spójnym.

Podobnie, graf



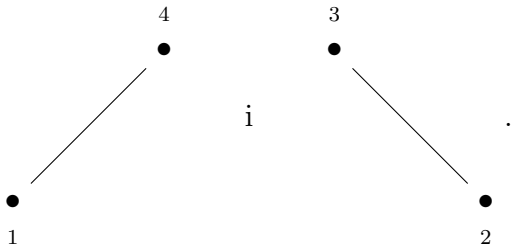
jest spójny.

Przykładem grafu niespójnego jest graf



,

którego składowymi są grafy



i .

Uwaga.

Jeśli x jest wierzchołkiem grafu G, to graf $\langle\{x\}\rangle_G$ jest spójny. Stąd wynika, że każdy wierzchołek grafu G należy do pewnej składowej grafu G.

Ponadto, jeśli H' i H'' są składowymi grafu G, to albo $H' = H''$ albo $V_{H'} \cap V_{H''} = \varnothing$.

Dowód.

Wystarczy udowodnić drugą część. Załóżmy, że $x \in V_{H'} \cap V_{H''}$. Jeśli pokażemy, że graf $H := (V_{H'} \cup V_{H''}, E_{H'} \cup E_{H''})$ jest spójny, to z maksymalności grafów H' i H'' otrzymamy, że $H' = H = H''$. Przypuśćmy zatem, że istnieje podział zbioru $V_{H'} \cup V_{H''}$ na zbiory U i W takie, że $E_{H'} \cup E_{H''} \subseteq \mathcal{P}_2(U) \cup \mathcal{P}_2(W)$. Bez straty ogólności możemy założyć, że $x \in U$. Wtedy ze spójności grafów H' i H'' wynika, że $V_{H'} \subseteq U$ i $V_{H''} \subseteq U$, więc $W = \varnothing$.

Oznaczenie.

Jeśli G jest grafem i x wierzchołkiem grafu G, to przez $G - x$ oznaczamy graf

$$(V_G \setminus \{x\}, E_G \setminus \{e : x \in e\})$$

(tzn. graf $G - x$ jest otrzymany z grafu G przez usunięcie wierzchołka x oraz wszystkich krawędzi incydentnych z wierzchołka x).

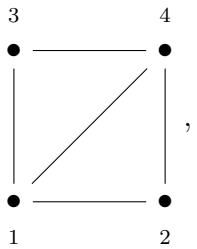
Podobnie, jeśli e jest krawędzią grafu G, to przez $G - e$ oznaczamy graf

$$(V_G, E_G \setminus \{e\})$$

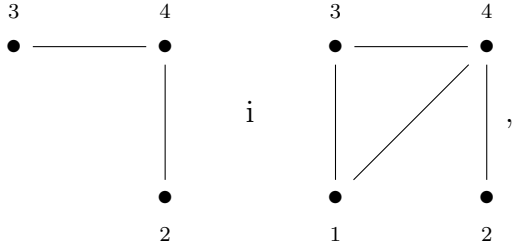
(tzn. graf $G - e$ jest otrzymany z grafu G przez usunięcie krawędzi e).

Przykład.

Jeśli G jest grafem



$x := 1$ i $e := \{1, 2\}$, to $G - x$ i $G - e$ są grafami



odpowiednio.

Uwaga.

Zauważmy, że jeśli x jest wierzchołkiem grafu G i $H := G - x$, to

$$|V_H| = |V_G| - 1 \qquad \text{i} \qquad |E_H| = |E_G| - \deg_G x.$$

Podobnie, jeśli e jest krawędzią grafu G i $H := G - e$, to

$$|V_H| = |V_G| \qquad \text{i} \qquad |E_H| = |E_G| - 1.$$

Lemat 6.2.

Jeśli x jest wierzchołkiem graf spójnego G i $\deg_G x = 1$, to graf $G - x$ jest spójny.

Dowód.

Niech $H := G - x$. Gdyby istniał podział zbioru $V_H = V_G \setminus \{x\}$ na niepuste zbioru U i W takie, że $E_H \subseteq \mathcal{P}_2(U) \cup \mathcal{P}_2(W)$, to bez straty ogólności moglibyśmy założyć, że jeśli $\{x, y\} \in E_G$, to $y \in U$. Wtedy zbiory $U \cup \{x\}$ i W tworzyłyby podział zbioru V_G taki, że $E_G \subseteq \mathcal{P}_2(U \cup \{x\}) \cup \mathcal{P}_2(W)$, co byłoby sprzeczne z założeniem spójności grafu G.

