
DOWODY KOMBINATORYCZNE**1. Oznaczenia**

Przypuśćmy, że dany jest zbiór skończony A . Wtedy

$$\begin{aligned}|A| &= \text{liczba elementów zbioru } A, \\ P(A) &= \{B : B \subseteq A\}, \\ P_k(A) &= \{B \in P(A) : |B| = k\}.\end{aligned}$$

W szczególności

$$\begin{aligned}P_0(A) &= \{\emptyset\}, \\ P_1(A) &= \{\{a\} : a \in A\}, \\ P_m(A) &= \{A\},\end{aligned}$$

gdzie $|A| = m$. Ponadto

$$\begin{aligned}[n] &= \{1, 2, \dots, n\}, \\ [0] &= \emptyset, \\ [1] &= \{1\}, \\ [2] &= \{1, 2\}, \\ P(n) &= P([n]) = P(\{1, 2, \dots, n\}), \\ P_k(n) &= P_k([n]) = P_k(\{1, 2, \dots, n\}), \\ P_k(0) &= P_k(\emptyset).\end{aligned}$$

Będą potrzebne dwie funkcje. Jeśli $1 \leq k \leq n$, to

$$(n)_k = n \cdot (n-1) \cdot \dots \cdot (n-k+1).$$

Dla $k > n$ przyjmujemy $(n)_k = 0$. Wreszcie

$$n! = (n)_n = 1 \cdot 2 \cdot \dots \cdot n$$

oraz $0! = 1$.

2. Reguła dodawania

Zauważmy bez dowodu, że jeśli A i B są zbiorami skończonymi oraz $A \cap B = \emptyset$, to

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

Ogólnie, jeśli dane są zbiory skończone $A_1, A_2, \dots, A_n$ oraz $A_i \cap A_j = \emptyset$ dla $i \neq j$, to

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

Stąd w szczególności mamy:

$$\begin{aligned}
 |A \cup B| &= |(A \setminus B) \cup (A \cap B) \cup (B \setminus A)| = \\
 &= |A \setminus B| + |A \cap B| + |B \setminus A| = \\
 &= |A \setminus B| + |A \cap B| + |B \setminus A| + |A \cap B| - |A \cap B| = \\
 &= |(A \setminus B) \cup (A \cap B)| + |(B \setminus A) \cup (A \cap B)| - |A \cap B| = \\
 &= |A| + |B| - |A \cap B|
 \end{aligned}$$

oraz

$$\begin{aligned}
 |A \cup B \cup C| &= |(A \cup B) \cup C| = \\
 &= |A \cup B| + |C| - |(A \cup B) \cap C| = \\
 &= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| = \\
 &= |A| + |B| + |C| - |A \cap B| - (|A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|) = \\
 &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.
 \end{aligned}$$

W następnym wykładzie zajmiemy się uogólnieniami tych wzorów.

Regułę dodawania możemy wysłowić w następujący sposób. Przypuśćmy, że możemy wykonać n czynności; pierwsza kończy się jednym z m_1 wyników, druga jednym z m_2 wyników i tak dalej, aż do ostatniej, kończącej się jednym z m_n wyników. Zakładamy przy tym, że wszystkie te wyniki są różne, tzn. żadne dwie z tych czynności nie mogą kończyć się tym samym wynikiem. Założmy następnie, że mamy wykonać jedną, dowolnie przez nas wybraną czynność. Możemy wtedy otrzymać jeden z $m_1 + m_2 + \dots + m_n$ wyników.

3. Reguła mnożenia

Zacniemy od następującej oczywistej równości

$$|A \times B| = |A| \cdot |B|.$$

Możemy ją wysłowić w następujący sposób. Przypuśćmy, że mamy do wykonania dwie czynności. Pierwsza kończy się jednym z m wyników, druga jednym z n wyników. Wykonanie obu, jedna po drugiej, zakończy się zatem jednym z $m \cdot n$ możliwych wyników. Przy tym sformułowaniu zakładamy, że niezależnie od wyniku pierwszej czynności, druga kończy się zawsze jednym z n **tych samych** wyników. Inaczej mówiąc, zbiór wyników drugiej czynności jest ustalony; nie zależy od tego, w jaki sposób zakończy się pierwsza czynność.

Zbiór wyników drugiej czynności może jednak zależeć od tego, jak zakończyła się pierwsza czynność. Popatrzmy na przykład. Z talii 52 kart wyciągamy kolejno dwie karty i układamy koło siebie (z zachowaniem kolejności). Pierwszą czynnością jest wyciągnięcie pierwszej karty. Może ona zakończyć się jednym z 52 wyników. Drugą czynnością jest wyciągnięcie drugiej karty. Widzimy, że zbiór możliwych wyników drugiej czynności zależy od tego, jakiej karty już nie ma w talii, czyli od wyniku pierwszej czynności.

Zauważmy jednak, że druga czynność, niezależnie od wyniku pierwszej, zakończy się jednym z 51 wyników, bo niezależnie, od tego, jaką kartę wyciągniemy, w talii pozostanie 51 kart.

Przypuśćmy zatem, że mamy do wykonania dwie czynności. Pierwsza kończy się jednym z m wyników: $x_1, x_2, \dots, x_m$. Dla każdego x_k zbiór A_k możliwych wyników drugiej czynności ma zawsze n elementów:

$$|A_1| = |A_2| = \dots = |A_m| = n.$$

Wykonujemy obie czynności po kolei. Wynikiem będzie para (x, y) , gdzie x jest wynikiem pierwszej czynności, a y wynikiem drugiej. Zbiór wyników ma zatem postać:

$$\{(x_k, y) : k = 1, 2, \dots, m, y \in A_k\}.$$

Ten zbiór możemy przedstawić w postaci sumy m zbiorów rozłącznych:

$$\begin{aligned} \{(x_k, y) : k = 1, 2, \dots, m, y \in A_k\} = \\ = \{(x_1, y) : y \in A_1\} \cup \{(x_2, y) : y \in A_2\} \cup \dots \cup \{(x_m, y) : y \in A_m\}. \end{aligned}$$

Każdy z m zbiorów po prawej stronie ma n elementów, a więc z reguły dodawania wynika, że

$$|\{(x_k, y) : k = 1, 2, \dots, m, y \in A_k\}| = m \cdot n.$$

Regułę mnożenia możemy zatem wysłowić w następujący sposób. Mamy do wykonania dwie czynności. Pierwsza kończy się jednym z m wyników. Druga, niezależnie od wyniku pierwszej, kończy się jednym z n wyników (przy czym zbiory wyników drugiej mogą być różne w zależności od wyniku pierwszej). Wykonanie obu czynności po kolei zakończy się wtedy jednym z $m \cdot n$ wyników.

Regułę mnożenia możemy łatwo uogólnić na większą liczbę czynności. Dokładne jej sformułowanie pozostawię jako ćwiczenie.

4. Zliczanie funkcji i podzbiorów

Niech $|A| = m$ i $|B| = n$. Wtedy z reguły mnożenia wynika natychmiast, że

$$|A^B| = m^n.$$

Wartość $f(b)$ dla każdego elementu zbioru B wybieramy bowiem na jeden z m sposobów; tych elementów zbioru B jest n , więc dokonujemy n wyborów.

Podobnie

$$|\{f \in A^B : f \text{ jest } 1-1\}| = (m)_n.$$

Znów wybieramy n wartości: pierwszą wartość $f(b)$ wybieramy na jeden z m sposobów, drugą na jeden z $m - 1$ sposobów i tak dalej.

Definiujemy **współczynnik dwumianowy** $\binom{m}{n}$ wzorem

$$\binom{m}{n} = |P_n(m)|.$$

5. Permutacje, kombinacje i wariacje

Niech $|A| = m$. Wtedy mamy następujące obiekty kombinatoryczne znane ze szkoły.

- 1) **Wariacjami n -elementowymi z powtórzeniami ze zbioru A** nazywamy ciągi $(a_1, \dots, a_n)$ o wyrazach ze zbioru A . Wówczas

$$|\{(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}| = |A^{[n]}| = m^n.$$

- 2) **Wariacjami n -elementowymi bez powtórzeń ze zbioru A** nazywamy ciągi różnowartościowe $(a_1, \dots, a_n)$ o wyrazach ze zbioru A . Wówczas

$$|\{(a_1, \dots, a_n) \in A^{[n]} : a_i \neq a_j \text{ dla } i \neq j\}| = (m)_n = \frac{m!}{(m-n)!}.$$

- 3) **Permutacjami zbioru A** nazywamy m -elementowe wariacje bez powtórzeń. Wówczas

$$|\{(a_1, \dots, a_m) \in A^{[m]} : a_i \neq a_j \text{ dla } i \neq j\}| = m!$$

- 4) **Kombinacjami n -elementowymi ze zbioru A** nazywamy n -elementowe podzbiory zbioru A . Wówczas

$$|P_n(A)| = \binom{m}{n}.$$

Zobaczmy teraz jeden ważny przykład występowania kombinacji. Niech będzie dany zbiór C składający się ze wszystkich ciągów długości m o dwóch wyrazach a i b , w których litera a występuje n razy, a litera b występuje $m - n$ razy. Otóż wtedy $|C| = \binom{m}{n}$. Każdy taki ciąg jest bowiem jednoznacznie wyznaczony przez wskazanie, które spośród m wyrazów są literami a ; pozostałe są równe b . Wskazać te n wyrazów możemy właśnie na $\binom{m}{n}$ sposobów. W szczególności istnieje $\binom{m+n}{m}$ ciągów, w których jest dokładnie m wyrazów równych a i n wyrazów równych b .

Oprócz powyższych obiektów znanych ze szkoły zdefiniujemy teraz **kombinacje z powtórzeniami**. Kombinacje wskazują, które elementy zbioru A zostały wybrane, bez uwzględnienia kolejności, w jakiej te elementy były wybierane. Kombinacje z powtórzeniami wskazują ponadto, że elementy zbioru A mogły być wybrane wielokrotnie, przy czym nadal nie wskazujemy kolejności wybierania. Pokażemy teraz dwa sposoby definiowania takich kombinacji z powtórzeniami. Możemy przedstawiać je jako funkcje $c : A \rightarrow \mathbb{N}$, gdzie liczba $c(a)$ wskazuje, ile razy element a został wybrany. Zatem **kombinacjami n -elementowymi z powtórzeniami ze zbioru A** nazywamy funkcje $c : A \rightarrow \mathbb{N}$ takie, że

$$\sum_{a \in A} c(a) = n.$$

Popatrzmy na przykład. Niech $A = \{p, q, r, s, t\}$ będzie zbiorem pięcioelementowym. Funkcja $c : A \rightarrow \mathbb{N}$ określona w następujący sposób

$$c(p) = 3, \quad c(q) = 2, \quad c(r) = 1, \quad c(s) = 1, \quad c(t) = 0$$

jest kombinacją, w której element p został wybrany 3 razy, element q został wybrany 2 razy, elementy r i s po jednym razie i wreszcie element t ani razu. Tę kombinację z powtórzeniami moglibyśmy zatem zapisać w postaci ciągu $pppqqrs$. Taki właśnie sposób zapisu kombinacji z powtórzeniami będzie podstawą innej definicji. Ten drugi sposób definiowania kombinacji z powtórzeniami wymaga uporządkowania najpierw zbioru A . Przyjmijmy, że

$$A = \{a_1, a_2, \dots, a_m\}.$$

Kombinacją n -elementową z powtórzeniami ze zbioru A nazwiemy teraz dowolny ciąg $(x_1, x_2, \dots, x_n)$ elementów zbioru A , w którym dla dowolnych $i, j = 1, 2, \dots, m$, jeśli $i < j$, to wszystkie wyrazy równe a_i występują przez wszystkie wyrazami równymi a_j . Inaczej mówiąc, w takim ciągu najpierw występuje blok wartości a_1 , potem blok wartości a_2 i tak dalej aż do ostatniego bloku wartości a_m ; może się zdarzyć, że niektóre z tych bloków będą puste. W naszym przykładzie zbioru $A = \{p, q, r, s, t\}$ takie ciągi będą składać się z bloku liter p na początku, potem będą występować kolejno bloki liter q , r i s i wreszcie na końcu znajdzie się blok liter t . Przypominamy, że niektóre z tych bloków mogą być puste. Widzieliśmy wyżej przykład takiego ciągu: $pppqqrs$. W tym ciągu mieliśmy najpierw blok trzech liter p , następnie blok dwóch liter q , po nim dwa bloki jednoliterowe liter r i s i wreszcie na końcu pusty blok liter t .

Zajmiemy się teraz zliczaniem kombinacji z powtórzeniami. Zaczniemy od przykładu. Niech $|A| = 5$ i $n = 7$. Zliczamy zatem kombinacje siedmioelementowe z powtórzeniami z pięcioelementowego zbioru A . Uporządkujmy elementy zbioru A :

$$A = \{p, q, r, s, t\}.$$

Weźmy znany nam przykład kombinacji z powtórzeniami zapisanej w postaci ciągu: $pppqqrs$. Oddzielmy pionowymi kreskami bloki liter:

$$p \ p \ p \mid q \ q \mid r \mid s \mid$$

Zwracamy uwagę na kreskę na końcu. Oddziela ona jednoliterowy blok s od pustego bloku liter t . Teraz możemy zauważyć, że nie jest już potrzebne pisanie liter. Wiemy bowiem, że w pierwszym bloku muszą wystąpić litery p , w drugim litery q i tak dalej. Istotne jest tylko zaznaczenie, ile liter jest w każdym bloku. Rysujemy zatem kropki w miejscu liter. Narysujemy więc 7 kropek, oznaczających elementy wybrane podzielnymi czterema pionowymi kreskami na pięć części. Wskażemy tym samym, które kropki oznaczają kolejne elementy zbioru A . W naszym przykładzie otrzymamy następujący ciąg kropek i kresek

$$\bullet \bullet \bullet \mid \bullet \bullet \mid \bullet \mid \bullet \mid$$

oznaczający, że element p został wybrany 3 razy (przed pierwszą kreską są 3 kropki), element q został wybrany 2 razy (między pierwszą i drugą kreską są 2 kropki), elementy r i s zostały wybrane po jednym razie (między kolejnymi kreskami jest jedna kropka), wreszcie element t nie został wybrany ani razu (za ostatnią, czwartą kreską nie ma ani jednej kropki). Podobnie zapis

$$\bullet \bullet \mid \mid \mid \bullet \bullet \bullet \bullet \mid \bullet$$

oznacza, że element p został wybrany 2 razy, elementy q i r ani razu, element s został wybrany 4 razy i element t jeden raz. Każdy ciąg siedmiu kropek i czterech kresek odpowiada dokładnie jednej kombinacji z powtórzeniami. Mamy zatem łącznie 11 symboli: 7 kropek i 4 kreski. Z powyższych rozważań dotyczących kombinacji wynika, że istnieje $\binom{11}{4}$ różnych ciągów złożonych z 7 kropek i 4 kresek.

W ogólności mamy n kropek (wybieramy n elementów) i $m - 1$ kresek (dzielą one kropki na m bloków odpowiadających m elementom zbioru A). Mamy zatem $\binom{m+n-1}{m-1}$ ciągów n kropek i $m - 1$ kresek i tyle jest n -elementowych kombinacji z powtórzeniami z m -elementowego zbioru A .

Zwróćmy uwagę na dwie rzeczy. Po pierwsze, sposób kodowania kombinacji z powtórzeniami za pomocą ciągu kropek i kresek zależy od uporządkowania zbioru A . Przy innym uporządkowaniu ten sam ciąg będzie na ogół oznaczał inną kombinację. Po drugie, jeśli naszym zbiorem A jest zbiór $[m]$ z naturalnym uporządkowaniem, to kombinację z powtórzeniami możemy przedstawić jako ciąg liczb od 1 do m , w którym najpierw występują wyrazy równe 1, potem wyrazy równe 2 i tak dalej. Inaczej mówiąc, taką kombinację możemy zapisać w postaci ciągu niemalejącego długości n o wyrazach ze zbioru $[m]$. Stąd wynika, że istnieje $\binom{m+n-1}{m-1}$ niemalejących ciągów długości n o wyrazach ze zbioru $[m]$. Z tego wniosku kilkakrotnie dalej skorzystamy.

6. Podstawowe własności współczynników dwumianowych

Przypominamy, że

$$\binom{m}{n} = |P_n(A)|,$$

gdzie $|A| = m$. Oczywiście dla $n > m$ mamy $P_n(A) = \emptyset$, czyli $\binom{m}{n} = 0$ dla $n > m$. Przyjmujemy ponadto, że $\binom{m}{n} = 0$ dla $n < 0$.

Zauważmy następnie, że

$$P_0(A) = \{\emptyset\} \quad \text{oraz} \quad P_m(A) = \{A\}.$$

Zatem

$$\binom{m}{0} = \binom{m}{m} = 1. \quad (1.1)$$

Niech teraz $0 < n \leq m$. Udowodnimy, że

$$n \cdot \binom{m}{n} = m \cdot \binom{m-1}{n-1}.$$

Niech $|A| = m$. Rozpatrujemy zbiór

$$B = \{(a, N) : a \in N \in P_n(A)\}.$$

Zliczamy dwoma sposobami elementy zbioru B . Po pierwsze

$$B = \bigcup_{N \in P_n(A)} \{(a, N) : a \in N\},$$

przy czym sumowane zbiory są rozłączne dla różnych N . Z reguły dodawania mamy zatem

$$|B| = \sum_{N \in P_n(A)} |\{(a, N) : a \in N\}| = \sum_{N \in P_n(A)} n = n \cdot \binom{m}{n}.$$

Z drugiej strony

$$B = \bigcup_{a \in A} \{(a, N) : a \in N \in P_n(A)\},$$

przy czym znów sumowane zbiory są rozłączne (tym razem dla różnych a). Zatem

$$\begin{aligned} |B| &= \sum_{a \in A} |\{(a, N) : a \in N \in P_n(A)\}| = \\ &= \sum_{a \in A} |\{(a, \{a\} \cup K) : K \in P_{n-1}(A \setminus \{a\})\}| = \\ &= \sum_{a \in A} |\{(a, K) : K \in P_{n-1}(A \setminus \{a\})\}| = \\ &= \sum_{a \in A} \binom{m-1}{n-1} = \\ &= m \cdot \binom{m-1}{n-1}. \end{aligned}$$

Ponieważ liczba elementów zbioru skończonego nie zależy od sposobu zliczania tych elementów, więc otrzymujemy równość

$$n \cdot \binom{m}{n} = m \cdot \binom{m-1}{n-1}, \quad (1.2)$$

z której otrzymujemy

$$\binom{m}{n} = \frac{m}{n} \cdot \binom{m-1}{n-1}. \quad (1.3)$$

Zazwyczaj nie przedstawiamy dowodów tożsamości kombinatorycznych w sposób tak sformalizowany. Przedstawiamy natomiast „historyjkę”, którą można łatwo sformalizować i którą traktujemy jako dowód. Jest to tzw. **dowód kombinatoryczny**. A oto przykład historyjki będącej dowodem tożsamości (1.2).

Przypuśćmy, że w naszej firmie pracuje m osób. Chcemy wybrać spośród nich n osób ($n > 0$), które otrzymają nagrodę oraz chcemy jedną z nagrodzonych osób awansować. Na ile sposobów możemy tego dokonać?

Po pierwsze wybieramy osoby do nagrody. Możemy to zrobić na $\binom{m}{n}$ sposobów. Następnie wśród wybranych osób wskazujemy osobę przeznaczoną do awansu. Możemy to zrobić na n sposobów. Z reguły mnożenia wynika, że istnieje $n \cdot \binom{m}{n}$ sposobów łącznego wyboru.

Możemy także wybrać najpierw osobę do awansu: mamy m możliwości. Tę osobę także nagradzamy, mamy więc już jedną osobę nagrodzoną. Spośród pozostałych $m - 1$ osób

dobieramy jeszcze $n-1$ osób do nagrody; możemy to zrobić na $\binom{m-1}{n-1}$ sposobów. Z reguły mnożenia wynika, że mamy łącznie $m \cdot \binom{m-1}{n-1}$ sposobów wyboru.

