§1. Elementy teorii liczb

Oznaczenie.

$[i,j] := \{k \in \mathbb{Z} \mid i \leq k \leq j\}$, $[i,\infty) := \{k \in \mathbb{Z}k \geq i\}$ oraz $(-\infty,j] := \{k \in \mathbb{Z} \mid j \leq k\}$ dla $i,j \in \mathbb{Z}$.

Definicja.

Jeśli $a,b \in \mathbb{Z}$, to mówimy, że a dzieli b (piszemy $a \mid b$), jeśli istnieje $c \in \mathbb{Z}$ takie, że $b = ca$.

Uwaga.

Jeśli $a,b \in \mathbb{Z}$ oraz $a \neq 0$, to $a \mid b$ wtedy i tylko wtedy, gdy $\frac{b}{a} \in \mathbb{Z}$.

Przykład.

$a \mid a$ dla dowolnego $a \in \mathbb{Z}$.

Przykład.

Jeśli $a \mid b$ i $b \mid c$, to $a \mid c$.

Przykład.

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

Przykład.

$1 \mid a$ dla dowolnego $a \in \mathbb{Z}$. W szczególności, $a \mid 1$ wtedy i tylko wtedy, gdy $a = \pm 1$.

Przykład.

$a \mid 0$ dla dowolnego $a \in \mathbb{Z}$. W szczególności, $0 \mid a$ wtedy i tylko wtedy, gdy $a = 0$.

Uwaga.

Jeśli $a \mid b$ oraz $b \neq 0$, to $|a| \leq |b|$.

Uwaga.

Jeśli $a \mid b$ i $a \mid c$, to $a \mid b \pm c$ oraz $a \mid kc$ dla dowolnego $k \in \mathbb{Z}$. Ponadto, jeśli $am \mid bm$ dla $m \neq 0$, to $a \mid b$.

Definicja.

Jeśli $a,b \in \mathbb{Z}$, to $d \in \mathbb{Z}$ nazywamy największym wspólnym dzielnikiem liczb a i b (piszemy $d = (a,b)$), jeśli spełnione są następujące warunki:

(1) $d \geq 0$,

(2) $d \mid a$ i $d \mid b$,

(3) jeśli $c \mid a$ i $c \mid b$, to $c \mid d$.

Uwaga.

Jeśli d i d' są największymi wspólnymi dzielnikami liczb a i b, to $d = d'$

(z warunków (2) i (3) wynika, że $d \mid d'$ oraz $d' \mid d$, więc $d = d'$ na mocy warunku (1)).

Definicja.
Mówimy, że $a, b \in \mathbb{Z}$ są względnie pierwsze, jeśli $(a, b) = 1$.

Uwaga.
Z powyższej definicji nie jest jasne, czy największy wspólny dzielnik dwóch liczb całkowitych zawsze istnieje.

Przykład.
$(a, b) = (|a|, |b|)$ dla dowolnych $a, b \in \mathbb{Z}$.

Przykład.
$(a, a) = |a|$ dla dowolnego $a \in \mathbb{Z}$.

Przykład.
$(a, 1) = 1$ dla dowolnego $a \in \mathbb{Z}$.

Przykład.
$(a, 0) = |a|$ dla dowolnego $a \in \mathbb{Z}$.

Przykład.
$(a, b) = (b, a)$ dla dowolnych $a, b \in \mathbb{Z}$.

Lemat 1.1.
Jeśli $a = qb + r$ dla $a, b, r, q \in \mathbb{Z}$, to $(a, b) = (b, r)$.

Dowód.
Wystarczy pokazać, że $c \mid a, b$ wtedy i tylko wtedy, gdy $c \mid b, r$.

Twierdzenie 1.2 (Twierdzenie o dzieleniu z resztą).
Jeśli $a, b \in \mathbb{Z}$ oraz $b \neq 0$, to istnieją jednoznacznie wyznaczone $q, r \in \mathbb{Z}$ takie, że

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

Definicja.
Liczby q i r z powyższego twierdzenia nazywamy odpowiednio ilorazem (całkowitym) i resztą z dzielenia a przez b.

Oznaczenie.
Resztę z dzielenia $a \in \mathbb{Z}$ przez $b \in \mathbb{Z}$, $b \neq 0$, oznaczamy $a \bmod b$.

Dowód.
Istnienia dowodzimy wybierając q tak, aby

$$a - qb = \min\{a - q'b \mid q' \in \mathbb{Z},\ a - q'b \geq 0\}$$

oraz kładąc $r := a - qb$.

Dla dowodu jednoznaczności przypuśćmy, że istnieją $q', r' \in \mathbb{Z}$ takie, że $a = q'b + r'$ oraz $0 \leq r' < |b|$. Wtedy $r - r' = (q' - q)b$, więc $b \mid r - r'$, oraz $|r - r'| < |b|$, skąd $r - r' = 0$, a więc także $q' - q = 0$.

WNIOSEK 1.3.

Istnieje największy wspólny dzielnik liczb a i b dla dowolnych $a, b \in \mathbb{Z}$.

DOWÓD.

Indukcja ze względu na $n := \min(|a|, |b|)$.

Gdy $n = 0$, to $a = 0$ i $(a, b) = |b|$, lub $b = 0$ i $(a, b) = |a|$.

Załóżmy, że $n > 0$. Jeśli $|a| = n = |b|$, to $(a, b) = n$. W przeciwnym wypadku możemy założyć bez stary ogólności, że $|a| > n = |b|$. Niech q i r będą ilorazem i resztą z dzielenia a przez b. Wtedy $\min(|b|, |r|) = |r| < n$, więc istnieje (b, r) na mocy założenia indukcyjnego, zatem istnieje (a, b) na mocy Lematu 1.1.

ALGORYTM (ALGORYTM EUKLIDESA).

Wynikiem działania poniższej funkcji dla $a, b \in \mathbb{Z}$ jest (a, b).

```
int Euclides (int a, int b) {
  if (a == 0)
    return abs (b);
  if (b == 0)
    return abs (a);
  if (abs (a) == abs (b))
    return abs (a);
  if (abs (a) > abs (b))
    return Euclides (b, a % b);
  return Euclides (a, b % a);
}
```

STWIERDZENIE 1.4.

Jeśli $a, b \in \mathbb{Z}$, to istnieją $p, q \in \mathbb{Z}$ takie, że

$$(a, b) = pa + qb.$$

DOWÓD.

Indukcja ze względu na $n := \min(|a|, |b|)$.

Gdy $n = 0$, to $a = 0$ i $(a, b) = |b| = 0 \cdot a + (\operatorname{sign} b) \cdot b$, lub $b = 0$ i $(a, b) = |a| = (\operatorname{sign} a) \cdot a + 0 \cdot b$.

Załóżmy, że $n > 0$. Jeśli $|a| = n = |b|$, to $(a, b) = n = (\operatorname{sign} a) \cdot a + 0 \cdot b$. W przeciwnym wypadku możemy założyć bez stary ogólności, że $|a| > n = |b|$.

Niech q i r będą ilorazem i resztą z dzielenia a przez b. Wtedy $\min(|b|, |r|) = |r| < n$, więc na mocy założenia indukcyjnego istnieją $x, y \in \mathbb{Z}$ takie, że $(b, r) = xb + yr$. Wtedy $(a, b) = (b, r) = ya + (x - yr)b$, co kończy dowód.

Uwaga.

Jeśli $a, b \in \mathbb{Z}$, to $(a, b) \mid pa + qb$ dla dowolnych $p, q \in \mathbb{Z}$. W szczególności, jeśli istnieją $p, q \in \mathbb{Z}$ takie, że $1 = pa + qb$, to $(a, b) = 1$.

Algorytm (Rozszerzony algorytm Euklidesa).

Wynikiem działania poniższej funkcji dla $a, b \in \mathbb{Z}$ jest (a, b) oraz $p, q \in \mathbb{Z}$ takie, że $(a, b) = pa + qb$.

```
int Euclides (int a, int b, int & p, int & q) {
  if (a == 0) {
    p = 0;
    if (b > 0)
      q = 1;
    else
      q = -1;
    return abs (b);
  }
  if (b == 0 || abs (a) == abs (b)) {
    if (a > 0)
      p = 1;
    else
      p = -1;
    q = 0;
    return abs (a);
  }
  if (abs (a) > abs (b)) {
    int x;
    int y;
    int d = Euclides (b, a % b, x, y);
    p = y;
    q = x - y * (a / b);
    return d;
  }
  int x;
  int y;
  int d = Euclides (a, b % a, x, y);
  p = x - y * (a / b);
  q = y;
```

```
  return d;
}
```

Wniosek 1.5.

Jeśli $a, b, c \in \mathbb{Z}$, $c \neq 0$, $c \mid a$ i $c \mid b$, to $(\frac{a}{c}, \frac{b}{c}) = \frac{(a,b)}{|c|}$. W szczególności, jeśli $(a, b) \neq 0$, to $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$.

Dowód.

Oczywiście $\frac{(a,b)}{|c|} \geq 0$ oraz $\frac{(a,b)}{|c|} \mid \frac{a}{c}, \frac{b}{c}$, więc $\frac{(a,b)}{|c|} \mid (\frac{a}{c}, \frac{b}{c})$. Z drugiej strony jeśli $(a, b) = pa + qyb$ dla $p, q \in \mathbb{Z}$, to $\frac{(a,b)}{|c|} = (\operatorname{sign} c)p\frac{a}{c} + (\operatorname{sign} c)q\frac{b}{c}$, więc $(\frac{a}{c}, \frac{b}{c}) \mid \frac{(a,b)}{|c|}$, co kończy dowód.

Wniosek 1.6.

Jeśli $(a, b) = 1$ oraz $a \mid bc$, to $a \mid c$.

Dowód.

Ustalmy $p, q \in \mathbb{Z}$ takie, że $1 = pa + qb$. Wtedy $c = (cp)a + q(bc)$, co kończy dowód.

Wniosek 1.7.

Jeśli $(a, b) = 1$, $a \mid c$ i $b \mid c$, to $ab \mid c$.

Dowód.

Jeśli $a = 0$ lub $b = 0$, to $c = 0$ i teza jest oczywista. Załóżmy zatem, że $a \neq 0 \neq b$. Wiemy, że istnieją $p, q \in \mathbb{Z}$ takie, że $1 = pa + qb$. Wtedy $c = (p\frac{c}{b} + y\frac{c}{a})ab$, co kończy dowód.

Wniosek 1.8.

Jeśli $(a, b) = 1 = (a, c)$, to $(a, bc) = 1$.

Dowód.

Istnieją $x, y, p, q \in \mathbb{Z}$ takie, że $1 = xa + yb = pa + qc$ Wtedy $1 = (x + bpy)a + (qy)(bc)$, co kończy dowód.

Uwaga.

Jeśli $(a, bc) = 1$, to $(a, b) = 1 = (a, c)$.

Dowód.

Istnieją $p, q \in \mathbb{Z}$ takie, że $1 = pa + qbc$, co kończy dowód.

Definicja.

Liczbę całkowitą nazywamy pierwszą jeśli $p > 1$ oraz z warunku $a \mid p$ dla $a > 0$ wynika, że $a = 1$ lub $a = p$.

Oznaczenie.

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

Algorytm (Sito Eratostenesa).