Stwierdzenie 6.3.

Jeśli graf G jest spójny, to

$$|E_G| \geq |V_G| - 1.$$

Dowód.

Dowód będzie indukcyjny ze względu $|V_G|$. Oczywiście teza jest prawdziwa, gdy graf G jest pusty.

Załóżmy najpierw, że istnieje wierzchołek x grafu G taki, że $\deg_G x = 0$. Ze spójności grafu G wynika, że wtedy $V_G = \{x\}$ (w przeciwnym wypadku mamy podział na zbiory $\{x\}$ i $V_G \setminus \{x\}$). Stąd

$$|E_G| \geq 0 = 1 - 1 = |V_G| - 1.$$

Załóżmy teraz, że istnieje wierzchołek x grafu G taki, że $\deg_G x = 1$. Jeśli $H = G - x$, to graf H jest spójny na mocy Lematu 6.2. Ponieważ $|V_H| = |V_G| - 1 < |V_G|$, więc, korzystając z założenia indukcyjnego, otrzymujemy, że

$$|E_H| \geq |V_H| - 1.$$

Ponieważ $|E_H| = |E_G| - 1$, więc ostatecznie

$$|E_G| = |E_H| + 1 \geq |V_H| = |V_G| - 1.$$

Na zakończenie załóżmy, że $\deg_G x \geq 2$ dla każdego wierzchołka x grafu G. Wtedy Stwierdzenie 6.1 implikuje, że

$$2 \cdot |E_G| \geq 2 \cdot |V_G|,$$

co kończy dowód. □

Definicja.

Graf spójny G nazywamy drzewem, jeśli $|E_G| = |V_G| - 1$.

Definicja.

Drogą w grafie G nazywamy każdy ciąg $(x_0, \ldots, x_n)$ wierzchołków grafu G taki, że $\{x_{i-1}, x_i\} \in E_G$ dla każdego $i \in [1, n]$. W powyższej sytuacji mówimy, że droga łączy wierzchołki x_0 i x_n. Jeśli dodatkowo $x_0 = x_n$, $n > 2$, oraz $x_i \neq x_j$ dla wszystkich $i, j \in [1, n]$ takich, że $i \neq j$, to drogę nazywamy cyklem.

Stwierdzenie 6.4.

Graf G jest spójny wtedy i tylko wtedy, gdy dla dowolnych wierzchołków x i y grafu G istnieje droga łącząca wierzchołki x i y.

W szczególności, wierzchołki x i y grafu G należą do tej samej składowej wtedy i tylko wtedy, gdy istnieje droga łącząca te wierzchołki.

Dowód.

Przypuśćmy najpierw, że graf G jest spójny i ustalmy wierzchołek x grafu G. Oznaczmy przez U zbiór wszystkich wierzchołków V grafu G, do których istnieje droga łącząca wierzchołek x z wierzchołkiem v. Musimy pokazać, że $U = V_G$. Zauważmy, że zbiory U i $W := V_G \setminus U$ tworzą podział zbioru V_G. Ponadto, $E_G \subseteq \mathcal{P}_2(U) \cup \mathcal{P}_2(W)$. Istotnie, jeśli $\{y, z\} \in E_G$ i $y \in U$, to ponieważ istnieje droga z x do y, to istnieje również droga z x do z, więc $z \in U$. Ze spójności grafu G wynika zatem, że albo $U = \varnothing$ albo $W = \varnothing$. Ponieważ $x \in U$, więc $W = \varnothing$, skąd $U = V_G \setminus W = V_G$.

Załóżmy teraz, że graf G nie jest spójny. Wtedy istnieje podział zbioru V_G na niepuste podzbiory U i W takie, że $E_G \subseteq \mathcal{P}_2(U) \cup \mathcal{P}_2(W)$. Stąd natychmiast wynika, że jeśli $x \in U$ i $y \in W$, to nie istnieje droga łącząca x z y. Istotnie, gdyby ciąg $(x = x_0, \ldots, x_n = y)$ był taką drogą, to istniałoby $i \in [1, n]$ takie, że $x_{i-1} \in U$ oraz $x_i \in W$. Wtedy

$$\{x_{i-1}, x_i\} \in E_G \setminus (\mathcal{P}_2(U) \cup \mathcal{P}_2(W)),$$

sprzeczność.