Wreszcie, tak jak poprzednio, stwierdzamy, że liczba sposobów wyboru nie zależy od metody zliczania. Otrzymujemy zatem równość (1.2):

$$n \cdot \binom{m}{n} = m \cdot \binom{m-1}{n-1}, \quad (1.2)$$

co kończy dowód.

Tożsamość (1.3) pozwala obliczać współczynniki dwumianowe. Popatrzmy na przykład:

$$\begin{aligned} \binom{7}{4} &= \frac{7}{4} \cdot \binom{6}{3} = \frac{7}{4} \cdot \frac{6}{3} \cdot \binom{5}{2} = \frac{7}{4} \cdot \frac{6}{3} \cdot \frac{5}{2} \cdot \binom{4}{1} = \frac{7}{4} \cdot \frac{6}{3} \cdot \frac{5}{2} \cdot \frac{4}{1} \cdot \binom{3}{0} = \\ &= \frac{7}{4} \cdot \frac{6}{3} \cdot \frac{5}{2} \cdot \frac{4}{1} \cdot 1 = \frac{7 \cdot 6 \cdot 5 \cdot 4}{4 \cdot 3 \cdot 2 \cdot 1} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2} = 7 \cdot 5 = 35. \end{aligned}$$

Przykład ten uogólniamy w następnym twierdzeniu.

Twierdzenie 1.1. Jeśli $0 \leq n \leq m$, to

$$\binom{m}{n} = \frac{m!}{n! \cdot (m-n)!}. \quad (1.4)$$

Dowód. Stosujemy indukcję względem m . Zauważmy najpierw, że dla dowolnego n i dla $n = 0$ mamy

$$\binom{m}{0} = 1 \quad \text{oraz} \quad \frac{m!}{0! \cdot (m-0)!} = \frac{m!}{m!} = 1,$$

czyli

$$\binom{m}{0} = \frac{m!}{0! \cdot (m-0)!}.$$

W szczególności teza twierdzenia jest prawdziwa dla $m = 0$.

Zakładamy następnie, że dla pewnego m i dowolnego n takiego, że $0 \leq n \leq m$ prawdziwa jest równość

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

Niech teraz $0 \leq n \leq m+1$. Mamy dowieść, że

$$\binom{m+1}{n} = \frac{(m+1)!}{n! \cdot (m+1-n)!}.$$

Wiemy już, że ta równość jest prawdziwa dla $n = 0$. Niech zatem $n > 0$. Z równości (1.3) otrzymujemy

$$\binom{m+1}{n} = \frac{m+1}{n} \cdot \binom{m}{n-1}.$$

Ponieważ $0 \leq n-1 \leq m$, więc z założenia indukcyjnego otrzymujemy

$$\binom{m}{n-1} = \frac{m!}{(n-1)! \cdot (m - (n-1))} = \frac{m!}{(n-1)! \cdot (m+1-n)!}.$$

Stąd dostajemy

$$\begin{aligned} \binom{m+1}{n} &= \frac{m+1}{n} \cdot \frac{m!}{(n-1)! \cdot (m+1-n)!} = \\ &= \frac{m! \cdot (m+1)}{(n-1)! \cdot n \cdot (m+1-n)!} = \\ &= \frac{(m+1)!}{n! \cdot (m+1-n)!}, \end{aligned}$$

c. b. d. o.

Twierdzenie 1.1 można udowodnić w inny sposób. Zastanówmy się, jak można utworzyć dowolną permutację ustalonego m -elementowego zbioru A . Wykonujemy trzy czynności: najpierw wybieramy n -elementowy podzbiór B zbioru A , następnie porządkujemy elementy zbioru A , wreszcie porządkujemy elementy zbioru $A \setminus B$, ustawiając je za elementami zbioru B . Nietrudno zauważyć, że w ten sposób każdą permutację zbioru A otrzymamy dokładnie jeden raz. Popatrzmy teraz, ile możliwych wyników da każda z tych trzech czynności. Pierwsza ma $\binom{m}{n}$ możliwych wyników, druga $n!$, trzecia $(m-n)!$ wyników. Z reguły mnożenia otrzymujemy zatem

$$\binom{m}{n} \cdot n! \cdot (m-n)! = m!,$$

czyli

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

Pokażemy teraz dowód następującej tożsamości, podobnej do tożsamości (1.2):

$$n \cdot \binom{m}{n} = (m-n+1) \cdot \binom{m}{n-1}. \quad (1.5)$$

Niech $|A| = m$. Znów dwoma sposobami zliczamy elementy zbioru

$$B = \bigcup_{N \in P_n(A)} \{(a, N) : a \in N\}.$$

Tak jak poprzednio, zbiór $N \in P_n(A)$ możemy wybrać na $\binom{m}{n}$ sposobów, a jego element a możemy wybrać na n sposobów. To daje łącznie $n \cdot \binom{m}{n}$ par (a, N) . Możemy postąpić inaczej. Najpierw wybieramy zbiór $N' \in P_{n-1}(A)$. Możemy to zrobić na $\binom{m}{n-1}$ sposobów. Następnie wybieramy $a \in A \setminus N'$ i przyjmujemy $N = N' \cup \{a\}$. Element a możemy

wybrać na $m - n + 1$ sposobów, co daje łącznie $(m - n + 1) \cdot \binom{m}{n-1}$ par (a, N) . W ten sposób równość (1.5) została udowodniona.

Paragraf ten zakończymy dowodem tożsamości będącej naturalnym uogólnieniem tożsamości (1.2). Udowodnimy, że

$$\binom{m}{n} \binom{n}{k} = \binom{m}{k} \binom{m-k}{n-k}. \quad (1.6)$$

Niech M będzie zbiorem m -elementowym. Będziemy zliczać na dwa sposoby elementy zbioru

$$A = \{(N, K) : K \subseteq N \subseteq M, |K| = k, |N| = n\}.$$

Zbiór N możemy wybrać na $\binom{m}{n}$ sposobów. Następnie jego podzbiór k -elementowy K możemy wybrać na $\binom{n}{k}$ sposobów. To daje łączną liczbę $\binom{m}{n} \binom{n}{k}$ sposobów wyboru.

Możemy jednak wybierać te zbiory w innej kolejności. Najpierw wybieramy zbiór K ; mamy $\binom{m}{k}$ sposobów wyboru. Następnie spośród pozostałych $m - k$ elementów zbioru M wybieramy $n - k$ elementów. Łącznie z już wybranymi elementami utworzą one zbiór N . Te $n - k$ elementów możemy wybrać na $\binom{m-k}{n-k}$ sposobów. Łącznie daje to $\binom{m}{k} \binom{m-k}{n-k}$ sposobów wyboru elementów zbioru A . Znowu liczba elementów zbioru A nie zależy od kolejności zliczania, co dowodzi równości (1.6).

Do tego dowodu można ułożyć historyjkę podobną do historyjki w dowodzie tożsamości (1.2). Przypuśćmy, że w naszej firmie nadal pracuje m osób. Chcemy nagrodzić n z nich oraz k nagrodzonych osób awansować. Na ile sposobów możemy to zrobić? Zliczamy te sposoby wyboru dwiema metodami. Najpierw wybieramy osoby do nagrody: na $\binom{m}{n}$ sposobów, następnie spośród nich wybieramy k osób do awansu: na $\binom{n}{k}$ sposobów. To daje lewą stronę równości (1.6). Możemy też najpierw wybrać osoby do awansu (i jednocześnie nagrody): na $\binom{m}{k}$ sposobów, a następnie dobrać brakujące $n - k$ osób do nagrody: na $\binom{m-k}{n-k}$ sposobów. To daje prawą stronę. Zauważmy także, że dla $k = 1$ otrzymujemy równość (1.2).

7. Trójkąt Pascala

Ustawmy współczynniki dwumianowe w tablicy:

$$\begin{array}{cccccccc} & & & & \binom{0}{0} & & & \\ & & & & \binom{1}{0} & \binom{1}{1} & & \\ & & & \binom{2}{0} & \binom{2}{1} & \binom{2}{2} & & \\ & & \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} & & \\ \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} & & & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \end{array}$$

Tablicę tę nazywamy **trójkątem Pascala**. Widzimy zasadę umieszczania współczynników dwumianowych w trójkącie Pascala. Liczba m we współczynniku $\binom{m}{n}$ oznacza numer wiersza, przy czym wiersze numerujemy od zera. Liczba n oznacza kolejny numer współczynnika w wierszu, przy czym znowu numerujemy miejsca od zera. Zauważmy

następnie, że w wierszu o numerze m mamy $m + 1$ współczynników numerowanych liczbami n od zera do m . Możemy sobie oczywiście wyobrazić, że wszystkie wiersze są nieskończone i ich wyrazy są numerowane liczbami całkowitymi. Ponieważ $\binom{m}{n} = 0$ dla $n < 0$ i $n > m$, więc wszystkie współczynniki dwumianowe niewidoczne w trójkącie Pascala są równe zero. Inaczej mówiąc, w trójkącie Pascala pokazujemy tylko niezerowe współczynniki dwumianowe.

Pierwsze wiersze trójkąta Pascala wyglądają następująco:

$$\begin{array}{cccccccc}
 & & & & 1 & & & \\
 & & & & & 1 & & 1 \\
 & & & 1 & & 2 & & 1 \\
 & & 1 & & 3 & & 3 & & 1 \\
 & 1 & & 4 & & 6 & & 4 & & 1 \\
 \dots & & \dots & & \dots & & \dots & & \dots & \dots
 \end{array}$$

Zbadamy teraz własności trójkąta Pascala.

Zauważmy, że każdy wiersz trójkąta Pascala zaczyna się i kończy jedynką. Wynika to z równości (1.1):

$$\binom{m}{0} = \binom{m}{m} = 1.$$

Następnie zauważmy, że każdy wiersz jest symetryczny:

$$\binom{m}{n} = \binom{m}{m-n}. \quad (1.7)$$

Wynika to stąd, że jeśli $|A| = m$, to zbiory $P_n(A)$ i $P_{m-n}(A)$ są równoliczne, funkcja $f : P_n(A) \rightarrow P_{m-n}(A)$ określona wzorem $f(B) = A \setminus B$ ustala tę równoliczność. Inaczej mówiąc, wybór n elementów ze zbioru A jest tym samym, co odrzucenie pozostałych $m - n$ elementów tego zbioru A .

Wreszcie najważniejsza własność trójkąta Pascala. Każdy współczynnik dwumianowy $\binom{m}{n}$, gdzie $0 < n < m$, jest sumą dwóch współczynników stojących bezpośrednio nad nim. Tę zależność można zapisać wzorem

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}. \quad (1.8)$$

Podamy teraz trzy dowody tego wzoru.

Dowód 1. Korzystamy z równości (1.5) (podstawiając $m - 1$ w miejsce m). Mamy zatem

$$n \cdot \binom{m-1}{n} = (m-n) \cdot \binom{m-1}{n-1}.$$

Teraz, korzystając również z równości (1.3), dostajemy

$$\begin{aligned}
 \binom{m-1}{n-1} + \binom{m-1}{n} &= \binom{m-1}{n-1} + \frac{m-n}{n} \cdot \binom{m-1}{n-1} = \left(1 + \frac{m-n}{n}\right) \cdot \binom{m-1}{n-1} = \\
 &= \frac{m}{n} \cdot \binom{m-1}{n-1} = \binom{m}{n}.
 \end{aligned}$$

Dowód 2. Korzystamy ze wzoru (1.4). Mamy zatem

$$\begin{aligned}
 \binom{m-1}{n-1} + \binom{m-1}{n} &= \frac{(m-1)!}{(n-1)! \cdot (m-n)!} + \frac{(m-1)!}{n! \cdot (m-n-1)!} = \\
 &= \frac{(m-1)!}{(n-1)! \cdot (m-n-1)! \cdot (m-n)} + \frac{(m-1)!}{(n-1)! \cdot n \cdot (m-n-1)!} = \\
 &= \frac{(m-1)!}{(n-1)! \cdot (m-n-1)!} \cdot \left(\frac{1}{m-n} + \frac{1}{n} \right) = \\
 &= \frac{(m-1)!}{(n-1)! \cdot (m-n-1)!} \cdot \frac{m}{(m-n)n} = \\
 &= \frac{(m-1)! \cdot m}{(n-1)! \cdot n \cdot (m-n-1)! \cdot (m-n)} = \\
 &= \frac{m!}{n! \cdot (m-n)!} = \binom{m}{n}.
 \end{aligned}$$

Dowód 3. Podamy teraz dowód kombinatoryczny. W naszej firmie, razem z dyrektorem, pracuje m osób. Chcemy, by na konferencję pojechało m osób. Na ile sposobów możemy je wybrać?

Mamy dwa przypadki. W pierwszym przypadku zakładamy, że dyrektor jedzie na konferencję. Wtedy z pozostałych $m-1$ osób musimy wybrać $n-1$ osób. W drugim przypadku zakładamy, że dyrektor nie jedzie na konferencję. Wtedy z pozostałych $m-1$ osób musimy wybrać n osób jadących na konferencję. Z reguły dodawania wynika teraz wzór (1.8).

To rozumowanie można łatwo sformalizować. Mianowicie zauważamy, że

$$P_n(m) = P_n(m-1) \cup \{A \cup \{m\} : A \in P_{n-1}(m-1)\},$$

przy czym zbiory po prawej stronie są rozłączne oraz oczywiście

$$|P_n(m-1)| = \binom{m}{n} \quad \text{oraz} \quad |\{A \cup \{m\} : A \in P_{n-1}(m-1)\}| = \binom{m-1}{n-1}.$$

Dopiszmy do trójkąta Pascala współczynniki $\binom{m}{n}$ dla $n < 0$ i $n > m$:

$$\begin{array}{cccccccccccc}
 \dots & & \binom{0}{-2} & & \binom{0}{-1} & & \binom{0}{0} & & \binom{0}{1} & & \binom{0}{2} & & \dots \\
 & \binom{1}{-2} & & \binom{1}{-1} & & \binom{1}{0} & & \binom{1}{1} & & \binom{1}{2} & & \binom{1}{3} & \\
 \dots & & \binom{2}{-1} & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \binom{2}{3} & & \dots \\
 & \binom{3}{-1} & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \binom{3}{4} & \\
 \dots & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \dots \\
 & \dots & & \dots & & \dots & & \dots & & \dots & & \dots &
 \end{array}$$

Zauważmy, że w pierwszym wierszu występują same zera z wyjątkiem jednego miejsca:

$$\binom{0}{0} = 1.$$

We wszystkich następnych wierszach każdy współczynnik powstaje z położonych nad nim zgodnie ze wzorem (1.8). Dlatego odtąd we wzorze (1.8) nie będziemy przyjmować żadnych założeń o m i n , poza oczywistym założeniem, że $m - 1 \geq 0$, czyli $m \geq 1$.

Jeszcze jedną ważną własność trójkąta Pascala otrzymujemy z równości (1.5). Mianowicie z równości

$$n \cdot \binom{m}{n} = (m - n + 1) \cdot \binom{m}{n-1} \quad (1.5)$$

wynika, że

$$\binom{m}{n} = \frac{m - n + 1}{n} \cdot \binom{m}{n-1}.$$

Przypuśćmy teraz, że m jest liczbą parzystą: $m = 2p$. Niech teraz $n \leq p$. Wówczas

$$\frac{m - n + 1}{n} = \frac{m + 1}{n} - 1 = \frac{2p + 1}{n} - 1 \geq \frac{2n + 1}{n} - 1 > \frac{2n}{n} - 1 = 1,$$

skąd wynika, że

$$\binom{m}{n} > \binom{m}{n-1}.$$

Niech teraz $n > p$, czyli $n - 1 \geq p$. Wówczas

$$\frac{m - n + 1}{n} = \frac{m + 1}{n} - 1 = \frac{2p + 1}{n} - 1 \leq \frac{2(n-1) + 1}{n} - 1 = \frac{2n - 1}{n} - 1 < \frac{2n}{n} - 1 = 1,$$

skąd wynika, że

$$\binom{m}{n} < \binom{m}{n-1}.$$

Podsumowując, jeśli $m = 2p$, to

$$\binom{m}{0} = \binom{m}{m} < \binom{m}{1} = \binom{m}{m-1} < \dots < \binom{m}{p-1} = \binom{m}{p+1} < \binom{m}{p}.$$

Przypuśćmy teraz, że m jest liczbą nieparzystą: $m = 2p + 1$. Niech najpierw $n \leq p$. Wówczas

$$\frac{m - n + 1}{n} = \frac{m + 1}{n} - 1 = \frac{2p + 2}{n} - 1 \geq \frac{2n + 2}{n} - 1 > \frac{2n}{n} - 1 = 1,$$

skąd wynika, że

$$\frac{m}{n} > \frac{m}{n-1}.$$

Niech następnie $n = p + 1$. Wtedy

$$\frac{m - n + 1}{n} = \frac{2p + 1 - p - 1 + 1}{p + 1} = \frac{p + 1}{p + 1} = 1,$$

skąd wynika, że

$$\binom{m}{p+1} = \binom{m}{p}.$$

Wreszcie niech $n > p + 1$, czyli $p < n - 1$. Wówczas

$$\frac{m-n+1}{n} = \frac{m+1}{n} - 1 = \frac{2p+2}{n} - 1 < \frac{2(n-1)+2}{n} - 1 = \frac{2n}{n} - 1 = 1,$$

skąd wynika, że

$$\binom{m}{n} < \binom{m}{n-1}.$$

Podsumowując, jeśli $m = 2p + 1$, to

$$\binom{m}{0} = \binom{m}{m} < \binom{m}{1} = \binom{m}{m-1} < \dots < \binom{m}{p-1} = \binom{m}{p+2} < \binom{m}{p} = \binom{m}{p+1}.$$

Paragraf ten zakończymy wzorem na sumę współczynników dwumianowych jednego wiersza trójkąta Pascala:

$$\sum_{n=0}^m \binom{m}{n} = 2^m. \quad (1.9)$$

Dowód. Zauważmy, że, jeśli $|A| = m$, to

$$P(A) = P_0(A) \cup P_1(A) \cup \dots \cup P_m(A),$$

przy czym zbiory po prawej stronie są rozłączne oraz

$$P_n(A) = \binom{m}{n}$$

dla $n = 0, 1, \dots, m$. Równość (1.9) wynika teraz z reguły dodawania.

8. Wzór dwumianowy Newtona

W tym paragrafie podamy dwa dowody wzoru znanego (przynajmniej częściowo) ze szkoły. Dla dowolnych liczb rzeczywistych a i b i dowolnej liczby naturalnej $n \geq 1$ zachodzi równość:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k. \quad (1.10)$$

Wzór (1.10) nazywamy zazwyczaj **wzorem dwumianowym** Newtona.

Dowód 1. Stosujemy indukcję ze względu na n . Dla $n = 1$ mamy

$$P = \sum_{k=0}^1 \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b = (a+b)^1 = L.$$

Przypuśćmy następnie, że dla pewnej liczby naturalnej n równość (1.10) jest prawdziwa:

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

Mamy udowodnić, że

$$(a + b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.$$

Skorzystamy w tym celu z równości (1.8):

$$\begin{aligned} (a + b)^{n+1} &= (a + b)^n \cdot (a + b) = \\ &= \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) \cdot (a + b) = \\ &= a \cdot \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k + b \cdot \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = \\ &= \sum_{k=0}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^n \binom{n}{k} a^{n-k} b^{k+1} = \\ &= \sum_{k=0}^n \binom{n}{k} a^{n+1-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{n-k+1} b^k = \\ &= \sum_{k=0}^{n+1} \binom{n}{k} a^{n+1-k} b^k + \sum_{k=0}^{n+1} \binom{n}{k-1} a^{n+1-k} b^k = \\ &= \sum_{k=0}^n \left(\binom{n}{k} + \binom{n}{k-1} \right) a^{n-k} b^k = \\ &= \sum_{k=0}^n \binom{n+1}{k} a^{n-k} b^k, \end{aligned}$$

co kończy dowód.