Dla $n \in \mathbb{Z}$, $n > 0$, algorytm zwraca wszystkie liczba pierwsze nie większe niż n.

```
int Eratostenes (int n, int * primes) {
  int num = 0;
  bool * prime = new bool [n + 1];
  for (int i = 2; i <= n; i++)
    prime [i] = true;
  for (int i = 2; i <= n; i++)
    if (prime [i]) {
      primes [num] = i;
      num++;
      if (i <= sqrt (n))
        for (int j = 2 * i; j <= n; j += i)
          prime [j] = false;
    }
  delete [] prime;
  return num;
}
```

Lemat 1.9.

Jeśli $n \in \mathbb{Z}$, $n > 1$, to istnieją $p_1, \ldots, p_k \in \mathbb{P}$ takie, że $n = p_1 \cdots p_k$.

Dowód.

Dowód jest indukcyjny ze względu na n. Jeśli $n \in \mathbb{P}$, to teza jest oczywista. Załóżmy zatem, że $n \notin \mathbb{P}$. Wtedy istnieją $n_1, n_2 \in \mathbb{Z}$, $1 < n_1, n_2 < n$, takie, że $n_1 n_2 = n$. Z założenia indukcyjnego istnieją $p_1, \ldots, p_k, q_1, \ldots, q_l \in \mathbb{P}$ takie, że $n_1 = p_1 \cdots p_k$ i $n_2 = q_1 \ldots q_l$, i wtedy $n = p_1 \cdots p_k q_1 \cdots q_l$, co kończy dowód.

Wniosek 1.10.

Dla $a \in \mathbb{Z}$, $a \neq \pm 1$, istnieje $p \in \mathbb{P}$ taka, że $p \mid a$.

Twierdzenie 1.11.

$|\mathbb{P}| = \infty$.

Dowód (Euklides).

Pokażemy, że dla każdego podzbioru $P \subset \mathbb{P}$ takiego, że $|P| < \infty$ istnieje $p \in \mathbb{P} \setminus P$. Jeśli $P = \varnothing$, to teza jest oczywista. Przypuśćmy, że $P = \{p_1, \ldots, p_n\}$. Wtedy istnieje $p \in \mathbb{P}$ taka, że $p \mid p_1 \cdots p_n + 1$. Oczywiście $p \notin P$, co kończy dowód.

Stwierdzenie 1.12.

Jeśli $p \in \mathbb{P}$ oraz $p \mid ab$ dla $a, b \in \mathbb{Z}$, to $p \mid a$ lub $p \mid b$.

DOWÓD.
Przypuśćmy, że $p \nmid a$. Wtedy $(a, p) = 1$, więc teza wynika z Wniosku 1.6.

WNIOSEK 1.13.
Jeśli $p \in \mathbb{P}$ oraz $p \mid a_1 \cdots a_k$ dla $a_1, \ldots, a_k \in \mathbb{Z}$, to istnieje $i \in \{1, \ldots, k\}$ takie, że $p \mid a_i$.

LEMAT 1.14.
Jeśli $p_1 \leq \cdots \leq p_k$, $q_1 \leq \cdots \leq q_l \in \mathbb{P}$ oraz $p_1 \cdots p_k = q_1 \cdots q_l$, to $k = l$ oraz $p_i = q_i$ dla $i \in [1, k]$.

DOWÓD.
Dowód jest indukcyjny ze względu na k.

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

Załóżmy, że $k > 1$. Z poprzedniego wniosku wiemy, że istnieje $j \in [1, l]$ takie, że $p_k \mid q_j$, a więc $p_k = q_j$. Wtedy $p_1 \cdots p_{k-1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_l$, więc z założenia indukcyjnego wynika, że $k - 1 = l - 1$ (tzn. $k = l$) oraz $p_i = q_i$ dla $i \in [1, j - 1]$ i $p_i = q_{i+1}$ dla $j \in [j, k - 1]$. Ponadto, jeśli $j < k = l$, to $p_k^{k-j} \geq p_j \cdots p_{k-1} = q_{j+1} \cdots q_k \geq q_j^{k-j} = p_k^{k-j}$, skąd $p_j = \cdots = p_k = q_j = \cdots q_k$.

WNIOSEK 1.15 (ZASADNICZE TWIERDZENIE ARYTMETYKI).
Jeśli $n \in \mathbb{Z}$, $n > 1$, to istnieją jednoznacznie wyznaczone $p_1 < \cdots < p_k \in \mathbb{P}$ oraz $\alpha_1, \ldots, \alpha_k \in \mathbb{N}_+$ takie, że

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

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

$$\pi(x) := |\{p \in \mathbb{P} \mid p \leq x\}|.$$

TWIERDZENIE 1.16.
Mamy

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

DEFINICJA.
Niech $a, b, n \in \mathbb{Z}$ oraz $n \neq 0$. Mówimy, że a PRZYSTAJE DO b MODULO n (piszemy $a \equiv b \pmod{n}$), jeśli $n \mid a - b$.

LEMAT 1.17. Niech $a, b, c, d, n, m \in \mathbb{Z}$, $n, m \neq 0$.

(1) Jeśli $a \equiv b \pmod{n}$ oraz $c \equiv d \pmod{n}$, to

$$a \pm c \equiv b \pm d \pmod{n} \qquad \text{i} \qquad ac \equiv bd \pmod{n}.$$

(2) Jeśli $ac \equiv bc \pmod{n}$ oraz $(c, n) = 1$, to $a \equiv b \pmod{n}$.

(3) $ma \equiv mb \pmod{mn}$ wtedy i tylko wtedy, gdy $a \equiv b \pmod{n}$.

Dowód.

(1) Zauważmy, że $(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$ oraz $ac - bd = (a - b)c + (c - d)b$.

(2) Teza wynika z Wniosku 1.6.

(3) Oczywiste (przypomnijmy, że $m \neq 0$).

Stwierdzenie 1.18.
Niech $a, b, n \in \mathbb{Z}$, $n \neq 0$, i niech $d = (a, n)$.

(1) Istnieje $x \in \mathbb{Z}$ takie, że $ax \equiv b \pmod{n}$ wtedy i tylko wtedy, gdy $d \mid b$.

(2) Jeśli $d \mid b$ i $ax \equiv b \pmod{n}$ dla $x \in \mathbb{Z}$, to $ay \equiv b \pmod{n}$ dla $y \in \mathbb{Z}$ wtedy i tylko wtedy, gdy $x \equiv y \pmod{\frac{n}{d}}$.

Dowód.
Oczywiście, jeśli $d \nmid b$, to nie istnieje $x \in \mathbb{Z}$ taki, że $ax \equiv b \pmod{n}$. Przypuśćmy teraz, że $d \mid b$. Wtedy na mocy Lematu 1.17 (3) dla $x \in \mathbb{Z}$ mamy

$$ax \equiv b \pmod{n} \qquad \Longleftrightarrow \qquad a'x \equiv b' \pmod{n'},$$

gdzie $a' := \frac{a}{d}$, $b' := \frac{b}{d}$ i $n' := \frac{n}{d}$. Zauważmy, że $(a', n') = 1$, więc istnieją $p, q \in \mathbb{Z}$ takie, że $1 = pa' + qn'$, i wtedy dla $x = pb'$ mamy $a'x \equiv b' \pmod{n'}$. Z drugiej strony, jeśli $ay \equiv b \pmod{n}$ dla $y \in \mathbb{Z}$, to $a'y \equiv b' \pmod{n'}$ i $y \equiv (pa')y \equiv pb' \pmod{n'}$, co kończy dowód.

Twierdzenie 1.19 (Chińskie twierdzenie o resztach).
Niech $m_1, \ldots, m_k \in \mathbb{Z}$ będą parami względnie pierwsze i $b_1, \ldots, b_k \in \mathbb{Z}$.

(1) Istnieje $x \in \mathbb{Z}$ taki, że

$$x \equiv b_1 \pmod{m_1}, \ \ldots, \ x \equiv b_k \pmod{m_k}.$$

(2) Jeśli

$$x \equiv b_1 \pmod{m_1}, \ \ldots, \ x \equiv b_k \pmod{m_k}$$

i

$$y \equiv b_1 \pmod{m_1}, \ \ldots, \ y \equiv b_k \pmod{m_k}$$

dla $x, y \in \mathbb{Z}$ wtedy i tylko wtedy, gdy $x \equiv y \pmod{m}$, gdzie $m = m_1 \cdots m_k$.

Dowód.

(1) Niech $n_i := \frac{m}{m_i}$ dla $i \in [1,k]$. Z założeń wynika, że $(m_i, n_i) = 1$ dla wszystkich $i \in [1,k]$, zatem dla każdego $i \in [1,k]$ istnieją $p_i, q_i \in \mathbb{Z}$ takie, że $1 = p_i m_i + q_i n_i$. Wtedy $x := b_1 q_1 n_1 + \cdots + b_k q_k n_k$ ma żądane własności.

(2) Oczywiste.

Uwaga.

Niech $a, b, m, n \in \mathbb{Z}$, $m, n > 1$. Niech $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ i $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ dla $p_1 < \cdots < p_k \in \mathbb{P}$ oraz $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \in \mathbb{N}$. Istnieje $x \in \mathbb{Z}$ taki, że

$$x \equiv a \pmod{m} \qquad \text{i} \qquad x \equiv b \pmod{n}$$

wtedy i tylko wtedy, gdy $a \equiv b \pmod{p_i^{\min(\alpha_i, \beta_i)}}$ dla wszystkich $i \in [1,k]$. Jeśli powyższy warunek jest spełniony to powyższy układ kongruencji jest równoważny układowi

$$x \equiv c_i \pmod{p_i^{\max(\alpha_i, \beta_i)}}, \quad i \in [1,k],$$

gdzie

$$c_i := \begin{cases} a & \alpha_i \geq \beta_i, \\ b & \alpha_i < \beta_i, \end{cases} \qquad i \in [1,k].$$

Definicja.

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

$$\varphi(n) := |U_n|, \qquad \text{gdzie} \qquad U_n := \{a \in [0, n-1] \mid (a, n) = 1\}.$$

Przykład.

$\varphi(1) = 1$.

Przykład.

$\varphi(p) = p - 1$ jeśli $p \in \mathbb{P}$.

Przykład.

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

Lemat 1.20.

Jeśli $p \in \mathbb{P}$ oraz $k \in \mathbb{N}$, to $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$.

Dowód.

Mamy równości

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

LEMAT 1.21.

Jeśli $m, n \in \mathbb{N}_+$ oraz $(m, n) = 1$, to $\varphi(mn) = \varphi(m)\varphi(n)$.

DOWÓD.

Rozważmy funkcję $f : [0, mn-1] \to [0, m-1] \times [0, n-1]$ daną wzorem $f(k) := (k \bmod m, k \bmod n)$. Z Chińskiego Twierdzenia o Resztach wynika, że funkcja ta jest bijekcją. Ponadto

$$\begin{aligned}(k, mn) = 1 \iff & (k, m) = 1 \wedge (k, n) = 1 \\ \iff & (k \bmod m, m) = 1 \wedge (k \bmod n, n) = 1\end{aligned}$$

dla $k \in \mathbb{Z}$, zatem powyższa funkcja indukuje bijekcję $U_{mn} \to U_m \times U_n$.

UWAGA.

Przypuśćmy, że $p, q \in \mathbb{P}$, $p \neq q$, oraz $n = pq$. Wtedy znajomość n, p i q jest równoważna znajomości n i $\varphi(n)$.