Dla dowodu drugiej części załóżmy, że wierzchołki x i y należą do tej samej składowej H grafu G. Ponieważ graf H jest spójny, więc z części pierwszej wynika natychmiast, że istnieje droga w grafie H, a więc również w

grafie G, łącząca wierzchołki x i y. Z drugiej strony, przypuśćmy, że istnieje droga $(x_0, x_1, \ldots, x_n)$ łącząca wierzchołki x i y. Niech H będzie grafem, którego zbiorem wierzchołków jest $\{x_0, x_1, \ldots, x_n\}$, a zbiorem krawędzi $\{\{x_0, x_1\}, \ldots, \{x_{n-1}, x_n\}\}$. Wtedy H jest spójnym podgrafem grafu G zawierającym wierzchołki x i y (spójność można łatwo pokazać, korzystając z części pierwszej). Zatem istnieje składowa grafu G zawierająca graf H, a więc również wierzchołki x i y. □

Lemat 6.5.

Jeśli $(x_0, \ldots, x_n)$ jest cyklem w spójnym grafie G, to graf $G - \{x_0, x_1\}$ jest spójny.

Dowód.

Na mocy Stwierdzenia 6.4 wystarczy pokazać, że dla dowolnych dwóch wierzchołków x i y grafu G istnieje droga w grafie $G - \{x_0, x_1\}$ łącząca wierzchołki x i y. Ustalmy zatem wierzchołki x i y. Wtedy istnieje droga w grafie G łącząca wierzchołki x i y. Zastępując w tej drodze wszystkie podciągi (x_0, x_1) i (x_1, x_0) ciągami $(x_n, \ldots, x_1)$ oraz $(x_1, \ldots, x_n)$, odpowiednio, otrzymujemy drogę w grafie $G - \{x_0, x_1\}$ łączącą wierzchołki x i y.

Stwierdzenie 6.6.

Niepusty graf spójny G jest drzewem wtedy i tylko wtedy, gdy w grafie G nie ma cyklu.

Dowód.

Załóżmy najpierw, że graf G nie jest drzewem, tzn. $|E_G| \geq |V_G|$. Przez indukcję na $|V_G|$ udowodnimy, że w grafie G jest cykl.

Ponieważ graf G nie jest drzewem, więc $|V_G| > 1$. Wtedy ze spójności grafu G wynika, że $\deg_G x > 0$ dla każdego wierzchołka x grafu G.

Załóżmy najpierw, że istnieje wierzchołek x grafu G taki, że $\deg_G x = 1$. Jeśli $H = G - x$, to graf H jest spójny na mocy Lematu 6.2. Ponadto graf H jest też niepusty. Mamy $|V_H| = |V_G| - 1$ i $|E_H| = |E_G| - 1$, więc $|E_H| \geq |V_H|$, zatem graf H nie jest drzewem. Korzystając z założenia indukcyjnego, wiemy, że w grafie H (a więc także w grafie G) istnieje cykl.

Załóżmy zatem, że $\deg_G x \geq 2$ dla każdego wierzchołka x grafu G. Ponieważ graf G jest niepusty, więc możemy zdefiniować indukcyjnie ciąg $(x_0, x_1, \ldots)$ wierzchołków grafu G taki, że, dla każdego $i \in \mathbb{N}_+$, $\{x_{i-1}, x_i\}$ jest krawędzią w grafie G oraz $x_{i-1} \neq x_{i+1}$. Ponieważ zbiór V_G jest skończony, więc istnieją $m, n \in \mathbb{N}$ takie, że $m < n$ oraz ciąg $(x_m, \ldots, x_n)$ jest cyklem.

Załóżmy teraz, że w grafie G jest cykl $(x_0, \ldots, x_n)$. Z Lematu 6.5 wiemy, że graf $H := G - \{x_0, x_1\}$ jest spójny (i oczywiście niepusty), zatem $|E_H| \geq |V_H| - 1$ na mocy Stwierdzenia 6.3. Ponieważ $|E_H| = |E_G| - 1$ oraz $|V_H| = |V_G$,

więc $|E_G| \geq |V_G$, zatem graf G nie jest drzewem. □

6.2. Grafy planarne

Twierdzenie 6.7 (Euler).
Niech G będzie spójnym grafem planarnym (wraz z ustalonym „dobrym" rysunkiem). Jeśli n jest liczbą wierzchołków grafu G, m liczbą jego krawędzi i f liczbą obszarów, na które rysunek grafu G dzieli płaszczyznę, to

$$n - m + f = 2.$$

W szczególności, liczba f nie zależy od rysunku, a jedynie od grafu G (a dokładniej, od liczby jego wierzchołków i krawędzi).