Dowód 2. Przyjrzyjmy się lewej stronie:

$$(a + b)^n = \underbrace{(a + b) \cdot \dots \cdot (a + b)}_{n \text{ czynników}}.$$

Po wymnożeniu czynników w n nawiasach otrzymamy sumę iloczynów: dla każdego wyboru a lub b z kolejnego czynnika otrzymamy jeden składnik sumy. Mamy zatem łącznie 2^n składników; każdy z nich jest postaci $a^{n-k} b^k$ dla pewnego k . Składnik $a^{n-k} b^k$ powstaje w wyniku wyboru b z k czynników $a + b$; z pozostałych $n - k$ czynników wybieramy a . Ponieważ mamy $\binom{n}{k}$ możliwości k wyborów b z n czynników $a + b$, więc

składnik $a^{n-k}b^k$ pojawi się $\binom{n}{k}$ razy w naszej sumie. Zatem po uproszczeniu jednomian $a^{n-k}b^k$ wystąpi ze współczynnikiem $\binom{n}{k}$. Ponieważ k jest oczywiście jedną z liczb od 1 do n , więc ostatecznie otrzymujemy sumę występującą po prawej stronie wzoru (1.10), c. b. d. o.

9. Cztery dowody jednej tożsamości

W tym paragrafie udowodnimy następującą tożsamość dla $n \geq 1$:

$$\sum_{k=0}^n k \cdot \binom{n}{k} = n \cdot 2^{n-1}. \quad (1.11)$$

Podamy cztery dowody tej tożsamości.

Dowód 1. Skorzystamy najpierw ze wzoru (1.2). Wiemy, że:

$$\sum_{k=0}^n k \cdot \binom{n}{k} = \sum_{k=1}^n k \cdot \binom{n}{k} = \sum_{k=1}^n n \cdot \binom{n-1}{k-1} = n \cdot \sum_{k=1}^n \binom{n-1}{k-1} = n \cdot \sum_{k=0}^{n-1} \binom{n-1}{k}.$$

Teraz wystarczy skorzystać z równości (1.9):

$$\sum_{k=0}^{n-1} \binom{n-1}{k} = 2^{n-1},$$

skąd wynika równość (1.11).

Dowód 2. Prowadzimy dowód przez indukcję ze względu na n . Niech najpierw $n = 1$. Mamy wtedy

$$\sum_{k=0}^1 k \cdot \binom{1}{k} = 0 \cdot \binom{1}{0} + 1 \cdot \binom{1}{1} = 1$$

oraz

$$1 \cdot 2^{1-1} = 1,$$

co dowodzi, że wzór (1.11) jest prawdziwy dla $n = 1$.

Założmy teraz, że równość (1.11) jest prawdziwa dla pewnej liczby n . Wykażemy, że jest ona też prawdziwa dla liczby $n + 1$. Mamy zatem udowodnić, że

$$\sum_{k=0}^{n+1} k \cdot \binom{n+1}{k} = (n+1) \cdot 2^n.$$

W dowodzie skorzystamy ze wzoru (1.8):

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

A oto obliczenia:

$$\begin{aligned}
 \sum_{k=0}^{n+1} k \cdot \binom{n+1}{k} &= \sum_{k=1}^{n+1} k \cdot \binom{n+1}{k} = \sum_{k=1}^n k \cdot \binom{n+1}{k} + n + 1 = \\
 &= \sum_{k=1}^n k \cdot \binom{n}{k} + \sum_{k=1}^n k \cdot \binom{n}{k-1} + n + 1 = \\
 &= n \cdot 2^{n-1} + \sum_{k=0}^{n-1} (k+1) \cdot \binom{n}{k} + n + 1 = \\
 &= \sum_{k=0}^{n-1} k \cdot \binom{n}{k} + \sum_{k=0}^{n-1} \binom{n}{k} + n \cdot 2^{n-1} + n + 1 = \\
 &= n \cdot 2^{n-1} - n + 2^n - 1 + n \cdot 2^{n-1} + n + 1 = \\
 &= (n+1) \cdot 2^n.
 \end{aligned}$$

Dowód 3. Skorzystamy z prostego wniosku ze wzoru dwumianowego Newtona. Mianowicie dla każdej liczby rzeczywistej x prawdziwa jest równość:

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} \cdot x^k.$$

Po obu stronach znaku równości mamy więc dwie funkcje, których wartości w każdym punkcie są równe. Są to wielomiany, a więc funkcje różniczkowalne. Ich pochodne są więc też równe. Popatrzymy więc na te pochodne:

$$((1+x)^n)' = n \cdot (1+x)^{n-1}$$

oraz

$$\left(1 + \sum_{k=1}^n \binom{n}{k} \cdot x^k\right)' = \sum_{k=1}^n k \cdot \binom{n}{k} \cdot x^{k-1}.$$

Zatem mamy równość

$$n \cdot (1+x)^{n-1} = \sum_{k=1}^n k \cdot \binom{n}{k} \cdot x^{k-1},$$

w której wystarczy podstawić $x = 1$.

Dowód 4. Jest to dowód kombinatoryczny. Zauważmy najpierw, że wzór (1.11) można zapisać w następującej równoważnej postaci:

$$\sum_{k=1}^n k \binom{n}{k} = n \cdot 2^{n-1}. \quad (1.11)$$

Przypuśćmy zatem, że w naszej firmie pracuje n osób. Chcemy nagrodzić pewne osoby i jedną z nagrodzonych osób dodatkowo chcemy awansować. Na ile sposobów możemy to uczynić?

Różne wybory tych osób będziemy zliczać dwiema metodami. Po pierwsze, możemy najpierw zdecydować, ile osób nagradzamy, potem wybrać osoby, które nagrodzimy i na końcu wybierzemy jedną z tych nagrodzonych osób, by ją awansować. Przypuśćmy więc, że zdecydowaliśmy się nagrodzić k osób. Oczywiście k jest jedną z liczb od 0 (gdy nikogo nie chcemy nagrodzić) do n (gdy chcemy nagrodzić wszystkich). Osoby do nagrody możemy teraz wybrać na $\binom{n}{k}$ sposobów. Przy każdym takim wyborze jedną osobę do awansu możemy wybrać na k sposobów. Dla danej liczby k mamy więc $k \cdot \binom{n}{k}$ sposobów wykonania zadania. Liczba wszystkich sposobów jest zatem równa

$$\sum_{k=0}^n k \cdot \binom{n}{k}.$$

Możemy też popatrzeć na to samo zadanie z drugiej strony. Najpierw wybierzmy jedną osobę do awansu, a potem z pozostałych $n - 1$ osób wybierzmy niektóre do nagrody. Tę jedną osobę do awansu możemy oczywiście wybrać na n sposobów. A pewną liczbę pozostałych osób do nagrody możemy wybrać na 2^{n-1} sposobów – bo tyle jest podzbiorów zbioru liczącego $n - 1$ elementów. Łącznie mamy $n \cdot 2^{n-1}$ sposobów wykonania zadania. To kończy dowód równości (1.11).

10. Tożsamość Cauchy’ego (tożsamość Vandermonde’a)

W tym paragrafie udowodnimy tożsamość, z której kilkakrotnie skorzystamy w dalszym ciągu. Udowodnimy mianowicie, że dla dowolnych liczb naturalnych m , n i k zachodzi równość

$$\sum_{j=0}^k \binom{m}{j} \binom{n}{k-j} = \binom{m+n}{k}. \quad (1.12)$$

Tożsamość (1.12) nosi nazwę **tożsamości Cauchy’ego** (lub **tożsamości Vandermonde’a**). Pokażemy teraz trzy dowody tożsamości Cauchy’ego.

Dowód 1. Zastosujemy indukcję względem m . Pokażemy, że jeśli m jest dowolną liczbą naturalną, to dla dowolnych liczb naturalnych n i k zachodzi równość (1.12). Sprawdzamy najpierw, że ta równość zachodzi dla $m = 0$ i dowolnych n i k , tzn.

$$\sum_{j=0}^k \binom{0}{j} \binom{n}{k-j} = \binom{n}{k}.$$

Zauważmy, że dla $j \neq 0$ mamy $\binom{0}{j} = 0$. Zatem suma po lewej stronie składa się tylko z jednego składnika dla $j = 0$. Mamy zatem dowieść, że

$$\binom{0}{0} \binom{n}{k-0} = \binom{n}{k},$$

co jest oczywiste.

Przeprowadzimy teraz krok indukcyjny. Przypuśćmy więc, że tożsamość Cauchy'ego zachodzi dla pewnej liczby m i wszystkich liczb naturalnych n i k :

$$\sum_{j=0}^k \binom{m}{j} \binom{n}{k-j} = \binom{m+n}{k}.$$

Pokażemy, że wtedy dla dowolnych n i k zachodzi równość

$$\sum_{j=0}^k \binom{m+1}{j} \binom{n}{k-j} = \binom{m+n+1}{k}.$$

A oto obliczenia:

$$\begin{aligned} \sum_{j=0}^k \binom{m+1}{j} \binom{n}{k-j} &= \sum_{j=0}^k \left(\binom{m}{j} + \binom{m}{j-1} \right) \binom{n}{k-j} = \\ &= \sum_{j=0}^k \binom{m}{j} \binom{n}{k-j} + \sum_{j=0}^k \binom{m}{j-1} \binom{n}{k-j} = \\ &= \binom{m+n}{k} + \sum_{j=0}^{k-1} \binom{m}{j} \binom{n}{k-j-1} = \\ &= \binom{m+n}{k} + \binom{m+n}{k-1} = \\ &= \binom{m+n+1}{k}. \end{aligned}$$

Dowód 2. Jeszcze raz wykorzystamy równość

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k.$$

Popatrzmy na następujący iloczyn wielomianów:

$$(1+x)^{m+n} = (1+x)^m \cdot (1+x)^n = \left(\sum_{j=0}^m \binom{m}{j} x^j \right) \cdot \left(\sum_{j=0}^n \binom{n}{j} x^j \right).$$

Po lewej stronie równości mamy oczywiście wielomian stopnia $m+n$. Po prawej stronie mamy iloczyn dwóch wielomianów, jeden stopnia m i drugi stopnia n , a więc jest to także wielomian stopnia $m+n$. Porównajmy współczynniki stojące przy x^k w obu wielomianach. Po lewej stronie mamy zgodnie ze wzorem dwumianowym składnik $\binom{m+n}{k} x^k$. Po prawej stronie, zgodnie ze wzorem na mnożenie wielomianów, mamy

$$\sum_{j=0}^k \binom{m}{j} x^j \cdot \binom{n}{k-j} x^{k-j},$$

czyli

$$\sum_{j=0}^k \binom{m}{j} \binom{n}{k-j} x^k.$$

Porównując te współczynniki w obu wielomianach otrzymamy dowodzoną równość.

Dowód 3. Znów kończymy dowodem kombinatorycznym. W naszej firmie pracuje $m+n$ osób: m kobiet i n mężczyzn. Chcemy nagrodzić k osób. Oczywiście osoby do nagrody możemy wybrać na $\binom{m+n}{k}$ sposobów. Tę liczbę sposobów możemy jednak otrzymać w wyniku innego rozumowania. Najpierw zdecydujemy, ile kobiet powinno dostać nagrodę. Niech j oznacza liczbę nagrodzonych kobiet. Oczywiście j jest jedną z liczb od 0 (gdy nie nagrodzimy żadnej kobiety) do k (gdy nagrodzimy same kobiety). Dla każdej wartości j kobietom możemy przyznać nagrody na $\binom{m}{j}$ sposobów. Gdy rozdzielimy już nagrody między kobiety, zostanie nam $k-j$ „wolnych” nagród do rozdziału między mężczyzn. Tych mężczyzn do nagrody oczywiście możemy wybrać na $\binom{n}{k-j}$ sposobów. Łącznie, dla każdej wartości k mamy $\binom{m}{j} \binom{n}{k-j}$ sposobów przydziału k nagród. Teraz wystarczy zsumować otrzymane liczby sposobów ze względu na j , by otrzymać wzór (1.12).

Interesującym wnioskiem z tożsamości Cauchy’ego jest równość

$$\sum_{j=0}^n \binom{n}{j}^2 = \binom{2n}{n}, \quad (1.13)$$

którą otrzymujemy przyjmując $m = n = k$. Mamy wtedy

$$\binom{2n}{n} = \sum_{j=0}^n \binom{n}{j} \binom{n}{n-j} = \sum_{j=0}^n \binom{n}{j} \binom{n}{j} = \sum_{j=0}^n \binom{n}{j}^2.$$

11. Wybory ze zbiorów uporządkowanych

W dowodach kombinatorycznych, które widzieliśmy do tej pory, wybieraliśmy na początku dowolny zbiór skończony i nie była istotna żadna jego dodatkowa struktura. W tym paragrafie pokażemy kilka dowodów kombinatorycznych, w których istotne będzie to, że wybierzemy zbiór uporządkowany. Dla ustalenia uwagi będzie to zbiór $[n]$ dla pewnej liczby naturalnej n z naturalnym porządkiem.

Udowodnimy najpierw, że dla dowolnych liczb naturalnych m i n zachodzi równość

$$\sum_{k=0}^m \binom{k+n}{n} = \binom{m+n+1}{n+1}. \quad (1.14)$$

Dowód. Zauważmy, że

$$\begin{aligned} P_{n+1}(m+n+1) &= \bigcup_{k=0}^m \{A : |A| = n+1 \text{ oraz } \max(A) = k+n+1\} = \\ &= \bigcup_{k=0}^m \{A : k+n+1 \in A \text{ oraz } |A \cap [k+n]| = n\}. \end{aligned}$$

Zbiory będące składnikami sumy po prawej stronie oczywiście są rozłączne oraz

$$|\{A : k + n + 1 \in A \text{ oraz } |A \cap [k + n]| = n\}| = \binom{k + n}{k}.$$

Równość (1.14) wynika zatem z reguły dodawania.

Ten dowód można opisać słownie w następujący sposób. Mamy wybrać $n + 1$ elementów ze zbioru $[m + n + 1]$. Najpierw wybieramy największy element naszego zbioru. Niech będzie nim liczba l . Następnie ze zbioru $[l - 1]$ wybieramy pozostałe n elementów. Zauważmy, że $n + 1 \leq l \leq m + n + 1$. Liczbę l możemy zatem zapisać w postaci $l = k + n + 1$, gdzie $0 \leq k \leq m$. A więc: najpierw wybieramy liczbę $k + n + 1$, gdzie $k \in \{0, \dots, m\}$, a następnie ze zbioru $[k + n]$ wybieramy n elementów.

Podstawiając $m - n$ w miejsce m i zmieniając granice sumowania we wzorze (1.14) otrzymujemy jego postać równoważną:

$$\sum_{k=n}^m \binom{k}{n} = \binom{m+1}{n+1}. \quad (1.15)$$

Popatrzmy na kilka przykładów tego wzoru:

$$\sum_{k=1}^n \binom{k}{1} = \binom{n+1}{2}. \quad (1.16)$$

$$\sum_{k=1}^n \binom{k}{2} = \binom{n+1}{3}. \quad (1.17)$$

$$\sum_{k=1}^n \binom{k}{3} = \binom{n+1}{4}. \quad (1.18)$$

Ze wzorów tych skorzystamy w następnym paragrafie.

Udowodnimy teraz następujący wzór:

$$\sum_{k=0}^n k(n-k) = \binom{n+1}{3}. \quad (1.19)$$

Mianowicie

$$P_3(n+1) = \bigcup_{k=0}^n \{ \{a, b, c\} : a \in [k], \quad b = k+1, \quad c \in [n+1] \setminus [k+1] \}.$$

Wystarczy teraz zauważyć, że zbiory występujące w sumie po prawej stronie są rozłączne oraz

$$|\{ \{a, b, c\} : a \in [k], \quad b = k+1, \quad c \in [n+1] \setminus [k+1] \}| = k(n-k).$$

Inaczej mówiąc, trzy elementy a , b i c zbioru $[n+1]$ wybieramy w następujący sposób:

- najpierw ustalamy liczbę $k = 0, \dots, n$,
- potem wybieramy a spośród k najmniejszych liczb zbioru $[n+1]$ (tzn. spośród liczb $1, \dots, k$),
- następnie wybieramy $b = k+1$,
- wreszcie wybieramy c spośród $n-k$ największych elementów zbioru $[n+1]$ (tzn. spośród liczb $k+2, \dots, n+1$).

Paragraf ten zakończymy dowodem następującej tożsamości:

$$\sum_{k=0}^n \binom{2n-k}{n} \cdot 2^k = 4^n. \quad (1.20)$$

Rozpatrujemy zbiór $P(2n+1)$. Możemy przedstawić go w postaci sumy

$$P(2n+1) = P_+(2n+1) \cup P_-(2n+1),$$

gdzie

$$P_+(2n+1) = \{A \in P(2n+1) : |A| \geq n+1\}, \quad P_-(2n+1) = \{A \in P(2n+1) : |A| \leq n\}.$$

Zauważmy, że dla dowolnego zbioru $A \in P(2n+1)$

$$A \in P_+(2n+1) \Leftrightarrow [2n+1] \setminus A \in P_-(2n+1).$$

Stąd wynika, że

$$|P_+(2n+1)| = |P_-(2n+1)| = \frac{1}{2} \cdot |P(2n+1)| = \frac{1}{2} \cdot 2^{2n+1} = 2^{2n} = 4^n.$$

Zbiory A należące do $P_+(2n+1)$ mają co najmniej $n+1$ elementów. Będzie nas interesować położenie elementu $(n+1)$ -go w zbiorze A (licząc od najmniejszego elementu, w kolejności rosnącej). Zauważmy, że

$$P_+(2n+1) = \bigcup_{k=0}^n \{A \in P_+(2n+1) : 2n-k+1 \in A \text{ oraz } |A \cap [2n-k]| = n\}.$$

Inaczej mówiąc: mamy wybrać co najmniej $n+1$ elementów ze zbioru $[2n+1]$. Najmniejsze n elementów wybieramy ze zbioru $[2n-k]$, potem wybieramy element $2n-k+1$ i wreszcie dopełniamy dowolnymi elementami wybranymi ze zbioru $[2n+1] \setminus [2n-k+1]$, czyli spośród k największych elementów zbioru $[2n+1]$. Zatem oczywiście

$$|\{A \in P_+(2n+1) : 2n-k+1 \in A \text{ oraz } |A \cap [2n-k]| = n\}| = \binom{2n-k}{n} \cdot 2^k.$$

Ponadto zbiory występujące w sumie po prawej stronie są rozłączne. Do zakończenia dowodu wystarczy sprawdzić, jaki jest zakres zmienności parametru k . Otóż oczywiście

$2n - k \leq 2n$, skąd wynika, że $k \geq 0$. Ponadto $2n - k \geq n$, skąd wynika, że $k \leq n$. Zatem $k \in \{0, \dots, n\}$. To kończy dowód.