DOWÓD.

Zauważmy, że p i q są rozwiązaniami następującego układu równań

$$\begin{cases} pq = n \\ p + q = n + 1 - \varphi(n) \end{cases}.$$

WNIOSEK 1.22.

Jeśli $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ dla $p_1, \ldots, p_k \in \mathbb{P}$, $p_i \neq p_j$ dla $i \neq j$, $\alpha_1, \ldots, \alpha \in \mathbb{N}_+$, to

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1} = n\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_k}\Big).$$

TWIERDZENIE 1.23 (EULER).

Jeśli $n \in \mathbb{N}_+$, $a \in \mathbb{Z}$ i $(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \pmod{n}$.

DOWÓD.

Rozważmy funkcję $f : U_n \to U_n$ daną wzorem $f(b) := ab \bmod n$. Zauważmy, że założenie $(a, n) = 1$ implikuje, że funkcja f jest injekcją (Lemat 1.17 (2)) i surjekcją (Stwierdzenie 1.18 (1)), więc funkcja f jest bijekcją. Stąd

$$\prod_{b \in U_n} b = \prod_{b \in U_n} f(b) \equiv \prod_{b \in U_n} ab = a^{\varphi(n)} \prod_{b \in U_n} b \pmod{n},$$

skąd wynika teza, gdyż $(\prod_{b \in U_n} b, n) = 1$.

WNIOSEK 1.24.

Jeśli $a \in \mathbb{P}$, $a \in \mathbb{Z}$ i $(a, p) = 1$, to $a^{p-1} \equiv 1 \pmod{p}$.

Wniosek 1.25.
Jeśli $a \in \mathbb{P}$ i $a \in \mathbb{Z}$, to $a^p \equiv a \pmod{p}$.

Dowód.
Jeśli $(a,p) = 1$, to $a^p = aa^{p-1} \equiv a \pmod{p}$ na mocy poprzedniego wniosku. Gdy $(a,p) \neq 1$, to $p \mid a$, więc $a^p \equiv 0 \equiv a \pmod{p}$, co kończy dowód.

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 używanym do zapisu tekstu (litery, bądź ich parom, trójkom, ..., znaki przestankowe, itd.) z elementami zbioru $\{0, \ldots, N-1\}$ dla pewnego $N > 0$.

Definicja.
Systemem kryptograficznym nazywamy 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 $N > 0$ oraz $k \in [0, N-1]$. Niech $P := [0, N-1] := C$ oraz $f : P \to C$, gdzie $f(a) := (a + k) \bmod N$. Funkcją odwrotna $f^{-1} : C \to P$ dana jest wzorem $f^{-1}(b) := (b - k) \bmod N$. 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, $n := pq$, oraz wybierzmy (losowo) liczbę $e \in [2, \varphi(n) - 1]$ taką, że $(e, \varphi(n)) = 1$. Definiujemy $P := [0, n-1] =: C$ oraz $f : P \to C$ wzorem $f(a) := a^e \bmod n$. Parę (n, e) nazywamy kluczem szyfrującym. Kluczem deszyfrującym nazywamy parę (n, d), gdzie $d \in [2, \varphi(n) - 1]$ jest rozwiązaniem kongruencji $de \equiv 1 \pmod{\varphi(n)}$.

Lemat 1.26.
Jeśli p i q są różnymi liczbami pierwszymi, $n := pq$, $d, e \in [1, \varphi(n) - 1]$ oraz

$de \equiv 1 \pmod{\varphi(n)}$, to $a^{de} \equiv a \pmod{n}$ dla dowolnego $a \in \mathbb{Z}$.

Dowód.

Z Wniosku 1.24 wynika, że jeśli $(a, p) = 1$, to $a^{p-1} \equiv 1 \pmod{p}$, więc $a^{\varphi(n)} \equiv 1 \pmod{p}$, zatem również $a^{de-1} \equiv 1 \pmod{p}$. Stąd $a^{de} \equiv a \pmod{p}$. Ta kongruencja jest również prawdziwa, gdy $(a, p) \neq 1$. Analogicznie pokazujemy, że $a^{de} \equiv a \pmod{q}$, więc teza wynika z Chińskiego Twierdzenia o Resztach.

Uwaga.

Szyfr RSA jest przykładem szyfru asymetrycznego — znajomość klucza szyfrującego nie wystarcza do odszyfrowania wiadomości. Istotnie, wyliczenie d wymaga znajomości $\varphi(n)$, co jest równoważne znajomości rozkładu $n = pq$. 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.

Podstawowe obiekty kombinatoryczne

Definicja.

Jeśli $n \in \mathbb{N}$ oraz X jest zbiorem, to ciągiem długości n (n-elementowym) elementów zbioru X nazywamy każdą funkcję $a : [1, n] \to X$ (piszemy $a = (a_1, \ldots, a_n)$, gdzie $a_i := a(i)$ dla $i \in [1, n]$).

Uwaga.

Jeśli X jest zbiorem o k elementach dla $k \geq 0$, to istnieje k^n ciągów długości n elementów zbioru X dla $n \geq 0$ (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 dla $n > 0$.

Definicja.

Jeśli X jest zbiorem o n elementach, to permutacją zbioru X nazywamy każdy ciąg różnowartościowy długości n. Zbiór wszystkich permutacji zbioru X oznaczamy P_X.

Stwierdzenie 2.1.

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

Dowód.

Dowód będzie indukcyjny ze względu na n. Dla $n = 0$ teza jest oczywista. Przypuśćmy teraz, że $n > 1$. Funkcja $f : P_X \to \bigcup_{x \in X} P_{X \setminus \{x\}}$ dana wzorem

$$f(a) := (a_1, \ldots, a_{n-1})$$

jest bijekcją. Z założenie indukcyjnego wiemy, że $|P_{X \setminus \{x\}}| = (n - 1)!$ dla każdego $x \in X$, więc $|P_X| = n(n - 1)! = n!$, co kończy dowód.

Stwierdzenie 2.2.

Dla $n \in \mathbb{N}_+$ mamy

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

Dowód.

Przypomnijmy, że dla dowolnego $k \in \mathbb{N}_+$ mamy nierówności

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

Wykorzystując te nierówności mamy

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

i

$$\frac{n^n}{n!} = \frac{n^{n-1}}{(n-1)!} = \Big(\frac{n}{n-1}\Big)^{n-1} \Big(\frac{n-1}{n-2}\Big)^{n-2} \cdots \Big(\frac{2}{1}\Big)^1 \leq e^{n-1},$$

co kończy dowód.

TWIERDZENIE 2.3 (STIRLING).
Mamy

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

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

OZNACZENIE.
Jeśli $n, k \in \mathbb{N}$, to $C_{n,k} := C_{[1,n],k}$.

DEFINICJA.
Jeśli $n, k \in \mathbb{N}$, to SYMBOLEM NEWTONA n NAD k nazywamy

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

STWIERDZENIE 2.4.
Jeśli X jest zbiorem o n elementach oraz $k \in \mathbb{N}$, to $|C_{X,k}| = \binom{n}{k}$.

DOWÓD.
Oczywiście $C_{X,k} = \varnothing$, gdy $k > n$. Dla $k \leq n$ rozważmy funkcję $f : P_X \to C_{X,k}$ daną wzorem $f(a) := \{a_1, \ldots, a_k\}$ dla $a \in P_X$. Wtedy dla każdego $A \in C_{X,k}$ mamy

$$f^{-1}(A) = \{a \in P_X \mid (a_1, \ldots, a_k) \in P_A,\ (a_{k+1}, \ldots, a_n) \in P_{X \setminus A}\},$$

co kończy dowód.

Stwierdzenie 2.5.

Jeśli x i y są elementami pierścienia przemiennego R, to

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

Dowód.

Mamy równości

$$(x+y)^n = (x+y)\cdots(x+y) = \sum_{X\subset[1,n]} x^{|X|} y^{n-|X|} =$$
$$\sum_{k\in[0,n]} \sum_{X\in C_{n,k}} x^k y^{n-k} = \sum_{k\in[0,n]} |C_{n,k}| x^k y^{n-k}.$$

Metoda bijektywna

Uwaga.

Zauważmy, że w dowodach Stwierdzeń 2.1 i 2.4 liczyliśmy ilość obiektów kombinatorycznych konstruując funkcję pomiędzy rozważanym zbiorem oraz zbiorem, którego ilość elementów jest 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 2.6.

Jeśli $n, k \in \mathbb{N}_+$, to

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

Dowód.

Rozważmy funkcję $f : C_{n,k} \to C_{n-1,k} \cup C_{n-1,k-1}$ daną wzorem

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

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

$$g(Y) := \begin{cases} Y & Y \in C_{n-1,k}, \\ Y \cup \{n\} & Y \in C_{n-1,k-1}. \end{cases}$$

Uwaga.

Powyższa równość pozwala wyliczać wartości $\binom{n}{k}$ dla $n, k \in \mathbb{N}$ rekurencyjnie z warunkami początkowymi $\binom{n}{0} = 1$ dla $n \in \mathbb{N}$ oraz $\binom{0}{k} = 0$ dla $k \in \mathbb{N}_+$ (lub $\binom{n}{n} = 1$ dla $n \in \mathbb{N}$) — trójkąt Pascala.

Definicja.

Dla $k \in \mathbb{N}$ definiujemy $\binom{T}{k} \in \mathbb{C}[T]$ wzorem

$$\binom{T}{k} := \begin{cases} \frac{T(T-1)\cdots(T-(k-1))}{k!} & k > 0, \\ 1 & k = 0. \end{cases}$$

Uwaga.

Jeśli $k \in \mathbb{N}$, to $\deg \binom{T}{k} = k$, pierwiastkami (jednokrotnymi) wielomianu $\binom{T}{k}$ są $0, \ldots, k-1$.

Wniosek 2.7.

Jeśli $k \in \mathbb{N}_+$, to

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

W szczególności dla dowolnego $x \in \mathbb{C}$ mamy

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

Dowód.

Obie strony powyższej równości są wielomianami, które przyjmują takie same wartości dla $n \in \mathbb{Z}$, $n \geq k$.

Stwierdzenie 2.8.

Jeśli $n \in \mathbb{N}$ 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

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

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

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

Oznaczenie.

Jeśli X jest zbiorem, to

$$2^X := \{A \mid A \subset X\}.$$

Stwierdzenie 2.9.

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

Dowód.

Bez straty ogólności możemy założyć, że $X = [1, n]$ dla pewnego $n \in \mathbb{N}$. 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

$$f(A) := (a_1, \dots, a_n), \qquad \text{gdzie } a_i := \begin{cases} 1 & a_i \in A, \\ 0 & a_i \notin A. \end{cases}$$

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

$$g(a_1, \dots, a_n) := \{i \in [1, n] \mid a_i = 1\}.$$

Wniosek 2.10.

Dla $n \in \mathbb{N}$ mamy

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

Dowód.

Niech $X := 2^{[1,n]}$. Wtedy $|X| = 2^n$. Z drugiej strony $X = \bigcup_{k \in [0,n]} C_{n,k}$, $|C_{n,k}| = \binom{n}{k}$ dla wszystkich $k \in [0, n]$ oraz $C_{n,k} \cap C_{n,l} = \varnothing$ dla wszystkich $k \neq l$, co kończy dowód.