Dowód.
Dowód będzie indukcyjny ze względu na m. Przypomnijmy, że $m \geq n-1$ na mocy Stwierdzenia 6.3. Jeśli $m = n-1$, to graf G jest drzewem. Ze Stwierdzenia 6.6 wynika, że wtedy $f = 1$. Istotnie, każdy spójny graf planarny dzieli on płaszczyznę na obszary ograniczone oraz jeden obszar nieograniczony. Każdy obszar ograniczony jest jednak otoczony przez cykl, skąd wynika, że w przypadku drzew jednym obszarem jest obszar nieograniczony. Ostatecznie,

$$n - m + f = -(m - n) + f = -(-1) + 1 = 2.$$

Załóżmy teraz, że $m \geq n$. Wtedy graf G nie jest drzewem, a więc w grafie G istnieje cykl $(x_0, \ldots, x_l)$ na mocy Stwierdzenia 6.6. Jeśli $H := G - \{x_0, x_1\}$, n' jest liczbą wierzchołków grafu H, m' liczbą jego krawędzi i f' liczbą obszarów na, które rysunek grafu H (powstały z rysunku grafu G przez wymazanie łuku odpowiadającego krawędzi $\{x_0, x_1\}$) dzieli płaszczyznę, to

$$n' = n, \qquad m' = m - 1 \qquad \text{i} \qquad f' = f - 1.$$

Z Lematu 6.5 wiemy, że graf H jest spójny, więc z założenia indukcyjnego otrzymujemy, że

$$n' - m' + f' = 2.$$

Stąd natychmiast wynika teza. □

Wniosek 6.8.
Niech G będzie spójnym grafem planarnym, n liczbą wierzchołków grafu G oraz m liczbą jego krawędzi. Jeśli $n \geq 3$, to

$$m \leq 3 \cdot n - 6.$$

Dowód.

Ustalmy rysunek grafu G i niech f będzie liczbą obszarów, na które ten rysunek dzieli płaszczyznę. Jeśli graf G jest drzewem, to $m = n-1$. Ponadto, ponieważ $n \geq 3$, więc $n - 1 \leq 3 \cdot n - 6$, co kończy dowód w tym przypadku. Załóżmy zatem, że graf G nie jest drzewem. Ponieważ $n \geq 3$, więc każdy obszar jest otoczony przez co najmniej trzy krawędzie (precyzyjniej, łuki odpowiadające krawędziom) i każda krawędź jest granicą dla co najwyżej dwóch obszarów. Stąd, licząc na dwa sposoby liczbę par (F, e), gdzie F jest jednym z powyższych obszarów, zaś e krawędzią ograniczającą obszar F, otrzymujemy, że

$$3 \cdot f \leq 2 \cdot m.$$

Ponieważ,

$$3 \cdot f = 3 \cdot m - 3 \cdot n + 6$$

na mocy Twierdzenia Eulera, więc otrzymujemy tezę. □

Wniosek 6.9.

Niech n będzie liczbą całkowitą taką, że $n \geq 5$. Jeśli

$$G := ([1, n], \mathcal{P}_2([1, n])),$$

(tzn. G jest grafem pełnym o n wierzchołkach), to graf G nie jest planarny.

Dowód.

Zauważmy, że

$$|E_G| = \binom{n}{2} > 3 \cdot n - 6,$$

więc teza wynika z Wniosku 6.8. □

Stwierdzenie 6.10.

Jeśli G jest grafem planarnym, to istnieje wierzchołek x grafu G taki, że

$$\deg_G x \leq 5.$$

Dowód.

Bez straty ogólności możemy założyć, że graf G jest spójny oraz $|V_G| \geq 3$. Przypuśćmy, że $\deg_G x \geq 6$ dla każdego wierzchołka x grafu G. Wtedy ze Stwierdzenie 6.1 wynika, że

$$6 \cdot |V_G| \leq 2 \cdot |E_G|.$$

W połączeniu z Wnioskiem 6.8, otrzymujemy, że

$$6 \cdot |V_G| \leq 6 \cdot |V_G| - 12,$$

sprzeczność. □

6.3. Kolorowanie grafów

Uwaga.