12. Sumy potęg liczb naturalnych

Przyjmijmy oznaczenie

$$S_k(n) = \sum_{j=1}^n j^k = 1^k + \dots + n^k,$$

gdzie $n, k \geq 1$. W tym paragrafie wyprowadzimy wzory na $S_k(n)$ dla $k = 0, 1, 2, 3$. Pokażemy mianowicie, że

$$\begin{aligned} S_0(n) &= n, \\ S_1(n) &= \binom{n+1}{2} = \frac{n(n+1)}{2}, \\ S_2(n) &= \frac{1}{4} \cdot \binom{2n+2}{3} = \frac{n(n+1)(2n+1)}{6}, \\ S_3(n) &= \binom{n+1}{2}^2 = S_1(n)^2 = \frac{n^2(n+1)^2}{4}. \end{aligned}$$

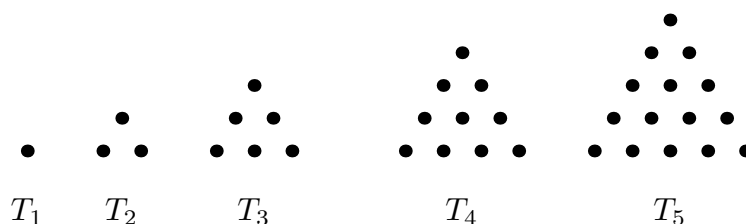
Równość $S_0(n) = n$ jest oczywista. W poprzednim paragrafie udowodniliśmy równość (1.16):

$$\sum_{k=1}^n \binom{k}{1} = \binom{n+1}{2}.$$

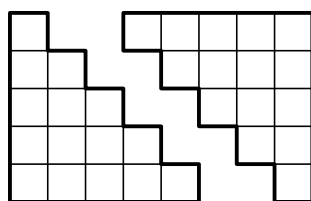
Mamy zatem

$$\sum_{k=1}^n k = \binom{n+1}{2} = \frac{n(n+1)}{2}. \quad (1.21)$$

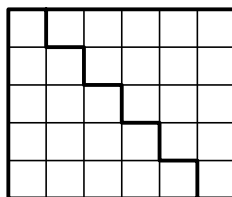
Liczby $T_n = S_1(n)$ nazywamy **liczbami trójkątnymi**. Tożsamość (1.21) wraz z następującym rysunkiem tłumaczy tę nazwę:



Inny dowód tożsamości (1.21) pokażemy na przykładzie. Dwie „piramidki” mające po T_5 kwadratów ustawiamy obok siebie tak jak na rysunku:



Po połączeniu ich otrzymujemy prostokąt o wymiarach 6×5 :



Ogólnie $2T_n = (n+1) \cdot n$, skąd dostajemy

$$S_1(n) = T_n = \frac{n(n+1)}{2}.$$

Następnie udowodnimy, że:

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}. \quad (1.22)$$

Skorzystamy tym razem z równości (1.17):

$$\sum_{k=1}^n \binom{k}{2} = \binom{n+1}{3}.$$

Mamy bowiem

$$\binom{n+1}{3} = \sum_{k=1}^n \binom{k}{2} = \sum_{k=1}^n \frac{k(k-1)}{2},$$

skąd dostajemy

$$2 \cdot \frac{(n+1)n(n-1)}{6} = \sum_{k=1}^n (k^2 - k),$$

czyli

$$\begin{aligned} S_2(n) &= \sum_{k=1}^n k^2 = \frac{(n+1)n(n-1)}{3} + \sum_{k=1}^n k = \\ &= \frac{n(n+1)(n-1)}{3} + \frac{n(n+1)}{2} = \frac{n(n+1)}{6} \cdot (2(n-1) + 3) = \\ &= \frac{n(n+1)(2n+1)}{6}. \end{aligned}$$

Pokażemy teraz dowód kombinatoryczny równości

$$\sum_{k=1}^n k^2 = \frac{1}{4} \cdot \binom{2n+2}{3}. \quad (1.23)$$

Z niej dostajemy natychmiast

$$\sum_{k=1}^n k^2 = \frac{1}{4} \cdot \binom{2n+2}{3} = \frac{(2n+2)(2n+1)(2n)}{4 \cdot 6} = \frac{n(n+1)(2n+1)}{6}.$$

Definiujemy dwa zbiory:

$$A = \{(i, j, k) : 1 \leq i, j \leq k \leq n\},$$

oraz

$$B = \{(i, j, k) : 1 \leq i \leq j \leq k \leq 2n\}.$$

Pokażemy najpierw, że $|A| = S_2(n)$. Mianowicie

$$A = \bigcup_{k=1}^n \{(i, j, k) : i, j \in [k]\}$$

oraz zbiory

$$A_k = \{(i, j, k) : i, j \in [k]\}$$

dla różnych k są rozłączne. Zauważmy ponadto, że $|A_k| = k^2$; z reguły dodawania wynika zatem, że $|A| = S_2(n)$. Wykażemy teraz, że

$$|B| = \binom{2n+2}{3}.$$

Zauważmy, że zbiór B jest zbiorem wszystkich niemalejących ciągów długości 3 o wyrazach ze zbioru $[2n]$. Z rozważań dotyczących kombinacji z powtórzeniami wynika, że takich ciągów jest tyle, ile 3-elementowych kombinacji z powtórzeniami ze zbioru $(2n)$ -elementowego, czyli właśnie $\binom{2n+2}{3}$.

Definiujemy teraz funkcję $f : B \rightarrow A$ w następujący sposób:

$$\begin{aligned} f(2i, 2j, 2k) &= (i, j, k), \\ f(2i, 2j, 2k-1) &= (j+1, i, k), \\ f(2i, 2j-1, 2k) &= (j, i, k), \\ f(2i, 2j-1, 2k-1) &= (j, i, k), \\ f(2i-1, 2j, 2k) &= (i, j, k), \\ f(2i-1, 2j, 2k-1) &= (j+1, i, k), \\ f(2i-1, 2j-1, 2k) &= (i, j, k), \\ f(2i-1, 2j-1, 2k-1) &= (i, j, k). \end{aligned}$$

Sprawdzenie, że $f(i, j, k) \in A$ dla $(i, j, k) \in B$ pozostawiamy jako ćwiczenie. Na przykład

$$f(1, 4, 6) = (1, 2, 3).$$

Można też łatwo pokazać, że jeśli $i \leq j$, to

$$f^{-1}((i, j, k)) = \{(2i, 2j, 2k), (2i-1, 2j, 2k), (2i-1, 2j-1, 2k), (2i-1, 2j-1, 2k-1)\}$$

oraz jeśli $i > j$, to

$$f^{-1}((i, j, k)) = \{(2j, 2i-1, 2k-1), (2j, 2i-1, 2k), (2j, 2i-2, 2k-1), (2j-1, 2i-2, 2k-1)\}.$$

Na przykład

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

Podobnie

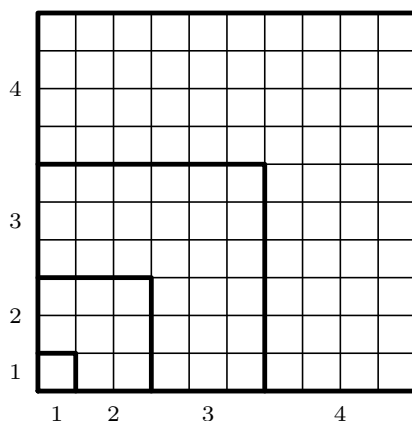
$$f^{-1}((2, 1, 3)) = \{(1, 2, 5), (2, 2, 5), (2, 3, 5), (2, 3, 6)\}.$$

Z tej własności funkcji f wynika, że $4 \cdot |A| = |B|$, co kończy dowód tożsamości (1.23).

Na zakończenie udowodnimy tożsamość

$$\sum_{k=1}^n k^3 = \binom{n+1}{2}^2 = \frac{n^2(n+1)^2}{4}. \quad (1.24)$$

Kwadrat o boku długości T_n podzielmy na T_n^2 kwadratów jednostkowych, a następnie na n części tak jak na rysunku (dla $n = 4$):



Długości odcinków, na jakie podzieliliśmy lewy i dolny bok kwadratu wynoszą kolejno: $1, 2, \dots, n$. Niech G_k oznacza liczbę kwadratów jednostkowych zawartych w k -tej części. Wtedy nietrudno zauważyć, że

$$G_k = T_k^2 - T_{k-1}^2 = \frac{k^2(k+1)^2}{4} - \frac{k^2(k-1)^2}{4} = \frac{k^2}{4} \cdot ((k+1)^2 - (k-1)^2) = \frac{k^2}{4} \cdot 4k = k^3.$$

Stąd wynika, że

$$S_3(n) = \sum_{k=1}^n G_k = T_n^2 = \frac{n^2(n+1)^2}{4},$$

co kończy dowód tożsamości (1.24).

Naszkicujemy jeszcze jeden dowód kombinatoryczny tożsamości (1.24). Definiujemy dwa zbiory

$$A = \{(i, j, k, l) : 0 \leq i, j, k < l \leq n\}$$

oraz

$$B = \{((i, j), (k, l)) : 0 \leq i < j \leq n, 0 \leq k < l \leq n\}.$$

Pozostawiamy jako ćwiczenie wykazanie, że

$$|A| = S_3(n) \quad \text{oraz} \quad |B| = \binom{n+1}{2}^2.$$

Następnie definiujemy funkcję $f : A \rightarrow B$ wzorem

$$f(i, j, k, l) = \begin{cases} ((i, j), (k, l)) & \text{jeśli } i < j, \\ ((k, l), (j, i)) & \text{jeśli } i > j, \\ ((j, l), (k, l)) & \text{jeśli } i = j. \end{cases}$$

Na przykład

$$\begin{aligned} f(1, 2, 3, 4) &= ((1, 2), (3, 4)), \\ f(2, 1, 3, 4) &= ((3, 4), (1, 2)), \\ f(1, 1, 3, 4) &= ((1, 4), (3, 4)). \end{aligned}$$

Pozostawiamy również jako ćwiczenie sprawdzenie, że funkcja f przekształca zbiór A wzajemnie jednoznacznie na zbiór B .

13. Sumy naprzemienne współczynników dwumianowych

Udowodnimy teraz, że jeśli $n \geq 1$, to

$$\sum_{k=0}^n (-1)^k \cdot \binom{n}{k} = 0. \quad (1.25)$$

Dowód. Zdefiniujmy najpierw dwa zbiory

$$\begin{aligned} \mathcal{P} &= \{n \in \mathbb{N} : 2 \mid n\}, \\ \mathcal{N} &= \{n \in \mathbb{N} : 2 \nmid n\}. \end{aligned}$$

Tożsamość (1.25) możemy teraz zapisać w postaci

$$\sum_{k \in [n] \cap \mathcal{P}} \binom{n}{k} = \sum_{k \in [n] \cap \mathcal{N}} \binom{n}{k},$$

czyli

$$\left| \bigcup_{k \in [n] \cap \mathcal{P}} P_k(n) \right| = \left| \bigcup_{k \in [n] \cap \mathcal{N}} P_k(n) \right|.$$

Nietrudno zauważyć, że funkcja

$$f : P(n) \rightarrow P(n)$$

określona wzorem

$$f(A) = A \dot{-} \{n\} = \begin{cases} A \setminus \{n\} & \text{jeśli } n \in A, \\ A \cup \{n\} & \text{jeśli } n \notin A \end{cases}$$

dla $A \in P(n)$ jest funkcją przekształcającą wzajemnie jednoznacznie zbiór $\bigcup_{k \in [n] \cap \mathcal{P}} P_k(n)$ na zbiór $\bigcup_{k \in [n] \cap \mathcal{N}} P_k(n)$ i na odwrót (zauważmy bowiem, że $f^{-1} = f$).

Oczywiście, jeśli $n = 0$, to

$$\sum_{k=0}^0 (-1)^k \cdot \binom{0}{k} = (-1)^0 \cdot \binom{0}{0} = 1. \quad (1.26)$$

Na zakończenie udowodnimy, że jeśli $n \geq 1$ i $m \geq 0$, to

$$\sum_{k=0}^m (-1)^k \cdot \binom{n}{k} = (-1)^m \cdot \binom{n-1}{m}. \quad (1.27)$$

Rozpatrujemy tę samą funkcję $f : P(n) \rightarrow P(n)$ określoną wzorem $f(A) = A \dot{-} \{n\}$ dla $A \in P(n)$. Wiemy, że funkcja f jest różnowartościowa. Będziemy rozpatrywać teraz dwa przypadki.

Przypadek 1. $m = 2p$. Tożsamość (1.27) przyjmuje postać

$$\sum_{k=0}^p \binom{n}{2k} - \sum_{k=0}^{p-1} \binom{n}{2k+1} = \binom{n-1}{2p},$$

czyli

$$\sum_{k=0}^p \binom{n}{2k} - \binom{n-1}{2p} = \sum_{k=0}^{p-1} \binom{n}{2k+1}. \quad (1.27a)$$

Zdefiniujmy trzy zbiory:

$$\begin{aligned} P &= \bigcup_{k=0}^p P_{2k}(n), \\ N &= \bigcup_{k=0}^{p-1} P_{2k+1}(n), \\ R &= P_{2p}(n-1) = \{A \in P_{2p}(n) : n \notin A\}. \end{aligned}$$

Zauważmy teraz, że $f(P \setminus R) = N$, co dowodzi tożsamości (1.27a).

Przypadek 2. $m = 2p + 1$. Tożsamość (1.27) przyjmuje teraz postać

$$\sum_{k=0}^p \binom{n}{2k} - \sum_{k=0}^p \binom{n}{2k+1} = -\binom{n-1}{2p+1},$$

czyli

$$\sum_{k=0}^p \binom{n}{2k} + \binom{n-1}{2p+1} = \sum_{k=0}^{p-1} \binom{n}{2k+1}. \quad (1.27b)$$

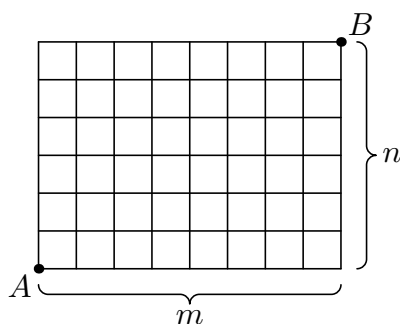
Zdefiniujmy trzy zbiory:

$$\begin{aligned} P &= \bigcup_{k=0}^p P_{2k}(n), \\ N &= \bigcup_{k=0}^{p-1} P_{2k+1}(n), \\ R &= P_{2p+1}(n-1) = \{A \in P_{2p+1}(n) : n \notin A\}. \end{aligned}$$

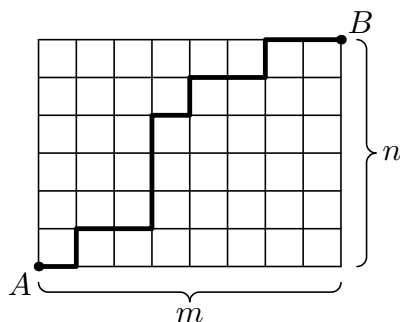
Zauważmy teraz, że $f(P) = N \setminus R$, co dowodzi tożsamości (1.27b). W ten sposób dowód tożsamości (1.27) został zakończony.

14. Zliczanie dróg

Mamy dany prostokąt o wymiarach $m \times n$ podzielony na mn kwadratów jednostkowych. Chcemy obliczyć liczbę dróg prowadzących z punktu A do punktu B , spełniających założenie: w czasie przechodzenia drogi wolno poruszać się tylko w prawo i do góry.



Przykład takiej drogi widzimy na następnym rysunku:



Każdą taką drogę możemy zakodować za pomocą $m + n$ znaków: m poziomych i n pionowych kresek. Kolejność tych kresek odpowiada przechodzonym odcinkom poziomym i pionowym od punktu A do punktu B . Powyższą drogę możemy zatem zakodować za pomocą ciągu

- | - - | | | - | - - | - -

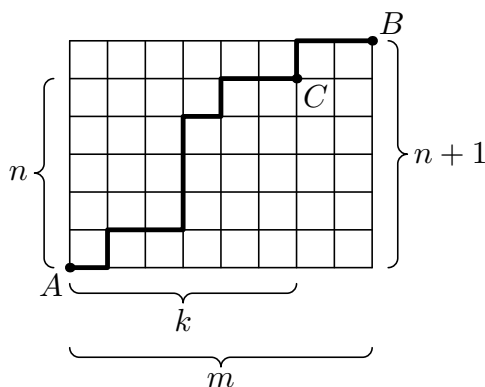
Oczywiste jest też, że każdy taki ciąg koduje dokładnie jedną drogę. Ciąg skład się z $m + n$ znaków. Jest on wyznaczony jednoznacznie po wskazaniu, na których miejscach znajdują się kreski poziome (równoważnie: kreski pionowe). Zatem istnieje $\binom{m+n}{m}$ (równoważnie: $\binom{m+n}{n}$) takich ciągów, a więc i tyle rozważanych dróg. Mamy zatem

$$\text{liczba dróg z } A \text{ do } B = \binom{m+n}{m} = \binom{m+n}{n}. \quad (1.28)$$

Tę interpretację kombinatoryczną współczynnika dwumianowego jako liczby dróg można wykorzystać do dowodu tożsamości kombinatorycznych. Udowodnimy najpierw tożsamość (1.14):

$$\sum_{k=0}^m \binom{k+n}{n} = \binom{m+n+1}{n+1}. \quad (1.14)$$

Weźmy prostokąt o wymiarach $m \times (n+1)$. Każda droga prowadząca z A do B w dokładnie jednym miejscu przechodzi z przedostatniej na ostatnią linię poziomą (i dalej już poziomo zmierza do B). Niech punkt C będzie ostatnim punktem naszej drogi znajdującym się na przedostatniej linii:



Niech odległość punktu C od lewego skraju prostokąta wynosi k kratek. Wtedy istnieje dokładnie $\binom{k+n}{n}$ dróg prowadzących z A do C . Ponieważ każda droga z A do B prowadzi przez jeden taki punkt C , z którego następnie przechodzi do ostatniej poziomej linii i dalej poziomo do B , więc łączna liczba dróg jest równa sumie

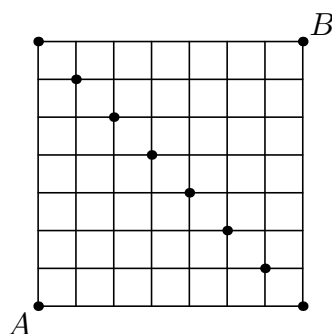
$$\sum_{k=0}^m \binom{k+n}{n}.$$

Z drugiej strony, ze wzoru (1.28) wynika, że ta liczba dróg jest równa $\binom{m+n+1}{n+1}$, co kończy dowód.

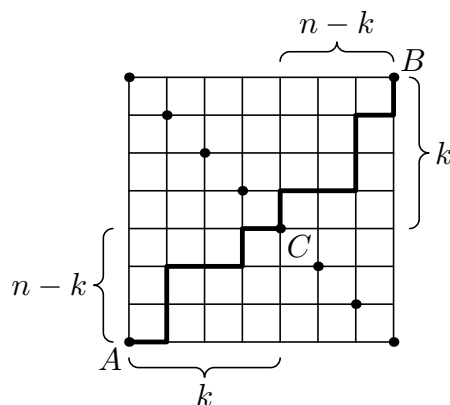
Udowodnimy teraz tożsamość (1.13).

$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}, \quad (1.13)$$

Weźmy kwadrat o boku długości n krutek. Każda droga z A do B przechodzi przez dokładnie jeden zaznaczony punkt leżący na przekątnej kwadratu.



Przypuśćmy, że nasza droga przechodzi przez punkt C położony w odległości k krutek od lewego boku kwadratu. Wtedy ten punkt leży także w odległości k krutek od boku górnego.



Każdą drogę z A do B przechodzącą przez punkt C dzielimy na dwie drogi: z A do C i z C do B . Droga z A do C znajduje się wewnątrz prostokąta o wymiarach $k \times (n-k)$; jest zatem $\binom{n}{k}$ takich dróg. Droga z C do B znajduje się wewnątrz prostokąta o wymiarach $(n-k) \times k$; takich dróg jest też $\binom{n}{k}$. Z reguły mnożenia wynika, że istnieje $\binom{n}{k}^2$ dróg z A do B przechodzących przez punkt C . Sumując te liczby dróg dla $k = 0, 1, \dots, n$, otrzymujemy tożsamość (1.13).

15. Zliczanie funkcji monotonicznych

W tym paragrafie zajmiemy się zliczaniem funkcji monotonicznych $f : [m] \rightarrow [n]$. Najpierw rozpatrujemy funkcje rosnące. Zauważmy, że funkcję rosnącą wyznacza jej zbiór

wartości. Stąd wynika, że liczba funkcji rosnących $f : [m] \rightarrow [n]$ jest równa $\binom{n}{m}$. Oczywiście takie funkcje istnieją, o ile $1 \leq m \leq n$. Nietrudno zauważyć, że funkcji malejących jest tyle samo.