Stwierdzenie 2.11 (wzór Chu–Vandermonde'a).

Jeśli $k, l, n \in \mathbb{N}$, to

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

Dowód.

Niech

$$X := \{(A_1, A_2) \mid A_1 \subset [1, k] \wedge A_2 \subset [k+1, k+l] \wedge |A_1| + |A_2| = n\}$$

i

$$Y := \{B \mid B \subset [1, k+l] \wedge |B| = n\}.$$

Oczywiście $|Y| = \binom{k+l}{n}$. Z drugiej strony $X = \bigcup_{i \in [0,n]} X_j$, gdzie

$$X_i := \{(A_1, A_2) \in X \mid |A_1| = i\}$$

dla $i \in [0, n]$. Zauważmy, że $|X_i| = \binom{k}{j}\binom{l}{n-j}$ dla dowolnego $i \in [1, n]$ oraz $X_i \cap X_j = \varnothing$ dla wszystkich $i \neq j$, więc $|X| = \sum_{i \in [0,n]} \binom{k}{i}\binom{l}{n-i}$.
Rozważmy funkcję $f : X \to Y$ daną wzorem

$$f(A_1, A_2) = A_1 \cup A_2.$$

Funkcja f jest poprawnie określona i jest bijekcją — funkcja odwrotna $g : Y \to X$ dana jest wzorem

$$g(B) = (B \cap [1, k], B \cap [k + 1, k + l]).$$

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

Wniosek 2.12.
Jeśli $x, y \in \mathbb{C}$ oraz $n \in \mathbb{N}$, to

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

Dowód.
Dla ustalonego n mamy dwa wielomiany $F, G \in \mathbb{C}[X, Y]$ dane wzorami

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

Z poprzedniego stwierdzenia wiemy, że $F(k, l) = G(k, l)$ dla dowolnych $k, l \in \mathbb{N}$, skąd wynika teza.

Definicja.
Niech $m, n \in \mathbb{N}$. Drogą z punktu $(0, 0)$ do punktu (m, n) nazywamy każdy ciąg $(a_0, \ldots, a_{m+n})$ punktów płaszczyzny $\mathbb{R}^2$ taki, że $a_0 = (0, 0)$, $a_{m+n} = (m, n)$, oraz dla każdego $i \in [1, m + n]$ albo $a_i = a_{i-1} + \mathbf{x}$ lub $a_i = a_{i-1} + \mathbf{y}$, gdzie $\mathbf{x} = (1, 0)$ oraz $\mathbf{y} = (0, 1)$.

Stwierdzenie 2.13.
Jeśli $m, n \in \mathbb{N}$, to dróg z punktu $(0, 0)$ do punktu (m, n) jest $\binom{m+n}{m}$.

Dowód.

Niech X będzie zbiorem wszystkich dróg z punktu $(0,0)$ do punktu (m,n). Rozważmy funkcję $f : C_{m+n,m} \to X$ daną wzorem

$$f(A) := (a_0, \dots, a_{m+n}),$$

gdzie

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

Funkcja f jest poprawnie określona oraz jest bijekcją — funkcja odwrotna $g : X \to C_{m+n,m}$ dana jest wzorem

$$g(a_0, \dots, a_{m+n}) := \{i \in [1, m+n] \mid a_i - a_{i-1} = \mathbf{x}\}.$$

Wniosek 2.14.

Jeśli $n, k \in \mathbb{N}$, to

$$|\{(x_1, \dots, x_k) \in \mathbb{N}^k \mid x_1 + \dots + x_k = n\}| = \binom{n+k-1}{n}.$$

Dowód.

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

$$Y := \{(x_1, \dots, x_k) \in \mathbb{N}^k \mid x_1 + \dots + x_k = n\}.$$

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

$$f(a_0, \dots, a_{n+k-1}) := (x_1, \dots, x_k),$$

gdzie

$$x_j := |\{i \in [1, n+k-1] \mid \pi(a_i) = j-1 = \pi(a_{i-1})\}|,\ j \in [1,k],$$

oraz $\pi : \mathbb{R}^2 \to \mathbb{R}$ jest rzutowaniem na pierwszą współrzędna. Funkcja f jest poprawnie określona oraz jest bijekcją — funkcja odwrotna $g : Y \to X$ dana jest wzorem

$$g(x_1, \dots, x_k) := (a_0, \dots, a_{n+k-1})$$

gdzie

$$a_i := (p, i-p) \qquad \text{i} \qquad p := \max\{j \in [0,k] \mid x_1 + \dots + x_j + j \le i\}.$$

Reguła włączania i wyłączania

Twierdzenie 2.15.

Dla dowolnych zbiorów $X_1, \ldots, X_n$ mamy

$$\Big|\bigcup_{i\in[1,n]} X_i\Big| = \sum_{k\in[1,n]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n} |X_{i_1}\cap\cdots\cap X_{i_k}|.$$

Dowód.

Indukcja względem n. Dla $n=1$ teza jest oczywista. Podobnie łatwo udowodnić powyższy wzór dla $n=2$. Załóżmy teraz, że $n>2$. Niech $Y_i := X_i \cap X_n$ dla $i\in[1,n-1]$. Wtedy

$$\begin{aligned}
\Big|\bigcup_{i\in[1,n]} X_i\Big| &= \Big|\bigcup_{i\in[1,n-1]} X_i\Big| + |X_n| - \Big|\Big(\bigcup_{i\in[1,n-1]} X_i\Big)\cap X_n\Big| \\
&= \Big|\bigcup_{i\in[1,n-1]} X_i\Big| + |X_n| - \Big|\bigcup_{i\in[1,n-1]} Y_i\Big| \\
&= \sum_{k\in[1,n-1]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n-1} |X_{i_1}\cap\cdots\cap X_{i_k}| \\
&+ |X_n| - \sum_{k\in[1,n-1]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n-1} |Y_{i_1}\cap\cdots\cap Y_{i_k}| \\
&= \sum_{k\in[1,n-1]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n-1} |X_{i_1}\cap\cdots\cap X_{i_k}| + |X_n| \\
&+ \sum_{k\in[2,n]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_{k-1}\le n-1} |X_{i_1}\cap\cdots\cap X_{i_{k-1}}\cap X_n| \\
&= \sum_{k\in[1,n]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n} |X_{i_1}\cap\cdots\cap X_{i_k}|
\end{aligned}$$

Przykład.

Jeśli $n = p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ dla $p_1,\ldots,p_m\in\mathbb{P}$, $p_i\neq p_j$ dla $i\neq j$, $\alpha_1,\ldots,\alpha_m\in\mathbb{N}_+$, to

$$\varphi(n) = n\Big(1-\frac{1}{p_1}\Big)\cdots\Big(1-\frac{1}{p_m}\Big).$$

Rozwiązanie.

Niech $A_i := \{l\in[0,n-1] \mid p_i \mid l\}$ dla $i\in[1,m]$. Zauważmy, ze

$$|A_{i_1}\cap\cdots\cap A_{i_k}| = \frac{n}{p_{i_1}\cdots p_{i_k}}$$

dla dowolnych $1\le i_1<\cdots<i_k\le m$. Stąd

$$\varphi(n) = \Big|[0,n-1]\setminus \bigcup_{i\in[1,m]} A_i\Big| = n - \Big|\bigcup_{i\in[1,m]} A_i\Big|$$

$$
\begin{aligned}
&= n - \sum_{k\in[1,m]} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le m} |A_{i_1}\cap\cdots\cap A_{i_k}| \\
&= n + \sum_{k\in[1,m]} (-1)^{k} \sum_{1\le i_1<\cdots<i_k\le m} \frac{n}{p_{i_1}\cdots p_{i_k}} \\
&= n\Big(\sum_{k\in[0,m]} (-1)^{k} \sum_{1\le i_1<\cdots<i_k\le m} \frac{1}{p_{i_1}\cdots p_{i_k}}\Big) \\
&= n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_m}).
\end{aligned}
$$

Przykład.

Jeśli $n \in \mathbb{N}_+$, $P_n := P_{[1,n]}$, oraz

$$P_n' := \{a \in P_n \mid a_i \neq i \text{ dla } i \in [1,n]\},$$

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

Dowód.

Zauważmy, że $P_n' = P_n \setminus (\bigcup_{i\in[1,n]} X_i)$, gdzie

$$X_i := \{a \in P_n \mid a_i = i\}$$

dla $i \in [1,n]$. Mamy

$$|X_{i_1}\cap\cdots\cap X_{i_k}| = |P_{[1,n]\setminus\{i_1,\ldots,i_k\}}| = (n-k)!$$

dla dowolnych $1 \le i_1 < \cdots < i_k \le n$, skąd

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

Oznaczenie.

Jeśli $x \in \mathbb{R}$, to przez $[x]$ oznaczamy taką liczbę całkowitą, że $|[x]-x| = \min\{|k-x| \mid k \in \mathbb{Z}\}$, przy czym $[x] < x$, gdy $\min\{|k-x| \mid k\in\mathbb{Z}\} = \frac{1}{2}$.

Wniosek 2.16.

(1) Jeśli $n \in \mathbb{N}_+$, to $|P_n'| = [\frac{n!}{e}]$.

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

Dowód.

Wiadomo, że

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

skąd

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

§3. Funkcje tworzące

Szeregi formalne

Definicja.

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

$$\mathcal{A} = \sum_{n \in \mathbb{N}} a_n T^n = a_0 + a_1 T + a_2 T^2 + \cdots ,$$

gdzie $a_n := \mathcal{A}(n) =: [T^n]\mathcal{A}$ dla $n \in \mathbb{N}$. Zbiór szeregów formalnych oznaczamy $\mathbb{C}[[T]]$. W zbiorze $\mathbb{C}[[T]]$ wprowadzamy działania dodawania i mnożenia wzorami

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

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

Lemat 3.1.

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

Dowód.

Niech $\mathcal{A} = \sum_{n \in \mathbb{N}} a_n T^n$. Jeśli szereg $\mathcal{A}$ jest odwracalny, to istnieje szereg $\mathcal{B} = \sum_{n \in \mathbb{N}} b_n T^n$ taki, że $\mathcal{A}\mathcal{B} = 1$, a więc w szczególności $a_0 b_0 = 1$, skąd $a_0 \neq 0$.

Przypuśćmy teraz, że $a_0 \neq 0$. Definiujemy szereg $\mathcal{B} = \sum_{n \in \mathbb{N}} b_n T^n$ wzorami

$$b_0 := \frac{1}{a_0},$$
$$b_n := -\frac{1}{a_0}\Big(\sum_{k \in [1,n]} a_k b_{n-k}\Big), \ n \in \mathbb{N}_+.$$

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

Definicja.

Symbolem $\mathbb{C}((T))$ oznaczamy zbiór ułamków $\frac{\mathcal{A}}{\mathcal{B}}$ dla szeregów $\mathcal{A}, \mathcal{B} \in \mathbb{C}[[T]]$, $\mathcal{B} \neq 0$, przy czym $\frac{\mathcal{A}}{\mathcal{B}} = \frac{\mathcal{C}}{\mathcal{D}}$ dla szeregów $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \in \mathbb{C}[[T]]$ wtedy i tylko wtedy, gdy $\mathcal{A}\mathcal{D} = \mathcal{B}\mathcal{C}$. W zbiorze $\mathbb{C}((T))$ wprowadzamy działania dodawania i mnożenia wzorami

$$\frac{\mathcal{A}}{\mathcal{B}} + \frac{\mathcal{C}}{\mathcal{D}} := \frac{\mathcal{A}\mathcal{D} + \mathcal{B}\mathcal{C}}{\mathcal{B}\mathcal{D}}, \qquad \frac{\mathcal{A}}{\mathcal{B}} \cdot \frac{\mathcal{C}}{\mathcal{D}} := \frac{\mathcal{A}\mathcal{C}}{\mathcal{B}\mathcal{D}}.$$

Zbiór $\mathbb{C}((T))$ wraz z powyższymi działaniami jest działaniami jest ciałem.