Rodzinę $U_1, \ldots, U_k$ podzbiorów zbioru V nazywamy podziałem zbioru V, jeśli:

- $V = U_1 \cup \cdots \cup U_k$;
- $U_i \cap U_j = \varnothing$ dla $i \neq j$.

Definicja.

Jeśli G jest grafem i k jest nieujemną liczbą całkowitą, to mówimy, że graf G jest k-kolorowalny, jeśli istnieje podział zbioru V_G na zbiory $U_1, \ldots, U_k$ takie, że jeśli $i \in [1, k]$, to w grafie nie istnieje krawędź łącząca wierzchołki ze zbioru U_i. Taki podział nazywamy k-kolorowaniem wierzchołków grafu G. Najmniejszą nieujemną liczbę całkowitą k taką, że graf G jest k-kolorowalny, nazywamy liczbą chromatyczną grafu G i oznaczamy χ_G.

Twierdzenie 6.11.

Jeśli G jest grafem planarny, to graf G jest 5-kolorowalny.

Dowód.

Dowód będzie indukcyjny ze względu na $|V_G|$. Teza jest oczywista, gdy $|V_G| \leq 5$. Ze Stwierdzenia 6.10 wiemy, że w grafie G istnieje wierzchołek x taki, że $\deg_G x \leq 5$. Jeśli $H := G - x$, to z założenia indukcyjnego wiemy, że graf H jest 5-kolorowalny. Jeśli $\deg_G x < 5$, to w oczywisty sposób możemy rozszerzyć 5-kolorowanie grafu H do 5-kolorowania grafu G. Załóżmy zatem, że $\deg_G x = 5$. Niech $y_1, \ldots, y_5$ będą kolejnymi, wypisanymi zgodnie z ruchem wskazówek zegara (zakładamy, że mamy ustalony rysunek grafu G) sąsiadami wierzchołka x. Możemy również założyć, że jeśli zbiory $U_1, \ldots, U_5$ tworzą 5-kolorowanie wierzchołków grafu H, to $y_i \in U_i$ dla każdego $i \in [1, 5]$. Dla $i, j \in [1, 5]$ takich, że $i \neq j$, oznaczmy przez $H_{i,j}$ podgraf grafu H indukowany przez zbiór $U_i \cup U_j$.

Pokażemy, że istnieją $i, j \in [1, 5]$ takie, że $i \neq j$ oraz wierzchołki y_i oraz y_j należą do różnych składowych grafu $H_{i,j}$. Istotnie, przypuśćmy, że wierzchołki y_1 oraz y_3 należą do tej samej składowej grafu $H_{1,3}$. Ze Stwierdzenia 6.4 wiemy, że w grafie $H_{1,3}$ istnieje $(z_0, \ldots, z_n)$ droga łącząca wierzchołki y_1 i y_3. Bez straty ogólności możemy założyć, że $z_k \neq z_l$ dla wszystkich $k, l \in [0, n]$ takich, że $k \neq l$. Wtedy ciąg $(x, z_0, \ldots, z_n, x)$ jest cyklem w grafie G nieprzechodzącym przez wierzchołki x_2 i x_4. Z planarności grafu G i Stwierdzenia 6.4 wynika zatem, że wierzchołki x_2 i x_4 należą do różnych składowych grafu $H_{2,4}$.

Wiemy, że istnieją $i, j \in [1, 5]$ takie, że $i \neq j$ oraz, jeśli wierzchołki y_i oraz y_j należą do składowych H' i H'' grafu $H_{i,j}$, odpowiednio, to $H' \neq H''$.

Definiujemy zbiory $U'_1, \ldots, U'_5$ wzorem

$$U'_k := \begin{cases} \{x\} \cup (U_i \setminus V_{H'}) \cup (U_j \cap V_{H'}) & \text{jeśli } k = i, \\ (U_j \setminus V_{H'}) \cup (U_i \cap V_{H'}) & \text{jeśli } k = j, \\ U_k & \text{jeśli } k \neq i, j, \end{cases}$$

(tzn. zamieniamy kolorami wierzchołki ze zbioru $V_{H'}$ oraz kolorujemy wierzchołek x kolorem i). Łatwo sprawdzić, że otrzymujemy w ten sposób 5-kolorowanie grafu G. □