Następnie zajmiemy się funkcjami niemalejącymi. Udowodnimy następujące twierdzenie.

Twierdzenie 1.2. Niech $m, n \geq 1$. Liczba niemalejących funkcji $f : [m] \rightarrow [n]$ jest równa $\binom{m+n-1}{m}$.

Dowód 1. Dla dowolnej funkcji $f : [m] \rightarrow [n]$ definiujemy funkcję $g : [m] \rightarrow [m+n-1]$ wzorem

$$g(k) = f(k) + k - 1$$

dla $k = 1, \dots, m$. Mamy zatem

$$\begin{aligned} g(1) &= f(1), \\ g(2) &= f(2) + 1, \\ g(3) &= f(3) + 2, \\ &\dots \dots \\ g(m-1) &= f(m-1) + m-2, \\ g(m) &= f(m) + m-1. \end{aligned}$$

Ponieważ $1 \leq f(k) \leq n$ dla $k \in [m]$, więc

$$1 \leq f(k) \leq f(k) + k - 1 = g(k) \leq f(k) + m - 1 \leq m + n - 1.$$

Zatem rzeczywiście $g : [m] \rightarrow [m+n-1]$. Teraz pokazujemy, że funkcja f jest niemalejąca wtedy i tylko wtedy, gdy funkcja g jest rosnąca. Przypuśćmy zatem, że funkcja f jest niemalejąca oraz $1 \leq k < l \leq m$. Wtedy $f(k) \leq f(l)$, skąd wynika, że

$$g(k) = f(k) + k - 1 \leq f(l) + k - 1 < f(l) + l - 1 = g(l).$$

Na odwrót, przypuśćmy, że funkcja g jest rosnąca oraz $1 \leq k \leq m$. Wtedy $g(k) < g(k+1)$, czyli

$$f(k) + k - 1 < f(k+1) + (k+1) - 1.$$

Zatem

$$f(k) + k - 1 < f(k+1) + k,$$

czyli

$$f(k) < f(k+1) + 1.$$

Stąd dostajemy $f(k) \leq f(k+1)$. Z dowolności k wynika, że funkcja f jest niemalejąca. Wreszcie pokazujemy, że każda funkcja rosnąca $g : [m] \rightarrow [m+n-1]$ powstaje w ten sposób z pewnej funkcji f . Otóż funkcję f definiujemy wzorem

$$f(k) = g(k) - k + 1$$

dla $k = 1, \dots, m$. Szczegóły dowodu, że $f : [m] \rightarrow [n]$ oraz że f jest niemalejąca, pozostawiamy jako ćwiczenie. Do zakończenia dowodu wystarczy zauważyć, że istnieje $\binom{m+n-1}{m}$ funkcji rosnących z $[m]$ do $[m+n-1]$.

Dowód 2. Funkcja niemalejąca $f : [m] \rightarrow [n]$ jest po prostu ciągiem niemalejącym długości m o wyrazach ze zbioru $[n]$. Przypominamy, że za pomocą takich ciągów definiowaliśmy kombinacje z powtórzeniami. Zatem liczba tych ciągów jest równa liczbie m -elementowych kombinacji z powtórzeniami z n -elementowego zbioru $[n]$, a więc jest równa $\binom{m+n-1}{n-1}$, czyli $\binom{m+n-1}{m}$. Każdą taką kombinację kodowaliśmy za pomocą ciągu kropek i kresek. Ze względu na znaczenie tego kodowania przypomnijmy je w kontekście kodowania funkcji niemalejących.

Każdą funkcję niemalejącą $f : [m] \rightarrow [n]$ kodujemy za pomocą ciągu $m+n-1$ symboli: m kropek i $n-1$ pionowych kresek. Popatrzmy na przykład. Niech $m = 8$ i $n = 7$. Weźmy funkcję $f : [8] \rightarrow [7]$ zdefiniowaną następująco:

$$\begin{aligned} f(1) &= 1, \\ f(2) &= 2, \\ f(3) &= 2, \\ f(4) &= 5, \\ f(5) &= 6, \\ f(6) &= 6, \\ f(7) &= 7, \\ f(8) &= 7. \end{aligned}$$

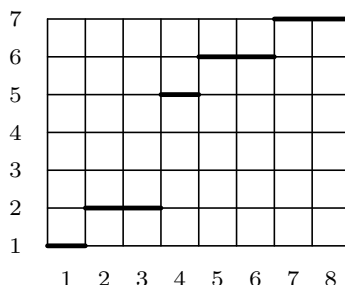
Kodem tej funkcji będzie ciąg ośmiu kropek i sześciu kresek:

• | • • | | | • | • • | • •

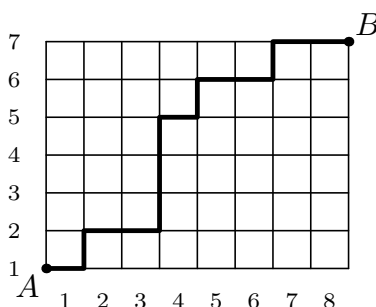
Pionowe kreski dzielą ciąg na 7 części odpowiadających możliwym wartościom funkcji f . Kolejne kropki odpowiadają argumentom. Jeśli k -ta kropka leży w l -tej części, to $f(k) = l$. Zatem pierwsza kropka leży w pierwszej części, druga i trzecia w drugiej części, czwarta w piątej części, piąta i szósta w szóstej części i wreszcie siódma i ósma w siódmej części. Ogólnie mamy m kropek odpowiadających argumentom i $n-1$ kresek dzielących ciąg na n części odpowiadających możliwym wartościom. Teraz wystarczy zauważyć, że każdy taki ciąg koduje dokładnie jedną funkcję niemalejącą i na odwrót, każda funkcja niemalejąca ma dokładnie jeden kod. Wreszcie zauważmy, że kod jest całkowicie wyznaczony, gdy wskażemy, na których miejscach znajdują się kropki; jest zatem $\binom{m+n-1}{m}$ takich kodów i tyle jest funkcji niemalejących $f : [m] \rightarrow [n]$.

Dowód 3. Wykorzystamy prostokąt o wymiarach $m \times (n-1)$ do sporządzenia wykresu funkcji. Na dolnym boku prostokąta numerujemy kolejne kratki liczbami od 1 do m . Na lewym boku numerujemy linie tworzące kratki liczbami od 1 do n . Następnie zaznaczamy pogrubioną linią m poziomych odcinków jednostkowych. Jeśli $f(k) = l$, to w k -tej kolumnie zaznaczamy odcinek znajdujący się na l -tej linii poziomej. Zwracamy uwagę

na to, że powstaje wykres funkcji, w którym wartości nie są punktami, ale odcinkami. Oto przykład takiego wykresu dla $m = 8$ i $n = 7$ i funkcji f określonej w dowodzie 2:



Poziome odcinki łączymy następnie odcinkami pionowymi, otrzymując tym samym drogę z punktu A do punktu B , spełniającą warunek sformułowany w poprzednim paragrafie. Oto droga utworzona z wykresu naszej funkcji f :



Zauważmy teraz, że każda funkcja niemalejąca definiuje w ten sposób dokładnie jedną drogę z A do B i na odwrót: każda droga z A do B spełniająca warunek z poprzedniego paragrafu definiuje dokładnie jedną funkcję niemalejącą. Stąd wynika, że istnieje $\binom{m+n-1}{m}$ takich funkcji. To kończy dowód twierdzenia.

16. Liczby Catalana

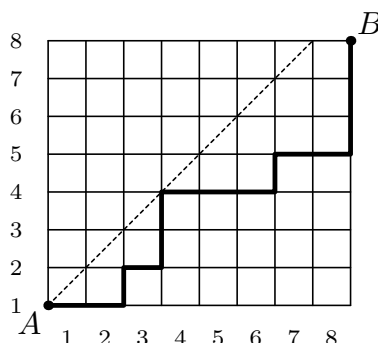
W tym paragrafie rozwiążemy następujące zadanie:

Zadanie. Oblicz, ile jest funkcji niemalejących $f : [n] \rightarrow [n]$ spełniających warunek

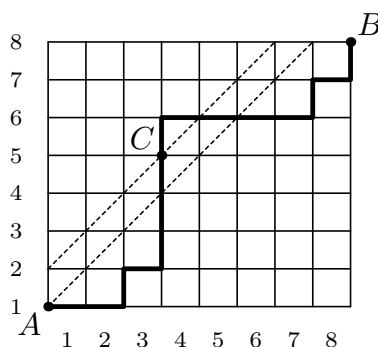
$$f(k) \leq k \quad \text{dla } k = 1, \dots, n. \quad (*)$$

W rozwiązaniu tego zadania wykorzystamy kodowanie funkcji niemalejących za pomocą dróg. Niech zatem dany będzie prostokąt wymiaru $n \times (n-1)$. Na dolnym boku numerujemy kratki liczbami od 1 do n , na lewym boku numerujemy linie od 1 do n . Wiemy już, że każda funkcja niemalejąca $f : [n] \rightarrow [n]$ definiuje dokładnie jedną drogę z punktu A do punktu B . Dodatkowy warunek $(*)$ nałożony na funkcje f oznacza, że droga odpowiadająca funkcji f nie może przekroczyć przerywanej linii zaznaczonej na rysunku

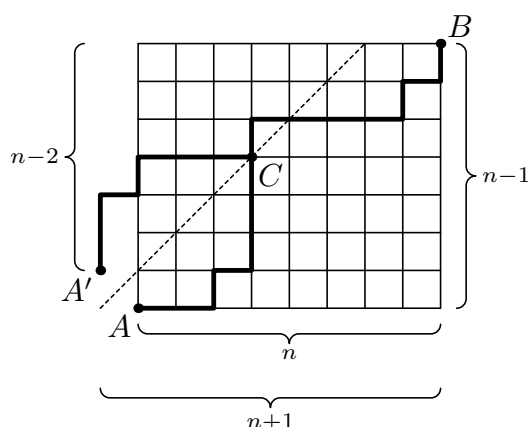
(gdzie przyjęto $n = 8$):



Interesujące nas drogi z A do B nieprzekraczające przerywanej linii zliczymy inaczej: od liczby $\binom{2n-1}{n-1}$ wszystkich dróg z A do B odejmiemy liczbę dróg przekraczających tę linię. Narysujmy więc nową przerywaną linię, położoną o jedną kratkę wyżej. Droga przekraczająca dolną linię przerywaną musi mieć punkt wspólny z wyższą linią przerywaną. Niech C będzie pierwszym punktem na drodze z A do B położonym na tej wyższej linii przerywanej.



Część drogi od punktu A do punktu C odbijamy teraz symetrycznie względem wyższej linii przerywanej. Otrzymujemy drogę z punktu A' do punktu B .



Odwrotnie, każda droga z punktu A' do punktu B musi przeciąć tę wyższą linię przerywaną. Niech C będzie pierwszym punktem wspólnym drogi i tej linii przerywanej. Odbijając symetrycznie część $A'C$ tej drogi względem linii przerywanej, otrzymujemy drogę z A do B przekraczającą dolną linię przerywaną. Zatem interesująca nas liczba

dróg z A do B przekraczających dolną linię przerywaną jest równa liczbie dróg z A' do B , czyli $\binom{2n-1}{n-2}$.

Liczba funkcji $f : [n] \rightarrow [n]$ spełniających warunek $(*)$ jest zatem równa

$$\binom{2n-1}{n-1} - \binom{2n-1}{n-2}.$$

Skorzystamy teraz ze wzoru (1.5):

$$n \cdot \binom{m}{n} = (m - n + 1) \cdot \binom{m}{n-1}. \quad (1.5)$$

Mamy wówczas

$$(n-1) \cdot \binom{2n-1}{n-1} = (2n-1 - (n-1) + 1) \cdot \binom{2n-1}{n-2} = (n+1) \cdot \binom{2n-1}{n-2},$$

czyli

$$\binom{2n-1}{n-2} = \frac{n-1}{n+1} \cdot \binom{2n-1}{n-1}.$$

Stąd otrzymujemy

$$\begin{aligned} \binom{2n-1}{n-1} - \binom{2n-1}{n-2} &= \binom{2n-1}{n-1} - \frac{n-1}{n+1} \cdot \binom{2n-1}{n-1} = \\ &= \left(1 - \frac{n-1}{n+1}\right) \cdot \binom{2n-1}{n-1} = \\ &= \frac{2}{n+1} \cdot \binom{2n-1}{n-1} = \frac{1}{n+1} \cdot \frac{2n}{n} \cdot \binom{2n-1}{n-1} = \\ &= \frac{1}{n+1} \cdot \binom{2n}{n}. \end{aligned}$$

Liczby

$$C_n = \frac{1}{n+1} \cdot \binom{2n}{n}$$

nazywamy **liczbami Catalana**. Oto kilka początkowych liczb Catalana:

$$C_1 = 1, \quad C_2 = 2, \quad C_3 = 5, \quad C_4 = 14, \quad C_5 = 42, \quad C_6 = 132, \quad C_7 = 429.$$

17. Podział zbioru na bloki równoliczne

Następne zadanie kombinatoryczne, którym będziemy się zajmować, polega na zliczaniu podziałów zbioru na równe części. Przypuśćmy, że dany jest mn -elementowy zbiór A . Chcemy wiedzieć, iloma sposobami możemy podzielić go na m zbiorów n -elementowych:

$$A = A_1 \cup \dots \cup A_m, \quad |A_1| = \dots = |A_m| = n.$$

Każdy taki podział możemy łatwo otrzymać z pewnej permutacji całego zbioru A . Mianowicie jako pierwszy zbiór podziału (czyli A_1) bierzemy zbiór składający się z elementów stojących na pierwszych n miejscach, jako drugi zbiór (czyli A_2) bierzemy zbiór elementów stojących na następnych n miejscach itd. Wreszcie zbiór A_m składa się z elementów stojących na ostatnich n miejscach. Oczywiście ten sam podział otrzymamy na ogół z różnych permutacji całego zbioru A .

Liczbę podziałów wyznaczymy dzieląc liczbę wszystkich permutacji przez liczbę permutacji dających ten sam podział zbioru A . Wszystkich permutacji jest oczywiście $(mn)!$. Ten sam podział otrzymamy z permutacji różniących się porządkiem elementów w każdym bloku n -elementowym oraz różniących się porządkiem tych bloków. Każdy blok n -elementowy możemy uporządkować na $n!$ sposobów. Takich bloków jest m , więc łącznie mamy $(n!)^m$ sposobów uporządkowania elementów wewnątrz każdego bloku. Wreszcie mamy $m!$ sposobów uporządkowania tych m bloków. To ostatecznie daje liczbę $(n!)^m \cdot m!$ permutacji wyznaczających ten sam podział zbioru A . Zatem liczba podziałów wynosi

$$\frac{(mn)!}{(n!)^m \cdot m!}.$$

Wyprowadzimy stąd następujący wniosek. Ponieważ liczba podziałów zbioru jest liczbą całkowitą, więc

$$(n!)^m \cdot m! \mid (mn)!$$

Otrzymany wniosek pozwoli nam łatwo rozwiązać następujące zadanie teorioliczne (XLIII Olimpiada Matematyczna, zawody III stopnia, zadanie 6).

Zadanie. Udowodnij, że dla dowolnej liczby naturalnej k

$$(k!)^{k^2+k+1} \mid (k^3)!$$

Rozwiązanie. Najpierw podstawimy $m = n = k$ i otrzymamy

$$(k!)^k \cdot k! \mid (k^2)!$$

czyli

$$(k!)^{k+1} \mid (k^2)!$$

Następnie podstawimy $m = k^2$ oraz $n = k$ i otrzymamy

$$(k!)^{k^2} \cdot (k^2)! \mid (k^3)!$$

Łącząc ze sobą ostatnie dwie zależności łatwo otrzymamy

$$(k!)^{k^2} \cdot (k!)^{k+1} \mid (k^3)!$$

czyli ostatecznie

$$(k!)^{k^2+k+1} \mid (k^3)!$$

18. Operator różnicowy

Niech $f : \mathbb{R} \rightarrow \mathbb{R}$. Definiujemy funkcję $\Delta f : \mathbb{R} \rightarrow \mathbb{R}$ wzorem

$$(\Delta f)(x) = f(x+1) - f(x).$$

Operator Δ tworzący z funkcji f funkcję Δf nazywamy **operatorem różnicowym**. Ten operator różnicowy można iterować. Definiujemy mianowicie ciąg funkcji $\Delta^k f$ dla $k = 1, 2, \dots$ wzorami:

$$\begin{aligned}\Delta^1 f &= \Delta f, \\ \Delta^{k+1} f &= \Delta(\Delta^k f),\end{aligned}$$

Czasami definiujemy ponadto $\Delta^0 f = f$. Popatrzmy teraz na kilka przykładów.

$$\begin{aligned}(\Delta^1 f)(x) &= (\Delta f)(x) = f(x+1) - f(x), \\ (\Delta^2 f)(x) &= (\Delta(\Delta^1 f))(x) = (\Delta f)(x+1) - (\Delta f)(x) = \\ &= (f(x+2) - f(x+1)) - (f(x+1) - f(x)) = \\ &= f(x+2) - 2f(x+1) + f(x), \\ (\Delta^3 f)(x) &= (\Delta(\Delta^2 f))(x) = (\Delta^2 f)(x+1) - (\Delta^2 f)(x) = \\ &= (f(x+3) - 2f(x+2) + f(x+1)) - (f(x+2) - 2f(x+1) + f(x)) = \\ &= f(x+3) - 3f(x+2) + 3f(x+1) - f(x), \\ (\Delta^4 f)(x) &= (\Delta(\Delta^3 f))(x) = (\Delta^3 f)(x+1) - (\Delta^3 f)(x) = \\ &= (f(x+4) - 3f(x+3) + 3f(x+2) - f(x+1)) - \\ &\quad - (f(x+3) - 3f(x+2) + 3f(x+1) - f(x)) = \\ &= f(x+4) - 4f(x+3) + 6f(x+2) - 4f(x+1) + f(x)\end{aligned}$$

i tak dalej. Udowodnimy teraz twierdzenie ogólne.

Twierdzenie 1.3. Niech $f : \mathbb{R} \rightarrow \mathbb{R}$. Wtedy dla dowolnego $k \geq 1$ i dowolnego $x \in \mathbb{R}$ mamy

$$(\Delta^k f)(x) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(x+j). \quad (1.29)$$

Dowód. Stosujemy indukcję względem k . Dla $k = 1$ mamy

$$L = (\Delta^1 f)(x) = f(x+1) - f(x)$$

oraz

$$\begin{aligned}P &= \sum_{j=0}^1 1(-1)^{1-j} \binom{1}{j} f(x+j) = \\ &= (-1)^{1-0} \binom{1}{0} f(x+0) + (-1)^{1-1} \binom{1}{1} f(x+1) = \\ &= (-1) \cdot f(x) + f(x+1) = f(x+1) - f(x) = \\ &= L.\end{aligned}$$

W kroku indukcyjnym zakładamy, że dla pewnego k mamy

$$(\Delta^k f)(x) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(x+j)$$

i dowodzimy, że

$$(\Delta^{k+1} f)(x) = \sum_{j=0}^{k+1} (-1)^{k+1-j} \binom{k+1}{j} f(x+j).$$

Zaczynamy od lewej strony:

$$\begin{aligned} L &= (\Delta^{k+1} f)(x) = (\Delta(\Delta^k f))(x) = (\Delta^k f)(x+1) - (\Delta^k f)(x) = \\ &= \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(x+1+j) - \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(x+j) = \\ &= \sum_{j=1}^{k+1} (-1)^{k-j+1} \binom{k}{j-1} f(x+j) + \sum_{j=0}^k (-1)^{k-j+1} \binom{k}{j} f(x+j) = \\ &= \sum_{j=1}^k (-1)^{k-j+1} \binom{k}{j-1} f(x+j) + (-1)^{k-(k+1)+1} \binom{k}{k} f(x+k+1) + \\ &\quad + (-1)^{k-0+1} \binom{k}{0} f(x+0) + \sum_{j=1}^k (-1)^{k-j+1} \binom{k}{j} f(x+j) = \\ &= (-1)^{k+1-0} \binom{k}{0} f(x+0) + \sum_{j=1}^k (-1)^{k+1-j} \left(\binom{k}{j-1} + \binom{k}{j} \right) f(x+j) + \\ &\quad + (-1)^{k+1-(k+1)} \binom{k}{k} f(x+k+1) = \\ &= (-1)^{k+1-0} \binom{k+1}{0} f(x+0) + \sum_{j=1}^k (-1)^{k+1-j} \binom{k+1}{j} f(x+j) + \\ &\quad + (-1)^{k+1-(k+1)} \binom{k+1}{k+1} f(x+k+1) = \\ &= \sum_{j=0}^{k+1} (-1)^{k+1-j} \binom{k+1}{j} f(x+j) = \\ &= P, \end{aligned}$$

c. b. d. o.