PRZYKŁAD.

Jeśli $\lambda \in \mathbb{C}$, to

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

FUNKCJE TWORZĄCE

DEFINICJA.

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

STWIERDZENIE 3.2.

Jeśli $k \in \mathbb{N}_+$, to

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

DOWÓD.

Dla $x \in \mathbb{R}$ niech $\mathcal{A}_x$ będzie funkcją tworzącą ciągu $(\binom{x}{n})_{n\in\mathbb{N}}$, tzn

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

Z Wniosku 2.12 wynika, że $\mathcal{A}_{x+y} = \mathcal{A}_x\mathcal{A}_y$ dla dowolnych $x, y \in \mathbb{R}$. W szczególności $\mathcal{A}_{-k}\mathcal{A}_k = \mathcal{A}_0 = 1$. Ponadto $\mathcal{A}_k = (1+T)^k$, zatem

$$\begin{aligned}
\frac{1}{(1+T)^k} = \frac{1}{\mathcal{A}_k} = \mathcal{A}_{-k} &= \sum_{n\in\mathbb{N}} \binom{-k}{n} T^n \\
&= \sum_{n\in\mathbb{N}} \frac{-k(-k-1)\cdots(-k-n+1)}{n!} T^n \\
&= \sum_{n\in\mathbb{N}} (-1)^n \frac{(k+n-1)\cdots(k+1)k}{n!} T^n \\
&= \sum_{n\in\mathbb{N}} (-1)^n \binom{k+n-1}{n} T^n = \sum_{n\in\mathbb{N}} (-1)^n \binom{k+n-1}{k-1} T^n.
\end{aligned}$$

UWAGA.

Z Wniosku 2.12 wynika, że jeśli $\mathcal{A}^k = 1 + T$ dla $k \in \mathbb{N}_+$ i szeregu $\mathcal{A} \in \mathbb{C}[[T]]$, to $\mathcal{A} = \varepsilon\mathcal{A}_{\frac{1}{k}}$ dla pierwiastka $\varepsilon \in \mathbb{C}$ k-tego stopnia z jedynki, tzn.

$$\sqrt[k]{1+T} = 1 + \sum_{n\in\mathbb{N}_+} (-1)^{n-1} \frac{(k-1)(2k-1)\cdots((n-1)k-1)}{k^n n!}.$$

Wniosek 3.3.

Jeśli $k \in \mathbb{N}_+$ i $\lambda \in \mathbb{C}$, to

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

Uwaga.

Jeśli $F, G \in \mathbb{C}[T]$, to istnieją wielomiany $Q, R \in \mathbb{C}[T]$ takie, że $\deg R < \deg G$ oraz

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

Uwaga.

Niech $F, G \in \mathbb{C}[T]$ będą takie, że $\deg F < \deg G$ oraz $G(0) = 1$. Jeśli $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ są parami różnymi pierwiastkami wielomianu G krotności $m_1, \ldots, m_n$ odpowiednio, to istnieją $A_{i,j} \in \mathbb{C}$, $j \in [1, m_n]$, $i \in [1, n]$, takie, że

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

Przykład.

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

Rozwiązanie.

Jeśli a_n jest szukaną wielkością, to funkcja tworząca $\mathcal{A}$ ciągu $(a_n)_{n \in \mathbb{N}}$ jest równa

$$\begin{aligned}
\mathcal{A} &= (1 + T + T^2 + \cdots)(1 + T^2 + T^4 + \cdots)(1 + T^5 + T^{10} + \cdots) \\
&= \frac{1}{(1-T)(1-T^2)(1-T^5)} = \\
&= \frac{13}{40} \cdot \frac{1}{1-T} + \frac{1}{4} \cdot \frac{1}{(1-T)^2} + \frac{1}{10} \cdot \frac{1}{(1-T)^3} + \frac{1}{8} \cdot \frac{1}{1+T} \\
&+ \frac{1}{25} \cdot \sum_{i \in [1,4]} \frac{2\varepsilon^{2i} + \varepsilon^{3i} + 2\varepsilon^{4i}}{1 - \varepsilon^i T},
\end{aligned}$$

więc

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

gdzie ε jest pierwiastkiem pierwotnym 5-tego stopnia z 1.

Rekurencja

Przykład.

Definiujemy ciąg Fibonacciego (F_n) wzorem

$$F_n := \begin{cases} 0 & n = 0, \\ 1 & n = 1, \\ F_{n-1} + F_{n-2}, & n \geq 2. \end{cases}$$

Policzymy funkcję tworzącą $\mathcal{F}$ ciągu (F_n). Zauważmy, że dla każdego $n \geq 2$ mamy $F_n T^n = F_{n-1} T^n + F_{n-2} T^n$, skąd

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

więc

$$\mathcal{F} = \frac{T}{1 - T - T^2}$$

Definicja.

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

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

dla $u_{r-1}, \ldots, u_0 \in \mathbb{C}$, $u_0 \neq 0$, oraz ciągu $(f_n)_{n \in \mathbb{N}}$. Rekurencję $(*)$ nazywamy jednorodną, jeśli $f_n = 0$ dla wszystkich $n \in \mathbb{N}$. Rekurencją jednorodną stowarzyszoną z rekurencją $(*)$ nazywamy rekurencję

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

Wielomianem charakterystycznym rekurencji $(*)$ nazywamy

$$T^\lambda + u_{r-1} T^{r-1} + \cdots + u_0 \in \mathbb{C}[T].$$

Mówimy, że ciąg $(a_n)_{n \in \mathbb{N}}$ jest rozwiązaniem rekurencji $(*)$ jeśli

$$a_{n+r} + u_{r-1} a_{n+r-1} + \cdots + u_0 a_n = f_n$$

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

Uwaga.

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

Twierdzenie 3.4.

Niech

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

będzie rekurencją liniową o stałych współczynnikach.

(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

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

jest rekurencją liniową o stałych współczynnikach, to zbiór A rozwiązań tej rekurencji możemy znajdować następująco:

(1) znajdujemy zbiór A' 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 3.5.

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

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

rzędu r, to ciągi $(n^j \lambda_i^n)_{n\in\mathbb{N}}$, $j \in [0, k_i - 1]$, $i \in [1, l]$, tworzą bazę przestrzeni rozwiązań rekurencji $(*)$.

DOWÓD.

Udowodnimy najpierw, że powyższe ciągi generują przestrzeń rozwiązań rekurencji $(*)$. Niech ciąg $a = (a_n)_{n\in\mathbb{N}}$ będzie rozwiązaniem rekurencji $(*)$. Policzymy funkcję tworzącą $\mathcal{A}$ ciągu a

$$\begin{aligned}
&(1 + u_{r-1}T + \cdots + u_0T^r)\mathcal{A} \\
&= \Bigl(\sum_{i\in[0,r]} u_iT^{r-i}\Bigr)\Bigl(\sum_{n\in\mathbb{N}} a_nT^n\Bigr) = \sum_{i\in[0,r]}\sum_{n\in\mathbb{N}} u_ia_nT^{n+r-i} \\
&= \sum_{i\in[0,r]}\sum_{m\in[-i,\infty)} u_ia_{m+i}T^{m+r} = \sum_{m\in[-r,\infty)}\Bigl(\sum_{i\in[\max(0,-m),r]} u_ia_{m+i}\Bigr)T^{m+r} \\
&= \sum_{m\in[-r,-1]}\Bigl(\sum_{i\in[-m,r]} u_ia_{m+i}\Bigr)T^{m+r} + \sum_{m\in\mathbb{N}}\Bigl(\sum_{i\in[0,r]} u_ia_{m+i}\Bigr)T^{m+r} \\
&= \sum_{n\in[0,r-1]}\Bigl(\sum_{i\in[r-n,r]} u_ia_{n+i-r}\Bigr)T^n,
\end{aligned}$$

gdzie $u_r := 1$, więc

$$\mathcal{A} = \frac{\sum_{n\in[0,r-1]}\Bigl(\sum_{i\in[r-n,r]} u_ia_{n+i-r}\Bigr)T^n}{1 + u_{r-1}T + \cdots + u_0T^r}.$$

Zauważmy, że

$$\deg\Bigl(\sum_{n\in[0,r-1]}\Bigl(\sum_{i\in[r-n,r]} u_ia_{n+i-r}\Bigr)T^n\Bigr) < r = \deg(1 + u_{r-1}T + \cdots + u_0T^r),$$

oraz że $\lambda_1^{-1}, \ldots, \lambda_l^{-1}$ są parami różnymi pierwiastkami wielomianu $1+u_{r-1}T+\cdots+u_0T^r$ krotności $k_1, \ldots, k_r$, odpowiednio. Stąd istnieją $A_{i,j} \in \mathbb{C}$, $i \in [1, l]$, $j \in [1, k_i]$, takie, że

$$\mathcal{A} = \sum_{i\in[1,n]}\sum_{j\in[1,k_i]} \frac{A_{i,j}}{(1 - \lambda_iT)^j}.$$

Z Wniosku 3.3 wynika, że

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

tzn.

$$a_n = A_{i,j}\binom{j+n-1}{j-1}\lambda_i^n \qquad \text{dla wszystkich } n \in \mathbb{N}.$$

Ponieważ $\binom{T}{j-1}$ jest wielomianem stopnia $j-1$, więc także $\binom{T+j-1}{j-1}$ jest wielomianem stopnia $j-1$, zatem ciąg $(\binom{j+n-1}{j-1})_{n\in\mathbb{N}}$ jest kombinacją liniową ciągów 1, n, $\ldots$, n^{j-1} dla $j \in [1, k_i]$, $i \in [1, l]$, co kończy dowód pierwszej części twierdzenia.

Aby zakończyć dowód wystarczy pokazać, że wymiar przestrzeni rozwiązań rekurencji $(*)$ jest równy r. Rozważmy przekształcenie liniowe $F : \mathbb{C}^r \to \mathbb{C}^{\mathbb{N}}$ dane wzorem

$$F(a_0, \ldots, a_{r-1}) := (a_0, a_1, \ldots),$$

gdzie

$$a_{n+r} := -(u_{r-1}a_{n+r-1} + \cdots + u_0 a_n) \qquad \text{dla } n \in \mathbb{N}.$$

Wtedy przekształcenie F jest różnowartościowa oraz obraz przekształcenia F jest równy przestrzeni rozwiązań rekurencji $(*)$, co kończy dowód.

Przykład.

Wielomianem charakterystycznym rekurencji $X_{n+2} = X_{n+1} + X_n$, $n \in \mathbb{N}$, jest wielomian $T^2 - T - 1 = 0$, którego pierwiastkami są $\frac{1\pm\sqrt{5}}{2}$. Zatem istnieją $\mu_1, \mu_2 \in \mathbb{C}$ takie, że

$$F_n = \mu_1\Big(\frac{1+\sqrt{5}}{2}\Big)^n + \mu_2\Big(\frac{1-\sqrt{5}}{2}\Big)^n, \ n \in \mathbb{N}.$$

Rozwiązując układ równań powstały przez podstawienie $n = 0$ i $n = 1$ otrzymujemy, że $\mu_1 = \frac{\sqrt{5}}{5}$ i $\mu_2 = -\frac{\sqrt{5}}{5}$, zatem ostatecznie

$$F_n = \frac{\sqrt{5}}{5}\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \frac{\sqrt{5}}{5}\Big(\frac{1-\sqrt{5}}{2}\Big)^n, \ n \in \mathbb{N}.$$

Twierdzenie 3.6.

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

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

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

Dowód.

Bez straty ogólności możemy założyć, że $f \neq 0$. Niech $m := \deg f$. Pokażemy najpierw, że istnieje rekurencja jednorodna

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

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 $F = (T-1)^{m+1}G$.

Dowód powyżej tezy będzie indukcyjny ze względu m. Rozważmy rekruencję

$$(***)\ \ X_{n+r+1} + (u_{r-1}-1)X_{n+r} + \cdots + (u_0 - u_1)X_{n+1} + X_n = f'(n),\ n \in \mathbb{N},$$

gdzie $f'(T) := f(T+1) - f(T)$. Zauważmy, że jeśli ciąg a jest rozwiązaniem rekurencji $(*)$, to ciąg a jest rozwiązaniem rekurencji $(***)$. Ponadto wielomian charakterystyczny rekurencji $(***)$ jest postaci $(T-1)F$. Wreszcie rząd rekurencji $(***)$ jest równy $r+1$, $\deg f' = m-1$, gdy $m > 0$, oraz $f' = 0$, gdy $m = 0$,, zatem teza wynika z założenia indukcyjnego.

Niech $\lambda_0 = 1$, λ_1, ..., λ_l będą pierwiastkami wielomianu G krotności $k_0 = k + m + 1$, k_1, ..., k_l, odpowiednio. Ustalmy rozwiązanie $(a_n)_{n\in\mathbb{N}}$ rekurencji $(*)$. Z poprzedniego twierdzenia wiemy, że istnieją $A_{i,j}$, $i \in [0,l]$, $j \in [0, k_l - 1]$, takie, że

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

dla wszystkich $n \in \mathbb{N}$. Ponieważ pierwiastkami wielomianu F są λ_0, λ_1, ..., λ_l, a ich krotności to k, k_1, ..., k_l, więc korzystając ponownie z poprzedniego twierdzenia otrzymujemy, że ciąg

$$\Big(\sum_{j\in[0,k_0-m-2]} A_{0,j} n^j + \sum_{i\in[1,l]} \sum_{j\in[0,k_l-1]} A_{i,j} n^j \lambda_i^n\Big)_{n\in\mathbb{N}}$$

jest rozwiązaniem rekurencji jednorodnej stowarzyszonej z rekurencją $(*)$. Wobec Twierdzenie 3.4 (3) oznacza to, że ciąg

$$\Big(\sum_{j\in[k,k+m]} A_{0,j} n^j\Big)_{n\in\mathbb{N}}$$

jest rozwiązaniem rekruencji $(*)$, co kończy dowód.

Uwaga.

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

PRZYKŁAD.
Niech

$$s_n := \sum_{k\in[1,n]} k^3 \; n \in \mathbb{N}.$$

Zauważmy, że ciąg $(s_n)_{n\in\mathbb{N}}$ jest rozwiązaniem rekurencji

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

Wielomianem charakterystycznym powyższej rekurencji jest wielomian $T-1$, którego jedynym pierwiastkiem (jednokrotnym) jest 1. Z powyższego twierdzenia wynika zatem, że istnieje ciąg $(s'_n)_{n\in\mathbb{N}}$ taki, że

$$(*) \quad s'_n = n(\mu'_3 n^3 + \mu'_2 n^2 + \mu'_1 n + \mu'_0), \; n \in \mathbb{N},$$

dla pewnych $\mu'_0, \mu'_1, \mu'_2, \mu'_3 \in \mathbb{C}$, oraz

$$s'_{n+1} - s'_n = n^3 + 3n^2 + 3n + 1, \; n \in \mathbb{N}.$$

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

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

którego rozwiązaniem są

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

Na mocy Twierdzenie 3.5 wynika zatem, że istnieje $\mu \in \mathbb{C}$ takie, że

$$s_n = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 + \mu.$$

Podstawiając $n = 0$ otrzymujemy, że $\mu = 0$, zatem ostatecznie

$$s_n = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2 = \frac{n^2(n+1)^2}{4}.$$

PRZYKŁAD (WIEŻE Z HANOI).
Załóżmy, że na pierwszym z trzech ponumerowanych drążków znajduje się n krążków o parami różnych średnicach, przy czym krążki ułożone są (patrząc

od dołu) od największego do najmniejszego. Niech r_n oznacza ilość przełożeń krążków niezbędną do przełożenia wszystkich krążków z drążka pierwszego na drugi, przy czym w żadnym momencie krążek większy nie może leżeć powyżej krążka mniejszego. Można zauważyć, że ciąg $(r_n)_{n\in\mathbb{N}}$ jest rozwiązaniem rekurencji

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

Wielomianem charakterystycznym powyższej rekurencji jest wielomian $T-2$, którego jedynym pierwiastkiem (jednokrotnym) jest 2. Z Twierdzenia 3.6 wynika zatem, że istnieje ciąg $(r'_n)_{n\in\mathbb{N}}$ taki, że

$$(*) \quad r'_n = \mu', \ n \in \mathbb{N},$$

dla pewnego $\mu' \in \mathbb{C}$, oraz

$$r'_{n+1} - 2r'_n = 1, \ n \in \mathbb{N}.$$

Podstawiając wzór $(*)$ do powyżej równości i porównując współczynniki przy poszczególnych potęgach n otrzymujemy, że $\mu' = -1$, zatem na mocy Twierdzenia 3.5 istnieje $\mu \in \mathbb{C}$ takie, że $r_n = -1 + \mu 2^n$. Podstawiając $n = 0$ otrzymujemy, że $\mu = 1$, zatem ostatecznie

$$r_n = 2^n - 1, \ n \in \mathbb{N}.$$

Twierdzenie 3.7.
Niech $\mathcal{A}$ będzie funkcją generującą ciągu $(a_n)_{n\in\mathbb{N}}$. Jeśli

$$\mathcal{A} = \frac{F}{1 + u_{r-1}T + \cdots + u_0 T^r}$$

dla pewnych $u_0, \ldots, u_{r-1} \in \mathbb{C}$, $u_0 \neq 0$, oraz wielomianu $F \in \mathbb{C}[T]$ takiego, że $\deg F < r$, to ciąg $(a_n)_{n\in\mathbb{N}}$ jest rozwiązaniem rekurencji

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

Dowód.
Zauważmy, że powyższa równość oznacza, że

$$(1 + u_{r-1}T + \cdots + u_0 T)\mathcal{A} = F,$$

zatem

$$0 = [T^n]F = [T^n]((1+u_{r-1}T+\cdots+u_0T)\mathcal{A}) = a_n + u_{r-1}u_{n-1} + \cdots + u_0 u_{n-r}$$

dla wszystkich $n \in \mathbb{N}$, $n \geq r$, co kończy dowód.

PRZYKŁAD.

Niech a_n będzie ilością ciągów binarnych długości n, $n \in \mathbb{N}$, w których występuje parzysta liczba jedynek oraz każde dwie jedynki rozdzielone są co najmniej jednym zerem. Takich ciągów zaczynających się od zera jest a_{n-1} gdy $n > 0$. Z drugiej strony, jeśli mamy ciąg $x = (x_1, \ldots, x_n)$ spełniający powyższe warunki taki, że $x_1 = 1$, to niech $k_x := \min\{i \in [2, n] \mid x_i = 1\}$. Zauważmy, że $k_x \in [3, n]$. Dla ustalonego $k \in [3, n-1]$ ciągów x dla których $k_x = k$ jest a_{n-k-1}, oraz jest jeden ciąg x dla którego $k_x = n$, jeśli $n \geq 3$ $(x = (1, 0, \ldots, 0, 1)$. Otrzymujemy zatem równość

$$a_n = \begin{cases} a_{n-1} & n = 1, 2, \\ a_{n-1} + \sum_{k\in[3,n-1]} a_{n-k-1} + 1 & n \geq 3. \end{cases}$$

Zauważmy też, że $a_0 = 1$. Z powyższej równości wynika, że

$$\begin{aligned} \mathcal{A} &= \sum_{n\in\mathbb{N}} a_n T^n \\ &= 1 + \sum_{n\in\mathbb{N}_+} a_{n-1} T^{n-1} T + \sum_{\substack{n\in\mathbb{N} \\ n\geq 3}} \sum_{k\in[3,n-1]} a_{n-k-1} T^{n-k-1} T^{k+1} + \sum_{\substack{n\in\mathbb{N} \\ n\geq 3}} T^n \\ &= 1 + T\mathcal{A} + \sum_{\substack{k\in\mathbb{N} \\ k\geq 3}} \sum_{\substack{n\in\mathbb{N} \\ n\geq k+1}} a_{n-k-1} T^{n-k-1} T^{k+1} + \frac{T^3}{1-T} \\ &= 1 + T\mathcal{A} + \sum_{\substack{k\in\mathbb{N} \\ k\geq 3}} \mathcal{A} T^{k+1} + \frac{T^3}{1-T} = 1 + T\mathcal{A} + \mathcal{A}\frac{T^4}{1-T} + \frac{T^3}{1-T}, \end{aligned}$$

skąd

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

a więc ciąg (a_n) jest rozwiązaniem rekurencji

$$X_{n+4} - 2X_{n+2} + X_{n+1} - X_n = 0, \ n \in \mathbb{N}.$$

Zauważmy, że $a_0 = a_1 = a_2 = 1$ oraz $a_3 = 2$.

PRZYKŁAD (LICZBY CATALANA).

Niech c_n oznacza liczbę drzew binarnych o n wierzchołkach dla $n \in \mathbb{N}$. Przypomnijmy, że drzewem binarnym o n wierzchołkach nazywamy $\varnothing$, gdy $n = 0$, oraz parę (L, R) drzew binarnych o k i $(n-1)-k$ wierzchołkach dla pewnego $k \in [0, n-1]$, gdy $n > 0$. Zauważmy, że $c_0 = 1$ oraz

$$c_n = \sum_{j\in[0,n-1]} c_j c_{n-1-j}$$

dla wszystkich $n \in \mathbb{N}_+$. Niech $\mathcal{C}$ będzie funkcją tworzącą ciągu $(c_n)_{n\in\mathbb{N}}$. Wtedy

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

skąd

$$\mathcal{C} = \frac{1 \pm \sqrt{1-4T}}{2T}.$$

Zauważmy, że

$$\sqrt{1-4T} = 1 - \sum_{n\in\mathbb{N}^+} \frac{1\cdot 3\cdots(2n-3)}{2^n n!} 4^n T^n = 1 - \sum_{n\in\mathbb{N}^+} \frac{2}{n}\binom{2n-2}{n-1} T^n.$$

Stąd

$$\mathcal{C} = \frac{1-\sqrt{1-4T}}{2T} = \sum_{n\in\mathbb{N}^+} \frac{1}{n}\binom{2n-2}{n-1} T^{n-1} = \sum_{n\in\mathbb{N}} \frac{1}{n+1}\binom{2n}{n} T^n,$$

a więc $c_n = \frac{1}{n+1}\binom{2n}{n}$ dla wszystkich $n \in \mathbb{N}$.