Operatory różnicowe Δ i Δ^n można stosować także do ciągów o wyrazach rzeczywistych. Niech $f : \mathbb{N} \rightarrow \mathbb{R}$. Definiujemy wtedy

$$(\Delta f)(n) = f(n+1) - f(n)$$

oraz

$$\begin{aligned}\Delta^1 f &= \Delta f, \\ \Delta^{k+1} f &= \Delta(\Delta^k f).\end{aligned}$$

Z twierdzenia 1.3 otrzymujemy wtedy następujący wniosek:

Wniosek 1.4. Niech $f : \mathbb{R} \rightarrow \mathbb{R}$. Wtedy dla dowolnego $k \geq 1$ i dowolnego $x \in \mathbb{R}$ mamy

$$(\Delta^k f)(x - k) = \sum_{j=0}^k (-1)^j \binom{k}{j} f(x - j). \quad (1.30)$$

Dowód otrzymujemy zmieniając najpierw kolejność sumowania:

$$\begin{aligned}(\Delta^k f)(x) &= \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(x + j) = \\ &= \sum_{j=0}^k (-1)^j \binom{k}{k-j} f(x + k - j) = \\ &= \sum_{j=0}^k (-1)^j \binom{k}{j} f(x + k - j),\end{aligned}$$

a następnie podstawiając $x - k$ w miejsce x .

Wniosek 1.5. Niech $f : \mathbb{N} \rightarrow \mathbb{R}$. Wtedy dla dowolnego $k \geq 1$ i dowolnego $n \geq 0$ mamy

$$(\Delta^k f)(n) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(n + j). \quad (1.31)$$

W szczególności dla $n = 0$ dostajemy

$$(\Delta^k f)(0) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(j). \quad (1.32)$$

Dla dowodu wystarczy rozszerzyć funkcję f na cały zbiór $\mathbb{R}$, przyjmując na przykład

$$f(x) = \begin{cases} 0 & \text{dla } x < 0, \\ f([x]) & \text{dla } x \geq 0, \end{cases}$$

gdzie $[x]$ oznacza część całkowitą liczby rzeczywistej x .

19. Zastosowania operatora różnicowego

Zacniemy od wykazania, że operator różnicowy jest operatorem liniowym. Przypuśćmy zatem, że mamy dane dwie funkcje $f, g : \mathbb{R} \rightarrow \mathbb{R}$ i dwie liczby rzeczywiste a i b . Definiujemy funkcję $h : \mathbb{R} \rightarrow \mathbb{R}$ wzorem

$$h(x) = a \cdot f(x) + b \cdot g(x)$$

dla $x \in \mathbb{R}$. Wówczas

$$\begin{aligned}(\Delta h)(x) &= h(x+1) - h(x) = a \cdot f(x+1) + b \cdot g(x+1) - a \cdot f(x) - b \cdot g(x) = \\ &= a \cdot (\Delta f)(x) + b \cdot (\Delta g)(x)\end{aligned}$$

dla $x \in \mathbb{R}$. Inaczej mówiąc

$$(\Delta(a \cdot f + b \cdot g))(x) = (a \cdot (\Delta f) + b \cdot (\Delta g))(x)$$

dla $x \in \mathbb{R}$, czyli

$$(\Delta(a \cdot f + b \cdot g)) = (a \cdot (\Delta f) + b \cdot (\Delta g)).$$

Stąd łatwo wynika przez indukcję, że

$$(\Delta^k(a \cdot f + b \cdot g)) = (a \cdot (\Delta^k f) + b \cdot (\Delta^k g))$$

dla $k \geq 1$.

Niech teraz funkcja $f : \mathbb{R} \rightarrow \mathbb{R}$ będzie określona wzorem $f(x) = x^n$ dla $x \in \mathbb{R}$. Wtedy

$$(\Delta f)(x) = f(x+1) - f(x) = (x+1)^n - x^n = \sum_{k=0}^{n-1} \binom{n}{k} x^k$$

dla $x \in \mathbb{R}$. Zatem funkcja Δf jest wielomianem stopnia $n-1$. Stąd i z liniowości operatora Δ wynika, że jeśli f jest wielomianem stopnia n , to Δf jest wielomianem stopnia $n-1$. Przez indukcję względem k łatwo dowodzimy, że $\Delta^k f$ jest wielomianem stopnia $n-k$ dla $k = 1, \dots, n$. W szczególności Δ^n jest wielomianem stałym. Stąd następnie wynika, że dla $k \geq n+1$ funkcja $\Delta^k f$ jest tożsamościowo równa 0.

Udowodnimy teraz przez indukcję, że jeśli funkcja $f : \mathbb{R} \rightarrow \mathbb{R}$ jest określona wzorem $f(x) = x^n$ dla $x \in \mathbb{R}$, to $(\Delta^n f)(x) = n!$ dla $x \in \mathbb{R}$. Tę równość będziemy zapisywać w skrócie jako $\Delta^n x^n = n!$.

Dla $n=1$ mamy $f(x) = x$ dla $x \in \mathbb{R}$. Zatem

$$(\Delta^1 f)(x) = f(x+1) - f(x) = x+1 - x = 1 = 1!$$

Założmy teraz, że dane są funkcje $f_k : \mathbb{R} \rightarrow \mathbb{R}$ określone wzorem $f_k(x) = x^k$ dla $k \geq 0$ i $x \in \mathbb{R}$. Założmy także, że $\Delta^n f_n = n!$. Pamiętamy również, że $\Delta^n f_k = 0$ dla $k < n$. Chcemy udowodnić, że $\Delta^{n+1} f_{n+1} = (n+1)!$. Otóż zauważmy najpierw, że

$$\begin{aligned}(\Delta f_{n+1})(x) &= f_{n+1}(x+1) - f_{n+1}(x) = (x+1)^{n+1} - x^{n+1} = \\ &= \sum_{k=0}^n \binom{n+1}{k} x^k = \left(\sum_{k=0}^n \binom{n+1}{k} f_k \right)(x)\end{aligned}$$

dla $x \in \mathbb{R}$. Zatem

$$\Delta f_{n+1} = \sum_{k=0}^n \binom{n+1}{k} f_k.$$

Stąd dostajemy

$$\begin{aligned} (\Delta^{n+1} f_{n+1}) &= (\Delta^n(\Delta f_{n+1})) = \Delta^n \left(\sum_{k=0}^n \binom{n+1}{k} f_k \right) = \sum_{k=0}^n \left(\binom{n+1}{k} (\Delta^n f_k) \right) = \\ &= \binom{n+1}{n} (\Delta^n f_n) = (n+1) \cdot n! = (n+1)! \end{aligned}$$

Pokażemy teraz kilka przykładów wykorzystania twierdzenia 1.3 oraz wniosków 1.4 i 1.5 do dowodu tożsamości kombinatorycznych.

Przykład 1. Weźmy funkcję $f : \mathbb{R} \rightarrow \mathbb{R}$ określoną wzorem $f(x) = 1$ dla $x \in \mathbb{R}$. Wtedy dla $n \geq 1$ mamy $\Delta^n f = 0$ i z tożsamości (1.30) dostajemy

$$(\Delta^n f)(x - n) = \sum_{k=0}^n (-1)^k \binom{n}{k} f(x - k) = \sum_{k=0}^n (-1)^k \binom{n}{k},$$

czyli

$$\sum_{k=0}^n (-1)^k \binom{n}{k} = 0.$$

Jest to tożsamość (1.25).

Przykład 2. Weźmy funkcję $f : \mathbb{R} \rightarrow \mathbb{R}$ określoną wzorem $f(x) = x$ dla $x \in \mathbb{R}$. Wtedy dla $n \geq 2$ mamy $\Delta^n f = 0$ i z tożsamości (1.30) dostajemy

$$(\Delta^n f)(x - n) = \sum_{k=0}^n (-1)^k \binom{n}{k} f(x - k) = \sum_{k=0}^n (-1)^k \binom{n}{k} (x - k),$$

czyli dla $x = n$ mamy

$$\sum_{k=0}^n (-1)^k \binom{n}{k} (n - k) = 0.$$

Ponieważ

$$\begin{aligned} \sum_{k=0}^n (-1)^k \binom{n}{k} (n - k) &= \sum_{k=0}^n (-1)^k \binom{n}{k} n - \sum_{k=0}^n (-1)^k \binom{n}{k} k = \\ &= n \cdot \sum_{k=0}^n (-1)^k \binom{n}{k} - \sum_{k=0}^n (-1)^k k \binom{n}{k}. \\ &= - \sum_{k=0}^n (-1)^k k \binom{n}{k}, \end{aligned}$$

więc

$$\sum_{k=0}^n (-1)^k k \binom{n}{k} = 0. \quad (1.33)$$

Nietrudno obliczyć, że

$$\sum_{k=0}^1 (-1)^k k \binom{1}{k} = 1 \quad (1.34)$$

oraz

$$\sum_{k=0}^0 (-1)^k k \binom{0}{k} = 0. \quad (1.35)$$

Przykład 3. Niech $n \geq 1$. Weźmy funkcję $f : \mathbb{R} \rightarrow \mathbb{R}$ określoną wzorem $f(x) = x^n$ dla $x \in \mathbb{R}$. Wtedy $\Delta^n f = n!$ i z tożsamości (1.30) dostajemy

$$(\Delta^n f)(x - n) = \sum_{k=0}^n (-1)^k \binom{n}{k} f(x - k) = \sum_{k=0}^n (-1)^k \binom{n}{k} (x - k)^n,$$

czyli

$$\sum_{k=0}^n (-1)^k \binom{n}{k} (x - k)^n = n!. \quad (1.36)$$

Nietrudno sprawdzić, że ta tożsamość jest prawdziwa także dla $n = 0$.

Przykład 4. Weźmy funkcję $f : \mathbb{N} \rightarrow \mathbb{R}$ określoną wzorem $f(n) = 2^n$ dla $n \in \mathbb{N}$. Wtedy nietrudno zauważyć, że $\Delta^n f = f$ dla $n \geq 1$ i z tożsamości (1.32) dostajemy

$$(\Delta^n f)(0) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} f(k) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} 2^k,$$

czyli

$$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} 2^k = 1. \quad (1.37)$$

Ta tożsamość jest też prawdziwa dla $n = 0$.

Przykład 5. Niech dana będzie liczba naturalna m . Definiujemy funkcję $f : \mathbb{N} \rightarrow \mathbb{R}$ wzorem

$$f(n) = \binom{m+n}{m}$$

dla $n \geq 0$. Z równości (1.32) dla ciągu f otrzymujemy

$$(\Delta^k f)(0) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(j),$$

czyli

$$\begin{aligned} (\Delta^k f)(0) &= \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} \binom{m+j}{m} = \\ &= \sum_{j=0}^k (-1)^j \binom{k}{k-j} \binom{m+k-j}{m} = \\ &= \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{m+k-j}{m}. \end{aligned}$$

Z drugiej strony udowodnimy przez indukcję, że

$$(\Delta^k f)(n) = \binom{m+n}{m-k}.$$

Dla $k = 1$ mamy

$$\begin{aligned} (\Delta^1 f)(n) &= (\Delta f)(n) = f(n+1) - f(n) = \binom{m+n+1}{m} - \binom{m+n}{m} = \\ &= \binom{m+n}{m} + \binom{m+n}{m-1} - \binom{m+n}{m} = \binom{m+n}{m-1}. \end{aligned}$$

W kroku indukcyjnym założmy, że

$$(\Delta^k f)(n) = \binom{m+n}{m-k}.$$

Mamy udowodnić, że

$$(\Delta^{k+1} f)(n) = \binom{m+n}{m-k-1}.$$

Otóż

$$\begin{aligned} (\Delta^{k+1} f)(n) &= (\Delta(\Delta^k f))(n) = (\Delta^k f)(n+1) - (\Delta^k f)(n) = \\ &= \binom{m+n+1}{m-k} - \binom{m+n}{m-k} = \binom{m+n}{m-k} + \binom{m+n}{m-k-1} - \binom{m+n}{m-k} = \\ &= \binom{m+n}{m-k-1}. \end{aligned}$$

Stąd otrzymujemy równość

$$\sum_{j=0}^k (-1)^j \binom{k}{j} \binom{m+k-j}{m} = \binom{m}{m-k}. \quad (1.38)$$

Przyjmując teraz $m = n + k$, otrzymujemy

$$\sum_{j=0}^k (-1)^j \binom{k}{j} \binom{n+2k-j}{n+k} = \binom{n+k}{n}. \quad (1.39)$$

Przykład 6. Niech teraz p i q będą dowolnymi liczbami naturalnymi i przyjmijmy

$$f(n) = \binom{p-n}{q}$$

dla $n \geq 0$. Z równości (1.32) dla ciągu f otrzymujemy

$$(\Delta^i f)(0) = \sum_{j=0}^i (-1)^{i-j} \binom{i}{j} f(j),$$

czyli

$$\begin{aligned} (\Delta^i f)(0) &= \sum_{j=0}^i (-1)^{i-j} \binom{i}{j} \binom{p-j}{q} = \\ &= \sum_{j=0}^i (-1)^{i+j} \binom{i}{j} \binom{p-j}{q}. \end{aligned}$$

Z drugiej strony udowodnimy przez indukcję, że

$$(\Delta^i f)(n) = (-1)^i \cdot \binom{p-n-i}{q-i}.$$

Dla $i = 1$ mamy

$$\begin{aligned} (\Delta^1 f)(n) &= (\Delta f)(n) = f(n+1) - f(n) = \binom{p-n-1}{q} - \binom{p-n}{q} = \\ &= \binom{p-n-1}{q} - \left(\binom{p-n-1}{q} + \binom{p-n-1}{q-1} \right) = -\binom{p-n-1}{q-1}. \end{aligned}$$

W kroku indukcyjnym założmy, że

$$(\Delta^i f)(n) = \binom{p-n-i}{q-i}.$$

Mamy udowodnić, że

$$(\Delta^{i+1} f)(n) = \binom{p-n-i-1}{q-i-1}.$$

Otóż

$$\begin{aligned} (\Delta^{i+1} f)(n) &= (\Delta(\Delta^i f))(n) = (\Delta^i f)(n+1) - (\Delta^i f)(n) = \\ &= \binom{p-n-i-1}{q-i} - \binom{p-n-i}{q-i} = \\ &= \binom{p-n-i-1}{q-i} - \left(\binom{p-n-i-1}{q-i} + \binom{p-n-i-1}{q-i-1} \right) = \\ &= -\binom{p-n-i-1}{q-i-1}. \end{aligned}$$

Stąd otrzymujemy równość

$$\sum_{j=0}^i (-1)^{i-j} \binom{i}{j} \binom{p-j}{q} = (-1)^i \cdot \binom{p-i}{q-i}. \quad (1.40)$$

Dzieląc obie strony przez $(-1)^i$ i korzystając z tego, że $(-1)^{-j} = (-1)^j$, otrzymujemy

$$\sum_{j=0}^i (-1)^j \binom{i}{j} \binom{p-j}{q} = \binom{p-i}{q-i}.$$

Przyjmując teraz $p = n + 2k$ i $q = n$, otrzymujemy

$$\sum_{j=0}^i (-1)^j \binom{i}{j} \binom{n+2k-j}{n} = \binom{n+2k-i}{n-i} = \binom{n+2k-i}{2k}. \quad (1.41)$$

19. Tożsamość Li Żeń-Szua

W książce opublikowanej w Nankinie w 1867 roku chiński matematyk Li Żeń-Szua podał szereg interesujących tożsamości – zgodnie z chińską tradycją bez dowodu. Wśród tych tożsamości znalazła się następująca:

$$\sum_{i=0}^k \binom{k}{i}^2 \binom{n+2k-i}{2k} = \binom{n+k}{k}^2. \quad (1.42)$$

Tożsamość tę nazywamy dzisiaj **tożsamością Li Żeń-Szua**. W tym paragrafie udowodnimy tę tożsamość, korzystając z wyników uzyskanych w poprzednim paragrafie. Najpierw jednak udowodnimy dwie tożsamości pomocnicze.

Niech k i j będą liczbami naturalnymi takimi, że $j \leq k$. Wtedy

$$\sum_{i=j}^k \binom{k}{i}^2 \binom{i}{j} = \binom{k}{j} \binom{2k-j}{k}. \quad (1.43)$$

Mianowicie

$$\begin{aligned} \sum_{i=j}^k \binom{k}{i}^2 \binom{i}{j} &= \sum_{i=j}^k \binom{k}{i} \binom{k}{i} \binom{i}{j} = \sum_{i=j}^k \binom{k}{i} \binom{k}{j} \binom{k-j}{i-j} = \\ &= \binom{k}{j} \sum_{i=j}^k \binom{k}{i} \binom{k-j}{i-j} = \binom{k}{j} \sum_{i=0}^k \binom{k}{i} \binom{k-j}{i-j} = \\ &= \binom{k}{j} \sum_{i=0}^k \binom{k}{i} \binom{k-j}{k-i} = \binom{k}{j} \binom{2k-j}{k}. \end{aligned}$$

Druga tożsamość ma postać:

$$\binom{n+2k-j}{n} \binom{2k-j}{k} = \binom{n+2k-j}{n+k} \binom{n+k}{k}. \quad (1.44)$$

Udowodnimy ją korzystając kilkakrotnie z tożsamości (1.5). Mianowicie

$$\begin{aligned}
 \binom{n+2k-j}{n} \binom{2k-j}{k} &= \binom{n+2k-j}{2k-j} \binom{2k-j}{k} = \\
 &= \binom{n+2k-j}{k} \binom{(n+2k-j)-k}{(2k-j)-k} = \\
 &= \binom{n+2k-j}{k} \binom{n+k-j}{k-j} = \\
 &= \binom{n+2k-j}{k} \binom{n+k-j}{n} = \\
 &= \binom{n+2k-j}{k} \binom{(n+2k-j)-k}{(n+k)-k} = \\
 &= \binom{n+2k-j}{n+k} \binom{n+k}{k}.
 \end{aligned}$$

Dowodzimy teraz tożsamości Li Zeń-Szua.

$$\begin{aligned}
 \sum_{i=0}^k \binom{k}{i}^2 \binom{n+2k-i}{2k} &= \sum_{i=0}^k \binom{k}{i}^2 \sum_{j=0}^i (-1)^j \binom{i}{j} \binom{n+2k-j}{n} = \\
 &= \sum_{i=0}^k \sum_{j=0}^i (-1)^j \binom{k}{i}^2 \binom{i}{j} \binom{n+2k-j}{n} = \\
 &= \sum_{j=0}^k \sum_{i=j}^k (-1)^j \binom{k}{i}^2 \binom{i}{j} \binom{n+2k-j}{n} = \\
 &= \sum_{j=0}^k (-1)^j \binom{n+2k-j}{n} \sum_{i=j}^k \binom{k}{i}^2 \binom{i}{j} = \\
 &= \sum_{j=0}^k (-1)^j \binom{n+2k-j}{n} \binom{k}{j} \binom{2k-j}{k} = \\
 &= \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{n+2k-j}{n} \binom{2k-j}{k} = \\
 &= \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{n+2k-j}{n+k} \binom{n+k}{k} = \\
 &= \binom{n+k}{k} \cdot \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{n+2k-j}{n+k} = \\
 &= \binom{n+k}{k} \cdot \binom{n+k}{n} = \\
 &= \binom{n+k}{k}^2.
 \end{aligned}$$

W dowodzie korzystaliśmy najpierw z tożsamości (1.41), potem z (1.43), następnie z (1.44) i wreszcie z (1.39).