Wielomiany wieżowe

Definicja.

Niech $n, m \in \mathbb{N}$. Szachownicą o n wierszach i m kolumnach nazywamy każdą trójkę $B = (I, J, F)$, gdzie I oraz J są zbiorami, $|I| = n$, $|J| = m$, oraz $F \subset I \times J$. 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.

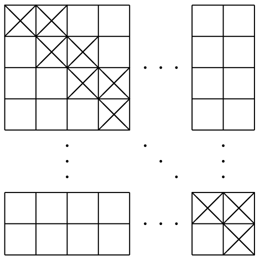
Niech $B = (I, J, F)$ będzie szachownicą oraz $k \in \mathbb{N}$. Rozstawieniem k wież na szachownicy B nazywamy każdy podzbiór $\{(i_1, j_1), \ldots, (i_k, j_k)\} \in I \times J \setminus F$ taki, że $i_p \neq i_q$ oraz $j_p \neq j_q$ dla wszystkich $p \neq q$. Ilość rozstawień k wież na szachownicy B oznaczamy r_k^B.

Przykład.

$r_0^B = 1$, $r_1^B = |I||J| - |F|$, oraz $r_k^B = 0$ dla wszystkich $k \geq \min(|I|, |J|)$, dla dowolnej szachownicy $B = (I, J, F)$.

Przykład.

Dla $n \in \mathbb{N}_+$ ilość permutacji σ zbioru $[1, n]$ takich, że $\sigma(i) \neq i, i+1$ dla wszystkich $i \in [1, n]$ jest równa r_n^B dla szachownicy

$B =$ 

o n wierszach i n kolumnach.

Definicja.

Wielomianem wieżowym szachownicy B nazywamy funkcję tworzącą ciągu $(r_k^B)_{k\in\mathbb{N}}$. Wielomian wieżowy szachownicy B oznaczamy 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 $F^{\mathrm{tr}} := \{(j, i) \mid (i, j) \in F\}$.

Przykład.

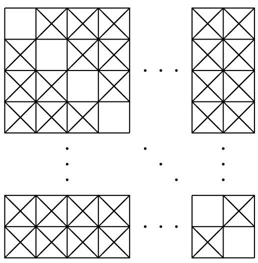
Jeśli $B = (I, J, \varnothing)$, to $R_B = \sum_{k\in\mathbb{N}} \binom{|I|}{k}\binom{|J|}{k} k! T^k$.

Przykład.

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

Przykład.

Jeśli

$B =$ 

jest szachownicą o n wierszach i n kolumnach, to $R_B = \sum_{k\in\mathbb{N}} \binom{n}{k} T^k = (1 + T)^n$.

Oznaczenie.

Jeśli $B = (I, J, F)$ jest szachownicą, $\sigma \in P_I$ i $\tau \in P_J$, to $B_\sigma := (I, J, F_\sigma)$, gdzie $F_\sigma := \{(\sigma(i), j) \mid (i, j) \in F\}$, oraz $B^\tau := (I, J, F^\tau)$, gdzie $F^\tau := \{(i, \tau(j)) \mid (i, j) \in F\}$. Mówimy, że szachownice B_σ i B^τ są otrzymane przez permutację wierszy i kolumn, odpowiednio. Zauważmy, że $(B_\sigma)^\tau = (B^\tau)_\sigma$ i tę szachownicę oznaczamy B_σ^τ.

UWAGA.

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

OZNACZENIE.

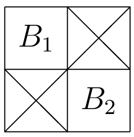
Jeśli $B = (I, J, F)$ jest szachownicą, $i_0 \in I$ i $j_0 \in J$, to $B_i := (I \setminus \{i_0\}, J, F_i)$, gdzie $F_{i_0} := \{(i, j) \in F \mid i \neq i_0\}$, oraz $B^{j_0} := (I, J \setminus \{j_0\}, F^{j_0})$, gdzie $F^{j_0} := \{(i, j) \in F \mid j \neq j_0\}$. Mówimy, że szachownice B_{i_0} i B^{j_0} są otrzymane przez usunięcie wiersza i_0 oraz kolumny j_0, odpowiednio. Zauważmy, że $(B_{i_0})^{j_0} = (B^{j_0})_{i_0}$ i tę szachownicę oznaczamy $B_{i_0}^{j_0}$.

UWAGA.

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

PRZYKŁAD.

Niech $B = (I, J, F)$ będzie szachownicą, $I = I_1 \cup I_2$, oraz $J = J_1 \cup J_2$, przy czym $I_1 \cap I_2 = \varnothing$ oraz $J_1 \cap J_2 = \varnothing$. Jeśli $I_1 \times J_2 \cup I_2 \times J_1 \subset F$, to $R_B = R_{B_1} R_{B_2}$, gdzie $B_1 = (I_1, J_1, F \cap (I_1 \times J_1))$ oraz $B_2 = (I_2, J_2, F \cap (I_2 \times J_2))$. Innymi słowy, jeśli

$B =$ 

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

TWIERDZENIE 3.8.

Jeśli $B = (I, J, F)$ jest szachownicą oraz $(i_0, j_0) \in (I \times J) \setminus F$, to $R_B = R_{B'} + T R_{B_{i_0}^{j_0}}$, gdzie $B' = (I, J, F \cup (i_0, j_0))$.

DOWÓD.

Ustalmy $k \in \mathbb{N}_+$. 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 jest zbiorem tych rozstawień A, dla których $(i_0, j_0) \in A$. Oczywiście $X_1 \cap X_2 = \varnothing$. Ponadto $|X_1| = r_k^{B'}$ oraz $|X_2| = r_{k-1}^{B_{i_0}^{j_0}}$, zatem

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

Oczywiście

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

co kończy dowód.

DEFINICJA.

NEGATYWEM SZACHOWNICY $B = (I, J, F)$ nazywamy szachownicę $\overline{B} := (I, J, \overline{F})$, gdzie $\overline{F} := (I \times J) \setminus F$.

TWIERDZENIE 3.9.

Jeśli $n \in \mathbb{N}$ oraz $B = (I, J, F)$ jest szachownicą taką, że $|I| = n = |J|$, to ilość rozstawień n wież na szachownicy $\overline{B}$ jest równa $\sum_{k \in [0,n]} (-1)^k r_k^B (n-k)!$.

DOWÓD.

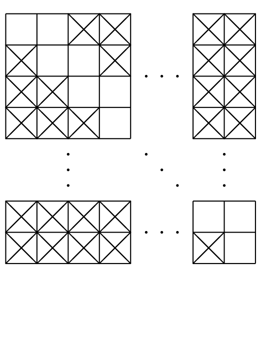
Bez straty ogólności możemy założyć, że $I = [1, n] = J$. Niech $B' := (I, J, \varnothing)$ oraz niech X i Y będą zbiorami wszystkich rozstawień n wież na szachownicach $\overline{B}$ i B', odpowiednio. Zauważmy, że $X = Y \setminus \bigcup_{i \in [1,n]} Y_i$, gdzie $Y_i := \{A \in Y \mid A \cap (\{i\} \times J) \cap F = \varnothing\}$ dla $i \in [1, n]$, tzn. Y_i jest zbiorem tych rozstawień A dla których wieża stojąca w wierszu i stoi na polu dozwolonym w szachownicy B. Ustalmy $k \in [0, n]$. Zbiór Z_k rozstawień k wież na szachownicy B możemy przedstawić w postaci sumy $Z_k = \bigcup_{1 \leq i_1 < \cdots < i_k \leq n} Z_{i_1,\ldots,i_k}$, gdzie $Z_{i_1,\ldots,i_k} := \{A \in Z_k \mid A \subset \{i_1, \ldots, i_k\} \times J\}$ dla $1 \leq i_1 < \cdots < i_k \leq n$, tzn. $Z_{i_1,\ldots,i_k}$ jest zbiorem tych rozstawień A k wież na szachownicy B, w których stoją one we wierszach $i_1, \ldots, i_k$. Zauważmy, że $|Y_{i_1} \cap \cdots \cap Y_{i_k}| = |Z_{i_1,\ldots,i_k}|(n-k)!$ dla dowolnych $1 \leq i_1 < \cdots < i_k \leq n$, zatem

$$\sum_{1 \leq i_1 < \cdots < i_k \leq n} |Y_{i_1} \cap \cdots \cap Y_{i_k}| = \sum_{1 \leq i_1 < \cdots < i_k \leq n} |Z_{i_1,\ldots,i_k}|(n-k)!$$
$$= |Z_k|(n-k)! = r_k^B (n-k)!,$$

zatem teza wynika ze wzoru włączeń i wyłączeń (zauważmy, że $|Y| = n! = 1 \cdot n! = r_0^B n!$).

PRZYKŁAD.

Ustalmy $n \in \mathbb{N}$. Niech a_n oznacza liczbę permutacji $\sigma \in P_n$ takich, że $\sigma(n) \neq n, n+1$. Z powyższego twierdzenia wynika, że $a_n = \sum_{k \in [0,n]} (-1)^k r_k^B (n-k)!$, gdzie

$B =$ 

Ponumerujmy pola dozwolone powyższej szachownicy liczbami całkowitymi ze zbioru $[1, 2n-1]$ poczynając od lewego górnego rogu. Dla ustalonego $k \in [1, n]$ rozstawienia k wież na szachownicy B są parametryzowane za pomocą k-elementowych podzbiorów zbioru $[1, 2n-k]$. 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 $r_B = \sum_{k \in [0,n]} \binom{2n-k}{k} T^k$, więc $a_n = \sum_{k \in [0,n]} (-1)^k \binom{2n-k}{k} (n-k)!$

§4. Systemy reprezentantów i twierdzenie Halla

Definicja.

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

Uwaga.

Niech $(A_1, \dots, A_n)$ będzie ciągiem podzbiorów zbioru X oraz niech $B := ([1, n], X, F)$, gdzie $F := \{(i, a) \in [1, n] \times X \mid a \notin A_i\}$. Wtedy ciąg $(A_1, \dots, A_n)$ posiada system reprezentantów wtedy i tylko wtedy, gdy $\deg R_B = n$. Ponadto ilość systemów reprezentantów jest równa $[T^n] R_B$.

Definicja.

Mówimy, że ciąg $(A_1, \dots, A_n)$ podzbiorów zbioru X spełnia warunek Halla, jeśli $|\bigcup_{i \in I} A_i| \geq |I|$ dla każdego podzbioru $I \subset [1, n]$.

Twierdzenie 4.1 (Hall).

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

Dowód.