20. Współczynniki wielomianowe

Współczynnik dwumianowy $\binom{m}{n}$ jest równy liczbie n -elementowych podzbiorów zbioru m -elementowego. Inaczej mówiąc, jest on równy liczbie podziałów zbioru m -elementowego na dwa zbiory: pierwszy n -elementowy i drugi $(m - n)$ -elementowy. Należy tu zwrócić uwagę na ustaloną kolejność zbiorów. Ta definicja współczynnika dwumianowego ma naturalne uogólnienie.

Przypuśćmy, że dany jest ciąg liczb $(n_1, \dots, n_k)$ takich, że $n_1 + \dots + n_k = m$. **Współczynnikiem wielomianowym** $\binom{m}{n_1, \dots, n_k}$ nazywamy liczbę ciągów $(A_1, \dots, A_k)$ takich, że:

- $A_1, \dots, A_k \subseteq [m]$,
- zbiory $A_1, \dots, A_k$ są parami rozłączne,
- $A_1 \cup \dots \cup A_k = [m]$,
- $|A_1| = n_1, \dots, |A_k| = n_k$.

W szczególności dla $k = 2$ mamy $\binom{m}{n_1, n_2} = \binom{m}{n_1}$, gdzie po lewej stronie mamy współczynnik wielomianowy, a po prawej znany nam współczynnik dwumianowy.

Rodzinę parami rozłącznych podzbiorów zbioru A , dających w sumie cały zbiór A , nazywamy **podziałem** tego zbioru A . Jeśli ustalimy kolejność zbiorów w tej rodzinie, czyli jeśli mamy do czynienia z ciągiem (a nie zbiorem) podzbiorów zbioru A , to będziemy mówić o **uporządkowanych** podziałach zbioru A . Współczynnik wielomianowy $\binom{m}{n_1, \dots, n_k}$ jest zatem równy liczbie uporządkowanych podziałów zbioru $[m]$ na k podzbiorów, z których pierwszy ma n_1 elementów, drugi ma n_2 elementów i tak dalej, aż wreszcie ostatni ma n_k elementów.

Inaczej mówiąc, współczynnik wielomianowy $\binom{m}{n_1, \dots, n_k}$ (gdzie $n_1 + \dots + n_k = m$) jest liczbą ciągów $(x_1, \dots, x_m)$ długości m o wyrazach ze zbioru $[k]$, mających n_1 wyrazów równych 1, n_2 wyrazów równych 2, ... i wreszcie mających n_k wyrazów równych k . Symbolicznie możemy to zapisać w następujący sposób:

$$|\{f \in [k]^{[m]} : |f^{-1}(1)| = n_1, \dots, |f^{-1}(k)| = n_k\}| = \binom{m}{n_1, \dots, n_k}.$$

Współczynniki wielomianowe mają następującą własność (która może być wykorzystana także do zdefiniowania ich przez indukcję względem k):

$$\binom{m}{n_1, \dots, n_k, n_{k+1}} = \binom{m}{n_{k+1}} \cdot \binom{m - n_{k+1}}{n_1, \dots, n_k}. \quad (1.45)$$

Aby bowiem podzielić zbiór $[m]$ na $k+1$ zbiorów, wybieramy najpierw n_{k+1} -elementowy zbiór A_{k+1} , a następnie zbiór mający pozostałe $m - n_{k+1}$ elementów dzielimy na k podzbiorów. Stąd wynika następujące twierdzenie.

Twierdzenie 1.6. Jeśli $n_1 + \dots + n_k = m$, to

$$\binom{m}{n_1, \dots, n_k} = \frac{m!}{n_1! \cdot \dots \cdot n_k!}. \quad (1.46)$$

Dowód. Stosujemy indukcję względem k . Dla $k = 2$ mamy $n_1 + n_2 = m$, skąd dostajemy $n_2 = m - n_1$. Mamy teraz

$$\binom{m}{n_1, n_2} = \binom{m}{n_1} = \frac{m!}{n_1! \cdot (m - n_1)!} = \frac{m!}{n_1! \cdot n_2!}.$$

W kroku indukcyjnym mamy natomiast

$$\begin{aligned} \binom{m}{n_1, \dots, n_k, n_{k+1}} &= \binom{m}{n_{k+1}} \cdot \binom{m - n_{k+1}}{n_1, \dots, n_k} = \\ &= \frac{m!}{n_{k+1}! \cdot (m - n_{k+1})!} \cdot \frac{(m - n_{k+1})!}{n_1! \cdot \dots \cdot n_k!} = \\ &= \frac{m!}{n_1! \cdot \dots \cdot n_k! \cdot n_{k+1}!}, \end{aligned}$$

co kończy dowód.

Z tożsamości (1.45) wynika, że

$$\binom{m}{n_1, \dots, n_k} = \binom{m}{n_1} \cdot \binom{m - n_1}{n_2} \cdot \dots \cdot \binom{m - n_1 - \dots - n_{k-1}}{n_k}. \quad (1.47)$$

Paragraf ten zakończymy podaniem uogólnienia wzoru dwumianowego Newtona. Ten wzór tłumaczy nazwę współczynnika wielomianowego. Mamy mianowicie wzór

$$(a_1 + \dots + a_k)^m = \sum_{\substack{(n_1, \dots, n_k) \\ n_1 + \dots + n_k = m}} \binom{m}{n_1, \dots, n_k} \cdot a_1^{n_1} \cdot \dots \cdot a_k^{n_k}. \quad (1.48)$$

Dowód tego wzoru, podobny do dowodu wzoru (1.10), pozostawiamy jako ćwiczenie.

21. Jeszcze jeden dowód tożsamości Li Żeń-Szua

Przypomnijmy tożsamość Li Żeń-Szua:

$$\sum_{i=0}^k \binom{k}{i}^2 \binom{n + 2k - i}{2k} = \binom{n + k}{k}^2. \quad (1.42)$$

Udowodnimy ją przy dodatkowym założeniu, że $k \leq n$. Dokładniej mówiąc, pokażemy dowód kombinatoryczny tożsamości nieco ogólniejszej. Przypuśćmy zatem, że $k \leq l$ oraz $k \leq n$. Wówczas

$$\sum_{i=0}^k \binom{k}{i} \binom{l}{i} \binom{n + k + l - i}{k + l} = \binom{n + k}{k} \binom{n + l}{l}. \quad (1.49)$$

Pomnożmy obie strony tej tożsamości przez $\binom{k+l}{k}$. Otrzymamy

$$\sum_{i=0}^k \binom{k}{i} \binom{l}{i} \binom{n + k + l - i}{k + l} \binom{k + l}{k} = \binom{n + k}{k} \binom{n + l}{l} \binom{k + l}{k}. \quad (1.50)$$

Skorzystamy teraz ze współczynników wielomianowych. Stosując kilkakrotnie tożsamość (1.45), otrzymujemy

$$\begin{aligned}
 \binom{n+k+l-i}{k-i, l-i, n-i, i, i} &= \binom{n+k+l-i}{n-i} \cdot \binom{k+l}{k-i, l-i, i, i} = \\
 &= \binom{n+k+l-i}{k+l} \cdot \binom{k+l}{i} \cdot \binom{k+l-i}{k-i, l-i, i} = \\
 &= \binom{n+k+l-i}{k+l} \cdot \binom{k+l}{i} \cdot \binom{k+l-i}{k-i} \cdot \binom{l}{l-i, i} = \\
 &= \binom{n+k+l-i}{k+l} \cdot \binom{k+l}{i} \cdot \binom{k+l-i}{k-i} \cdot \binom{l}{i} = \\
 &= \binom{n+k+l-i}{k+l} \cdot \binom{l}{i} \cdot \binom{k+l}{i} \cdot \binom{k+l-i}{k-i} = \\
 &= \binom{n+k+l-i}{k+l} \cdot \binom{l}{i} \cdot \binom{k+l}{k} \cdot \binom{k}{i}
 \end{aligned}$$

Tożsamość (1.50) jest zatem równoważna tożsamości

$$\sum_{i=0}^k \binom{n+k+l-i}{k-i, l-i, n-i, i, i} = \binom{n+k}{k} \binom{n+l}{l} \binom{k+l}{k}. \quad (1.51)$$

Udowodnimy teraz tożsamość (1.51) przy założeniu, że $k = \min\{k, l, n\}$.

Niech A będzie zbiorem wszystkich trójek (π, ρ, σ) , gdzie:

- π jest dowolnym ciągiem długości $k+l$ mającym k wyrazów równych 1 i l wyrazów równych 2.
- ρ jest dowolnym ciągiem długości $l+n$ mającym l wyrazów równych 2 i n wyrazów równych 3.
- σ jest dowolnym ciągiem długości $k+n$ mającym k wyrazów równych 1 i n wyrazów równych 3.

Inaczej mówiąc, $A = A_1 \times A_2 \times A_3$, gdzie

$$\begin{aligned}
 A_1 &= \{\pi \in \{1, 2\}^{[k+l]} : |\pi^{-1}(1)| = k, |\pi^{-1}(2)| = l\}, \\
 A_2 &= \{\rho \in \{2, 3\}^{[l+n]} : |\rho^{-1}(2)| = l, |\rho^{-1}(3)| = n\}, \\
 A_3 &= \{\sigma \in \{1, 3\}^{[k+n]} : |\sigma^{-1}(1)| = k, |\sigma^{-1}(3)| = n\}.
 \end{aligned}$$

Oczywiście istnieje $\binom{k+l}{k}$ ciągów π , $\binom{n+l}{l}$ ciągów ρ oraz $\binom{n+k}{k}$ ciągów σ :

$$|A_1| = \binom{k+l}{k}, \quad |A_2| = \binom{l+n}{l}, \quad |A_3| = \binom{k+n}{k}.$$

Zatem

$$|A| = \binom{n+k}{k} \cdot \binom{n+l}{l} \cdot \binom{k+l}{k}.$$

Niech teraz B będzie zbiorem wszystkich ciągów τ długości $n+k+l-i$, (gdzie i przebiega zbiór $\{0, 1, \dots, k\}$) mających:

- $k-i$ wyrazów równych 1,
- $l-i$ wyrazów równych 2,
- $n-i$ wyrazów równych 3,
- i wyrazów równych 4,
- i wyrazów równych 5.

Inaczej mówiąc, niech X oznacza zbiór wszystkich ciągów skończonych o wyrazach w zbiorze $[5]$. Wtedy

$$B = \bigcup_{i=0}^k B_i,$$

gdzie

$$B_i = \{\tau \in X : |\tau^{-1}(1)| = k-i, |\tau^{-1}(2)| = l-i, |\tau^{-1}(3)| = n-i, |\tau^{-1}(4)| = i, |\tau^{-1}(5)| = i\}$$

dla $i = 0, 1, \dots, k$. Oczywiście jeśli $\tau \in B_i$, to $\tau : [n+k+l-i] \rightarrow [5]$. Wprost z definicji współczynników wielomianowych wynika, że

$$|B_i| = \binom{n+k+l-i}{k-i, l-i, n-i, i, i},$$

dla $i = 0, 1, \dots, k$. Zatem

$$|B| = \sum_{i=0}^k \binom{n+k+l-i}{k-i, l-i, n-i, i, i}.$$

Wystarczy teraz dowieść, że zbiory A i B mają tyle samo elementów. W tym celu pokażemy, w jaki sposób można z trójki ciągów $(\pi, \rho, \sigma) \in A$ utworzyć ciąg $\tau \in B$ tak, by otrzymana odpowiedniość była wzajemnie jednoznaczna.

Przypuśćmy zatem, że mamy trójkę ciągów $(\pi, \rho, \sigma) \in A$. Pamiętajmy, że ciągi π i ρ mają po k wyrazów równych 1, ciągi ρ i σ mają po l wyrazów równych 2 oraz ciągi π i σ mają po n wyrazów równych 3. Niech ε oznacza ciąg pusty. Przyjmijmy na początku, że $\tau = \varepsilon$. W kolejnych krokach będziemy dopisywać wyrazy na końcu ciągu τ , skreślając przy tym pewne wyrazy ciągów π, ρ, σ . Robimy to, kierując się następującymi regułami:

- 1) jeśli $\pi_1 = \sigma_1 = 1$, to z każdego z ciągów π i σ usuwamy pierwszy wyraz i na końcu ciągu τ dopisujemy 1;
- 2) jeśli $\pi_1 = \rho_1 = 2$, to z każdego z ciągów π i ρ usuwamy pierwszy wyraz i na końcu ciągu τ dopisujemy 2;
- 3) jeśli $\rho_1 = \sigma_1 = 3$, to z każdego z ciągów ρ i σ usuwamy pierwszy wyraz i na końcu ciągu τ dopisujemy 3;
- 4) jeśli $\pi_1 = 1$, $\rho_1 = 2$ i $\sigma_1 = 3$, to z każdego z ciągów π, ρ i σ usuwamy pierwszy wyraz i na końcu ciągu τ dopisujemy 4;
- 5) jeśli $\pi_1 = 2$, $\rho_1 = 3$ i $\sigma_1 = 1$, to z każdego z ciągów π, ρ i σ usuwamy pierwszy wyraz i na końcu ciągu τ dopisujemy 5.

Nietrudno zauważyć, że jeśli wszystkie ciągi π , ρ i σ są niepuste, to zachodzi dokładnie jeden warunek opisany w punktach od 1) do 5) powyżej. Musimy zastanowić się, jak wyglądają dwa pozostałe ciągi, jeśli jeden z nich stanie się pusty (w wyniku dokonywanych skreśleń pierwszych wyrazów). Przypuśćmy zatem, że w pewnym momencie w czasie konstrukcji ciągu τ usuwamy jedyny wyraz któregoś z ciągów, np. z ciągu σ . Przypuśćmy, że do tego momentu włącznie i razy stosowaliśmy regułę 4) (usuwając pierwszy wyraz każdego ciągu), j razy stosowaliśmy regułę 5) oraz p , q i r razy stosowaliśmy odpowiednio reguły 1), 2) i 3). Zatem:

- z ciągu π usunęliśmy $i + p$ wyrazów równych 1 i $j + q$ wyrazów równych 2;
- z ciągu ρ usunęliśmy $i + q$ wyrazów równych 2 i $j + r$ wyrazów równych 3;
- z ciągu σ usunęliśmy $j + p$ wyrazów równych 1 i $i + r$ wyrazów równych 3.

Ponieważ z ciągu σ usunęliśmy wszystkie wyrazy, więc $j + p = k$ oraz $i + r = n$. W ciągu π pozostało zatem $k - (i + p) = (j + p) - (i + p) = j - i$ wyrazów równych 1 oraz $l - (j + q)$ wyrazów równych 2. W ciągu ρ pozostało natomiast $l - (i + q)$ wyrazów równych 2 oraz $n - (j + r) = (i + r) - (j + r) = i - j$ wyrazów równych 3. Zauważmy jednak, że $i - j = -(j - i)$. Jeśli $i \neq j$, to jedna z liczb $i - j$ i $j - i$ jest ujemna, co jest niemożliwe. Zatem $i = j$. To pokazuje, że w chwili, gdy usuniemy wszystkie wyrazy ciągu σ , w pozostałych ciągach pozostaną już tylko wyrazy równe 2. Ponadto liczba czwórek dopisanych do ciągu τ jest równa liczbie dopisanych piątek. Ponieważ $l - (j + q) = l - (i + q)$, więc w ciągach π i ρ zostało tyle samo dwójek. To znaczy, że od tej chwili będziemy stosować już tylko regułę 2), do ciągu τ dopisując $l - (j + q)$ dwójek.

Podobnie będzie, gdy wyczerpiemy wszystkie wyrazy ciągu π lub ρ . Jeśli zatem usuniemy wszystkie wyrazy któregoś z trzech ciągów, to od tego momentu do końca będziemy stosować reguły od 1) do 3). Może się też okazać, że usuniemy jednocześnie pierwsze wyrazy z trzech ciągów długości 1; wtedy jednocześnie wszystkie trzy ciągi staną się puste. Poprzednie rozumowanie obejmuje także ten przypadek; nigdzie nie zakładaliśmy, że liczba pozostałych dwójek jest różna od zera. Wykazaliśmy przy tym, że w otrzymanym ciągu τ liczba czwórek jest równa liczbie piątek. Jeśli i razy dopisaliśmy do ciągu τ czwórkę i tyle samo razy piątkę, to także $k - i$ razy dopisaliśmy jedynekę (bo jeszcze tyle jedynek musieliśmy usunąć z ciągu π), $l - i$ razy dopisaliśmy dwójkę i $n - i$ razy trójkę. Otrzymany ciąg τ należy zatem do zbioru B .

Popatrzmy teraz na trzy przykłady zastosowania opisanej procedury. W kolejnych wierszach wyrazy usuwane z ciągów π , ρ i σ i dopisywane do ciągu τ są wytłuszczone. We wszystkich przykładach $k = 2$, $l = 3$ i $n = 4$. A oto pierwszy przykład:

π	ρ	σ	τ
(1 , 2, 1, 2, 2)	(3, 2, 2, 3, 3, 2, 3)	(1 , 3, 1, 3, 3, 3)	(1)
(2, 1, 2, 2)	(3 , 2, 2, 3, 3, 2, 3)	(3 , 1, 3, 3, 3)	(1, 3)
(2 , 1, 2, 2)	(2, 2, 3, 3, 2, 3)	(1, 3, 3, 3)	(1, 3, 2)
(1 , 2, 2)	(2, 3, 3, 2, 3)	(1 , 3, 3, 3)	(1, 3, 2, 1)
(2 , 2)	(2 , 3, 3, 2, 3)	(3, 3, 3)	(1, 3, 2, 1, 2)
(2)	(3 , 3, 2, 3)	(3 , 3, 3)	(1, 3, 2, 1, 2, 3)
(2)	(3 , 2, 3)	(3 , 3)	(1, 3, 2, 1, 2, 3, 3)
(2)	(2 , 3)	(3)	(1, 3, 2, 1, 2, 3, 3, 2)
ε	(3)	(3)	(1, 3, 2, 1, 2, 3, 3, 2, 3)

Z ciągów $\pi = (1, 2, 1, 2, 2)$, $\rho = (3, 2, 2, 3, 3, 2, 3)$ i $\sigma = (1, 3, 1, 3, 3, 3)$ otrzymaliśmy ciąg $\tau = (1, 3, 2, 1, 2, 3, 3, 2, 3)$. Zauważmy, że w ciągu τ nie ma ani jednej czwórki i piątki; za każdym razem korzystaliśmy bowiem z reguł od 1) do 3). Gdy skreśliliśmy wszystkie wyrazy ciągu π , w dwóch pozostałych ciągach mieliśmy po jednej trójce. A teraz drugi przykład:

π	ρ	σ	τ
(2, 2, 1, 2, 1)	(3 , 2, 3, 2, 3, 3, 2)	(3 , 1, 1, 3, 3, 3)	(3)
(2 , 2, 1, 2, 1)	(2 , 3, 2, 3, 3, 2)	(1, 1, 3, 3, 3)	(3, 2)
(2 , 1, 2, 1)	(3 , 2, 3, 3, 2)	(1 , 1, 3, 3, 3)	(3, 2, 5)
(1 , 2, 1)	(2, 3, 3, 2)	(1, 3, 3, 3)	(3, 2, 5, 1)
(2 , 1)	(2 , 3, 3, 2)	(3, 3, 3)	(3, 2, 5, 1, 2)
(1)	(3 , 3, 2)	(3 , 3, 3)	(3, 2, 5, 1, 2, 3)
(1)	(3 , 2)	(3 , 3)	(3, 2, 5, 1, 2, 3, 3)
(1)	(2)	(3)	(3, 2, 5, 1, 2, 3, 3, 4)

Tym razem z ciągów $\pi = (2, 2, 1, 2, 1)$, $\rho = (3, 2, 3, 2, 3, 3, 2)$ i $\sigma = (3, 1, 1, 3, 3, 3)$ otrzymaliśmy ciąg $\tau = (3, 2, 5, 1, 2, 3, 3, 4)$. Po jednym razie korzystaliśmy z reguł 4) i 5); to dało po jednym wyrazie 4 i 5. Zauważmy, że w tym przykładzie jednocześnie wyczerpałiliśmy wszystkie wyrazy trzech ciągów. Wreszcie popatrzmy na trzeci przykład:

π	ρ	σ	τ
(1, 1, 2, 2, 2)	(3 , 2, 2, 3, 3, 3, 2)	(3 , 3, 3, 1, 3, 1)	(3)
(1 , 1, 2, 2, 2)	(2 , 2, 3, 3, 3, 2)	(3 , 3, 1, 3, 1)	(3, 4)
(1 , 2, 2, 2)	(2 , 3, 3, 3, 2)	(3 , 1, 3, 1)	(3, 4, 4)
(2 , 2, 2)	(3 , 3, 3, 2)	(1, 3, 1)	(3, 4, 4, 5)
(2, 2)	(3 , 3, 2)	(3 , 1)	(3, 4, 4, 5, 3)
(2 , 2)	(3 , 2)	(1)	(3, 4, 4, 5, 3, 5)
(2)	(2)	ε	(3, 4, 4, 5, 3, 5, 2)

W tym przykładzie z ciągów $\pi = (1, 1, 2, 2, 2)$, $\rho = (3, 2, 2, 3, 3, 3, 2)$ i $\sigma = (3, 3, 3, 1, 3, 1)$ otrzymaliśmy ciąg $\tau = (3, 4, 4, 5, 3, 5, 2)$. Zauważmy, że w ciągu τ nie występuje wyraz równy 1; mianowicie w tym przykładzie $i = k = 2$.