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

Przypuśćmy, że ciąg $(A_1', A_2, \dots, A_n)$ nie spełnia warunku Halla. Wtedy istnieje podzbiór $I \subset [2, n]$ taki, że $|B| \leq |I|$, gdzie $B := A_1' \cup \bigcup_{i \in I} A_i$. Aby pokazać, że ciąg $(A_1'', A_2, \dots, A_n)$ spełnia warunek Halla wystarczy pokazać, że $|A_1'' \cup \bigcup_{i \in J} A_i| > |J|$ dla dowolnego podzbioru $J \subset [2, n]$. Ustalmy podzbiór $J \subset [2, n]$ 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 $B \cap C \supset \bigcup_{i \in I \cap J} A_i$, 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 $d \in \mathbb{N}_+$ takie, że $|A_i| \geq d$ dla każdego $i \in [1, n]$, oraz $|\{i \in [1, n] \mid x \in A_i\}| \leq d$ dla każdego elementu $x \in X$, to ciąg $(A_1, \ldots, A_n)$ spełnia warunek Halla.

Dowód.

Ustalmy podzbiór $I \subset [1, n]$ oraz niech $B := \bigcup_{i \in I} A_i$. Niech $M := \{(i, x) \in I \times X \mid x \in A_i\}$. Wtedy $M \geq d|I|$, gdyż $|A_i| \geq d$ dla każdego $i \in I$. Zarazem z drugiego warunku wynika, że $M \leq |B|d$, co oznacza, że $|B| \geq |I|$ i kończy dowód.

Definicja.

Niech $m, n \in \mathbb{N}$. 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 $i_1, i_2 \in [1, m]$ 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

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

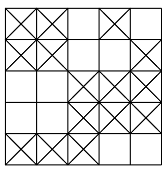
jest prostokątem łacińskim.

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 $i \in [1, m]$ i $j \in [1, n]$.

Przykład.

Ilość 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 $m, n \in \mathbb{N}$, $m \leq n$, to każdy prostokąt łaciński o m wierszach i n kolumnach można rozszerzyć do kwadratu łacińskiego.

Dowód.

Jeśli $m = n$, to nie ma co dowodzić, załóżmy zatem, że $m < n$. Niech A będzie prostokątem łacińskim m wierszach i n kolumnach. Wystarczy udowodnić, że prostokąt A można rozszerzyć do prostokątu łacińskiego o $m+1$ wierszach. Niech $A_j := [1, n] \setminus \{a_{i,j} \mid i \in [1, m]\}$ dla $j \in [1, n]$. Zauważmy, że $|A_j| = n - m$. Podobnie, $|\{j \in [1, n] \mid i \in A_j\|= n - m$ dla każdego $i \in [1, n]$. 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

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

jest prostokątem łacińskim, który jest rozszerzeniem prostokąta A.

Definicja.

Niech $n \in \mathbb{N}$. Macierz P o n wierszach i n kolumnach o współczynnikach w zbiorze $\mathbb{N}$ nazywamy macierzą permutacji, jeśli $\sum_{j \in [1,n]} p_{i,j} = 1$ dla każdego $i \in [1, n]$ oraz $\sum_{i \in [1,n]} p_{i,j} = 1$ dla każdego $j \in [1, n]$.

Twierdzenie 4.4 (Birkhoff).

Niech $n \in \mathbb{N}$, 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 $i \in [1, n]$ oraz $\sum_{i \in [1,n]} a_{i,j} = l$ dla każdego $j \in [1, n]$, to macierz A jest sumą l macierzy permutacji.

Dowód.

Dla każdego $i \in [1, n]$ niech $A_i := \{j \in [1, n] \mid a_{i,j} \neq 0\}$. Pokażemy, że ciąg $(A_1, \ldots, A_n)$ spełnia warunek Halla. Istotnie, jeśli $I \subset [1, n]$, to

$$|I|l = \sum_{i \in I} \sum_{j \in [1,n]} a_{i,j} = \sum_{i \in I} \sum_{j \in \bigcup_{p \in I} A_p} a_{i,j} = \sum_{j \in \bigcup_{p \in I} A_p} \sum_{i \in I} a_{i,j} \leq \Big|\bigcup_{p \in I} A_p\Big| l.$$

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

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

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

§5. Ważne ciągi liczbowe

Liczby Stirlinga

Definicja.

Niech $k \in \mathbb{N}$. Rozkładem zbioru X na k części nazywamy każdą rodzinę $\{A_1, \ldots, A_k\}$ niepustych podzbiorów zbioru X taką, że $X = \bigcup_{i \in [1,k]} A_i$ oraz $A_i \cap A_j = \varnothing$ dla wszystkich $i \neq j$.

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 $n \in \mathbb{N}_+$.

Przykład.

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

Przykład.

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

Przykład.

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

Przykład.

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

Przykład.

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

Twierdzenie 5.1.

Jeśli $n, k \in \mathbb{N}_+$, to $\left\{ {n \atop k} \right\} = k \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$.

Dowód.

Niech X będzie zbiorem wszystkich rozkładów zbioru $[1, n]$ na k części. Możemy założyć, że jeśli $\{A_1, \ldots, A_k\} \in X$, to $n \in A_k$. Wtedy $X = X_1 \cup X_2$, gdzie

$$X_1 := \{\{A_1, \ldots, A_k\} \in X \mid A_k = \{n\}\}$$

i

$$X_2 := \{\{A_1, \ldots, A_k\} \in X \mid A_k \neq \{n\}\}.$$

Zauważmy, że $X_1 \cap X_2 = \varnothing$. Ponadto $|X_1| = \left\{ {n-1 \atop k-1} \right\}$. Istotnie, jeśli Y_1 jest zbiorem wszystkich rozkładów zbioru $[1, n-1]$ na $k-1$ części, to funkcja $f : X_1 \rightarrow$

Y_2 dana wzorem $f(\{A_1, \dots, A_k\}) = \{A_1, \dots, A_{k-1}\}$ dla $\{A_1, \dots, A_k\} \in X_1$ jest poprawnie określona i jest bijekcją — funkcja odwrotna $g : Y_1 \to X_1$ dana jest wzorem $g(\{B_1, \dots, B_{k-1}\}) := \{B_1, \dots, B_{k-1}, \{n\}\}$ dla $\{B_1, \dots, B_{k-1}\} \in Y_1$.

Niech Y_2 będzie zbiorem wszystkich podziałów zbioru $[1, n-1]$ na k części oraz rozważmy funkcję $f : X_2 \to Y_2$ daną wzorem $f(\{A_1, \dots, A_k\}) := \{A_1, \dots, A_k \setminus \{n\}\}$ dla $\{A_1, \dots, A_k\} \in X_2$. Wtedy funkcja f jest poprawnie określona. Ponadto,

$$f^{-1}(\{B_1, \dots, B_k\}) = \{\{B_1 \cup \{n\}, B_2, \dots, B_k\}, \dots, \{B_1, \dots, B_{k-1}, B_k \cup \{n\}\}\}$$

dla każdego $\{B_1, \dots, B_k\} \in Y_2$. Stąd $|X_2| = k|Y_2| = k\left\{{n-1 \atop k}\right\}$, co kończy dowód.

OZNACZENIE.

Dla $k \in \mathbb{N}$ 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

$$\mathcal{S}_k = \frac{T^k}{(1-T) \cdots (1-kT)}.$$

DOWÓD.

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

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

skąd $\mathcal{S}_k = \frac{T}{1-kT} \mathcal{S}_{k-1}$, więc teza wynika przez prostą indukcję.

STWIERDZENIE 5.3.

Jeśli A i B są zbiorami, to liczba surjekcji $\varphi : A \to B$ jest równa $k!\left\{{n \atop k}\right\}$, 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. Wtedy $|Y| = \left\{{n \atop k}\right\}$. Rozważmy funkcję $f : X \to Y$ daną wzorem $f(\varphi) := \{\varphi^{-1}(1), \dots, \varphi^{-1}(k)\}$ dla $\varphi \in X$. Wtedy funkcja f jest poprawnie określona. Ponadto dla $\{A_1, \dots, A_k\} \in Y$ mamy $f^{-1}(A_1, \dots, A_k) = \{\varphi_\sigma \mid \sigma \in P_k\}$, gdzie $\varphi_\sigma(a) := \sigma(i)$ dla $a \in A_i$ i $\sigma \in P_k$. Stąd $|X| = |P_k||Y| = k!\left\{{n \atop k}\right\}$, co kończy dowód.

Wniosek 5.4.

Jeśli $n, k \in \mathbb{N}$, to

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

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 $X_i := \{\varphi \in X \mid |\varphi([1,n])| = i\}$ dla $i \in [0,k]$. Wtedy $|X_i| = \binom{k}{i} i! \left\{ {n \atop i} \right\}$ dla wszystkich $i \in [0,k]$ oraz $X_i \cap X_j = \varnothing$ dla wszystkich $i \neq j$, skąd wynika teza.

Wniosek 5.5.

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

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

Dowód.

Wystarczy zauważyć, że $\sum_{i \in [0,k]} i! \binom{k}{i} \left\{ {n \atop i} \right\} = \sum_{i \in [0,n]} i! \binom{k}{i} \left\{ {n \atop i} \right\}$ dla dowolnego $k \in \mathbb{N}$ (gdyż $\binom{k}{i} = 0$ dla $i > k$ oraz $\left\{ {n \atop i} \right\} = 0$ dla $i > n$) i skorzystać z poprzedniego wniosku.

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

Dowód.

Korzystając z Wniosku 5.4 otrzymujemy, że

$$\sum_{k \in \mathbb{N}} \frac{k^n}{k!} = \sum_{k \in \mathbb{N}} \sum_{i \in [0,k]} \frac{i!}{k!} \binom{k}{i} \left\{ {n \atop i} \right\} = \sum_{i \in \mathbb{N}} \sum_{\substack{k \in \mathbb{N} \\ k \geq i}} \frac{1}{(k-i)!} \left\{ {n \atop i} \right\}$$
$$= \sum_{i \in \mathbb{N}} \sum_{k \in \mathbb{N}} \frac{1}{k!} \left\{ {n \atop i} \right\} = eB_n,$$

co kończy dowód.

STWIERDZENIE 5.7.

Jeśli $n \in \mathbb{N}$, to

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

DOWÓD.

Niech X będzie zbiorem wszystkich rozkładów zbioru $[1, n+1]$. Możemy założyć, że jeśli $\{A_1, \dots, A_l\} \in X$, to $n+1 \in A_l$. Wtedy $X = \bigcup_{k\in[0,n]} X_k$, gdzie $X_k := \{\{A_1, \dots, A_l\} \mid |A_l| = k+1\}$ dla $k \in [0,n]$. Oczywiście $X_i \cap X_j = \varnothing$ dla wszystkich $i \neq j$. Ponadto $X_k = \binom{n}{k} B_{n-k}$ dla wszystkich $k \in [0,n]$, co kończy dowód.

STWIERDZENIE 5.8.

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

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

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

DOWÓD.

Udowodnimy indukcyjnie, że $b_{n,m} = \sum_{k\in[0,n]} \binom{n}{k} B_{m-k}$ dla wszystkich $m \in \mathbb{N}$ oraz $n \in [0,m]$. W szczególności wobec poprzedniego stwierdzenia $b_{n,n} = \sum_{k\in[0,n]} \binom{n}{k} B_{n-k} = B_{n+1}$ dla wszystkich $n \in \mathbb{N}$, 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 powyższych rachunków $b_{0,m} = b_{m-1,m-1} = B_m = \sum_{k\in[0,m]} \binom{m}{k} B_{m-k}$, załóżmy zatem, że $n \in [1,m]$. Wtedy z założenia indukcyjnego wynika, że

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

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 $B_5 = 52$.