Z każdego ciągu $\tau \in B$ możemy w jednoznaczny sposób otrzymać trójkę ciągów (π, ρ, σ) należącą do zbioru A . Najpierw przyjmujemy $\pi = \rho = \sigma = \varepsilon$. Później kierujemy się następującymi regułami:

- 1) jeśli $\tau_1 = 1$, to na końcu ciągów π i σ dopisujemy jedynekę,
- 2) jeśli $\tau_1 = 2$, to na końcu ciągów π i ρ dopisujemy dwójkę,
- 3) jeśli $\tau_1 = 3$, to na końcu ciągów ρ i σ dopisujemy trójkę,
- 4) jeśli $\tau_1 = 4$, to na końcu ciągów π , ρ i σ odpowiednio dopisujemy jedynekę, dwójkę i trójkę,
- 5) jeśli $\tau_1 = 5$, to na końcu ciągów π , ρ i σ odpowiednio dopisujemy dwójkę, trójkę i jedynekę,
- 6) za każdym razem z ciągu τ usuwamy pierwszy wyraz.

Działanie tej procedury zilustrujemy przykładami. Niech $\tau = (1, 3, 2, 1, 2, 3, 3, 2, 3)$. Tak jak poprzednio wyrazy usuwane z ciągu τ i dopisywane do ciągów π , ρ i σ są wytłuszczone:

τ	π	ρ	σ
(1 , 3, 2, 1, 2, 3, 3, 2, 3)	(1)	ε	(1)
(3 , 2, 1, 2, 3, 3, 2, 3)	(1)	(3)	(1, 3)
(2 , 1, 2, 3, 3, 2, 3)	(1, 2)	(3, 2)	(1, 3)
(1 , 2, 3, 3, 2, 3)	(1, 2, 1)	(3, 2)	(1, 3, 1)
(2 , 3, 3, 2, 3)	(1, 2, 1, 2)	(3, 2, 2)	(1, 3, 1)
(3 , 3, 2, 3)	(1, 2, 1, 2)	(3, 2, 2, 3)	(1, 3, 1, 3)
(3 , 2, 3)	(1, 2, 1, 2)	(3, 2, 2, 3, 3)	(1, 3, 1, 3, 3)
(2 , 3)	(1, 2, 1, 2, 2)	(3, 2, 2, 3, 3, 2)	(1, 3, 1, 3, 3)
(3)	(1, 2, 1, 2, 2)	(3, 2, 2, 3, 3, 2, 3)	(1, 3, 1, 3, 3, 3)

Z ciągu $\tau = (1, 3, 2, 1, 2, 3, 3, 2, 3)$ odtworzyliśmy zatem tę samą trójkę ciągów (π, ρ, σ) , którą widzieliśmy w pierwszym przykładzie. Przykład ten ilustruje zatem procedurę odwrotną do pierwszego przykładu. Następne przykłady będą w tym sensie odwrotne do przykładu drugiego i trzeciego. A oto przykład drugi:

τ	π	ρ	σ
(3 , 2, 5, 1, 2, 3, 3, 4)	ε	(3)	(3)
(2 , 5, 1, 2, 3, 3, 4)	(2)	(3, 2)	(3)
(5 , 1, 2, 3, 3, 4)	(2, 2)	(3, 2, 3)	(3, 1)
(1 , 2, 3, 3, 4)	(2, 2, 1)	(3, 2, 3)	(3, 1, 1)
(2 , 3, 3, 4)	(2, 2, 1, 2)	(3, 2, 3, 2)	(3, 1, 1)
(3 , 3, 4)	(2, 2, 1, 2)	(3, 2, 3, 2, 3)	(3, 1, 1, 3)
(3 , 4)	(2, 2, 1, 2)	(3, 2, 3, 2, 3, 3)	(3, 1, 1, 3, 3)
(4)	(2, 2, 1, 2, 1)	(3, 2, 3, 2, 3, 3, 2)	(3, 1, 1, 3, 3, 3)

Wreszcie trzeci przykład:

τ	π	ρ	σ
(3 , 4, 4, 5, 3, 5, 2)	ε	(3)	(3)
(4 , 4, 5, 3, 5, 2)	(1)	(3, 2)	(3, 3)
(4 , 5, 3, 5, 2)	(1, 1)	(3, 2, 2)	(3, 3, 3)
(5 , 3, 5, 2)	(1, 1, 2)	(3, 2, 2, 3)	(3, 3, 3, 1)
(3 , 5, 2)	(1, 1, 2)	(3, 2, 2, 3, 3)	(3, 3, 3, 1, 3)
(5 , 2)	(1, 1, 2, 2)	(3, 2, 2, 3, 3, 3)	(3, 3, 3, 1, 3, 1)
(2)	(1, 1, 2, 2, 2)	(3, 2, 2, 3, 3, 3, 2)	(3, 3, 3, 1, 3, 1)

Nietrudno zauważyć, że z dowolnego ciągu $\tau \in B$ otrzymamy rzeczywiście trójkę ciągów (π, ρ, σ) należącą do zbioru A i że opisane dwie procedury są odwrotne do siebie. Szczegóły dowodu pozostawiamy jako ćwiczenie. Widzimy zatem, że zbiory A i B są równoliczne i w ten sposób dowód uogólnionej tożsamości Li Żeń-Szua (1.44) jest zakończony.

Spis tożsamości kombinatorycznych

$$\binom{m}{0} = \binom{m}{m} = 1. \quad (1.1)$$

$$n \cdot \binom{m}{n} = m \cdot \binom{m-1}{n-1}, \quad (1.2)$$

$$\binom{m}{n} = \frac{m}{n} \cdot \binom{m-1}{n-1}. \quad (1.3)$$

$$\binom{m}{n} = \frac{m!}{n! \cdot (m-n)!}. \quad (1.4)$$

$$n \cdot \binom{m}{n} = (m-n+1) \cdot \binom{m}{n-1}. \quad (1.5)$$

$$\binom{m}{n} \binom{n}{k} = \binom{m}{k} \binom{m-k}{n-k}. \quad (1.6)$$

$$\binom{m}{n} = \binom{m}{m-n}. \quad (1.7)$$

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}. \quad (1.8)$$

$$\sum_{n=0}^m \binom{m}{n} = 2^m. \quad (1.9)$$

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k. \quad (1.10)$$

$$\sum_{k=0}^n k \binom{n}{k} = n \cdot 2^{n-1} \quad \text{dla } n \geq 1. \quad (1.11)$$

$$\sum_{j=0}^k \binom{m}{j} \binom{n}{k-j} = \binom{m+n}{k}. \quad (1.12)$$

$$\sum_{j=0}^n \binom{n}{j}^2 = \binom{2n}{n}, \quad (1.13)$$

$$\sum_{k=0}^m \binom{k+n}{n} = \binom{m+n+1}{n+1}. \quad (1.14)$$

$$\sum_{k=n}^m \binom{k}{n} = \binom{m+1}{n+1}. \quad (1.15)$$

$$\sum_{k=1}^n \binom{k}{1} = \binom{n+1}{2}. \quad (1.16)$$

$$\sum_{k=1}^n \binom{k}{2} = \binom{n+1}{3}. \quad (1.17)$$

$$\sum_{k=1}^n \binom{k}{3} = \binom{n+1}{4}. \quad (1.18)$$

$$\sum_{k=0}^n k(n-k) = \binom{n+1}{3}. \quad (1.19)$$

$$\sum_{k=0}^n \binom{2n-k}{n} \cdot 2^k = 4^n. \quad (1.20)$$

$$\sum_{k=1}^n k = \binom{n+1}{2} = \frac{n(n+1)}{2}. \quad (1.21)$$

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}. \quad (1.22)$$

$$\sum_{k=1}^n k^2 = \frac{1}{4} \cdot \binom{2n+2}{3}. \quad (1.23)$$

$$\sum_{k=1}^n k^3 = \binom{n+1}{2}^2 = \frac{n^2(n+1)^2}{4}. \quad (1.24)$$

$$\sum_{k=0}^n (-1)^k \cdot \binom{n}{k} = 0 \quad \text{dla } n \geq 1. \quad (1.25)$$

$$\sum_{k=0}^n (-1)^k \cdot \binom{n}{k} = 1 \quad \text{dla } n = 0. \quad (1.26)$$

$$\sum_{k=0}^m (-1)^k \cdot \binom{n}{k} = (-1)^m \cdot \binom{n-1}{m}. \quad (1.27)$$

$$\text{liczba dróg z } A \text{ do } B = \binom{m+n}{m} = \binom{m+n}{n}. \quad (1.28)$$

$$(\Delta^k f)(x) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(x+j). \quad (1.29)$$

$$(\Delta^k f)(x-k) = \sum_{j=0}^k (-1)^j \binom{k}{j} f(x-j). \quad (1.30)$$

$$(\Delta^k f)(n) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(n+j). \quad (1.31)$$

$$(\Delta^k f)(0) = \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} f(j). \quad (1.32)$$

$$\sum_{k=0}^n (-1)^k k \binom{n}{k} = 0 \quad \text{dla } n \geq 2. \quad (1.33)$$

$$\sum_{k=0}^1 (-1)^k k \binom{1}{k} = 1 \quad (1.34)$$

$$\sum_{k=0}^0 (-1)^k k \binom{0}{k} = 0. \quad (1.35)$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} (x-k)^n = n!. \quad (1.36)$$

$$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} 2^k = 1. \quad (1.37)$$

$$\sum_{j=0}^k (-1)^j \binom{k}{j} \binom{m+k-j}{m} = \binom{m}{m-k}. \quad (1.38)$$

$$\sum_{j=0}^k (-1)^j \binom{k}{j} \binom{n+2k-j}{n+k} = \binom{n+k}{n}. \quad (1.39)$$

$$\sum_{j=0}^i (-1)^{i-j} \binom{i}{j} \binom{p-j}{q} = (-1)^i \cdot \binom{p-i}{q-i}. \quad (1.40)$$

$$\sum_{j=0}^i (-1)^j \binom{i}{j} \binom{n+2k-j}{n} = \binom{n+2k-i}{n-i} = \binom{n+2k-i}{2k}. \quad (1.41)$$

$$\sum_{i=0}^k \binom{k}{i}^2 \binom{n+2k-i}{2k} = \binom{n+k}{k}^2. \quad (1.42)$$

$$\sum_{i=j}^k \binom{k}{i}^2 \binom{i}{j} = \binom{k}{j} \binom{2k-j}{k}. \quad (1.43)$$

$$\binom{n+2k-j}{n} \binom{2k-j}{k} = \binom{n+2k-j}{n+k} \binom{n+k}{k}. \quad (1.44)$$

$$\binom{m}{n_1, \dots, n_k, n_{k+1}} = \binom{m}{n_{k+1}} \cdot \binom{m-n_{k+1}}{n_1, \dots, n_k}. \quad (1.45)$$

$$\binom{m}{n_1, \dots, n_k} = \frac{m!}{n_1! \cdot \dots \cdot n_k!}. \quad (1.46)$$

$$\binom{m}{n_1, \dots, n_k} = \binom{m}{n_1} \cdot \binom{m-n_1}{n_2} \cdot \dots \cdot \binom{m-n_1-\dots-n_{k-1}}{n_k}. \quad (1.47)$$

$$(a_1 + \dots + a_k)^m = \sum_{\substack{(n_1, \dots, n_k) \\ n_1 + \dots + n_k = m}} \binom{m}{n_1, \dots, n_k} \cdot a_1^{n_1} \cdot \dots \cdot a_k^{n_k}. \quad (1.48)$$

$$\sum_{i=0}^k \binom{k}{i} \binom{l}{i} \binom{n+k+l-i}{k+l} = \binom{n+k}{k} \binom{n+l}{l}. \quad (1.49)$$

$$\sum_{i=0}^k \binom{k}{i} \binom{l}{i} \binom{n+k+l-i}{k+l} \binom{k+l}{k} = \binom{n+k}{k} \binom{n+l}{l} \binom{k+l}{k}. \quad (1.50)$$

$$\sum_{i=0}^k \binom{n+k+l-i}{k-i, l-i, n-i, i, i} = \binom{n+k}{k} \binom{n+l}{l} \binom{k+l}{k}. \quad (1.51)$$

ZASADA WŁACZEŃ I WYŁĄCZEŃ

1. Przypomnienie

$$[n] = \{1, \dots, n\} \quad \text{dla } n > 0,$$

$$P_k(n) = \{A \subseteq [n] : |A| = k\}.$$

Przyjmijmy również oznaczenie

$$P_{\geq k}(n) = \{A \subseteq [n] : |A| \geq k\}.$$

Przypominamy, że w wykładzie 1 udowodniliśmy następujące dwie równości:

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (2.1)$$

oraz

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \quad (2.2)$$

Udowodnimy teraz twierdzenie będące uogólnieniem tych dwóch równości na przypadek dowolnej liczby zbiorów skończonych.

2. Wzór włączeń i wyłączeń

Twierdzenie 2.1. Jeśli $A_1, \dots, A_n$ są zbiorami skończonymi, to

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.3)$$

Dowód. Wprowadźmy oznaczenie:

$$S_k(B_1, \dots, B_m) = \sum_{T \in P_k(m)} \left| \bigcap_{j \in T} B_j \right|.$$

Teza twierdzenia przybiera wtedy postać:

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k+1} S_k(A_1, \dots, A_n).$$

Twierdzenia dowodzimy przez indukcję względem n . Dla $n = 1$ twierdzenie jest oczywiste. Dla $n = 2$ i $n = 3$ było już udowodnione. Zakładamy teraz, że dla dowolnych n zbiorów (gdzie $n \geq 2$) twierdzenie jest prawdziwe i dowodzimy, że jest prawdziwe dla dowolnych $n+1$ zbiorów. Niech więc $A_1, \dots, A_{n+1}$ będą dowolnymi zbiorami skończonymi. Wówczas

$$\begin{aligned} |A_1 \cup \dots \cup A_{n+1}| &= |(A_1 \cup \dots \cup A_n) \cup A_{n+1}| = \\ &= |A_1 \cup \dots \cup A_n| + |A_{n+1}| - |(A_1 \cup \dots \cup A_n) \cap A_{n+1}| = \\ &= |A_1 \cup \dots \cup A_n| + |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup \dots \cup (A_n \cap A_{n+1})|. \end{aligned}$$

Korzystamy teraz dwukrotnie z założenia indukcyjnego: dla zbiorów $A_1, \dots, A_n$ oraz dla zbiorów $A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}$:

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k+1} S_k(A_1, \dots, A_n),$$

$$|(A_1 \cap A_{n+1}) \cup \dots \cup (A_n \cap A_{n+1})| = \sum_{k=1}^n (-1)^{k+1} S_k(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}).$$

Zauważmy następnie, że

$$\begin{aligned} |A_1 \cup \dots \cup A_n| + |A_{n+1}| &= S_1(A_1, \dots, A_n) + |A_{n+1}| + \sum_{k=2}^n (-1)^{k+1} S_k(A_1, \dots, A_n) = \\ &= |A_1| + \dots + |A_n| + |A_{n+1}| + \sum_{k=2}^n (-1)^{k+1} S_k(A_1, \dots, A_n) = \\ &= S_1(A_1, \dots, A_{n+1}) + \sum_{k=2}^n (-1)^{k+1} S_k(A_1, \dots, A_n) \end{aligned}$$

oraz

$$\begin{aligned} |(A_1 \cap A_{n+1}) \cup \dots \cup (A_n \cap A_{n+1})| &= \sum_{k=1}^n (-1)^{k+1} S_k(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) = \\ &= \sum_{k=1}^{n-1} (-1)^{k+1} S_k(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) + \\ &\quad + (-1)^{n+1} S_n(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) = \\ &= \sum_{k=1}^{n-1} (-1)^{k+1} S_k(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) + \\ &\quad + (-1)^{n+1} |(A_1 \cap A_{n+1}) \cap \dots \cap (A_n \cap A_{n+1})| = \\ &= \sum_{k=1}^{n-1} (-1)^{k+1} S_k(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) + (-1)^{n+1} |A_1 \cap \dots \cap A_n \cap A_{n+1}| = \\ &= \sum_{k=2}^n (-1)^k S_{k-1}(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) - (-1)^{n+2} |A_1 \cap \dots \cap A_n \cap A_{n+1}| = \\ &= \sum_{k=2}^n (-1)^k S_{k-1}(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) - (-1)^{n+2} S_{n+1}(A_1, \dots, A_{n+1}) = \\ &= - \sum_{k=2}^n (-1)^{k+1} S_{k-1}(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) - (-1)^{n+2} S_{n+1}(A_1, \dots, A_{n+1}). \end{aligned}$$

Zatem

$$|A_1 \cup \dots \cup A_n| = S_1(A_1, \dots, A_{n+1}) + \sum_{k=2}^n (-1)^{k+1} S_k(A_1, \dots, A_n) +$$

$$\begin{aligned}
& + \sum_{k=2}^n (-1)^{k+1} S_{k-1}(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) + (-1)^{n+2} S_{n+1}(A_1, \dots, A_{n+1}) = \\
& = S_1(A_1, \dots, A_{n+1}) + \sum_{k=2}^n (-1)^{k+1} (S_k(A_1, \dots, A_n) + S_{n+1}(A_1, \dots, A_{n+1})) + \\
& \quad + (-1)^{n+2} S_{n+1}(A_1, \dots, A_{n+1}).
\end{aligned}$$

Następnie zauważmy, że

$$S_k(A_1, \dots, A_n) + S_{k-1}(A_1 \cap A_{n+1}, \dots, A_n \cap A_{n+1}) = S_k(A_1, \dots, A_{n+1})$$

Stąd ostatecznie dostajemy

$$\begin{aligned}
& |A_1 \cup \dots \cup A_n| = \\
& = S_1(A_1, \dots, A_{n+1}) + \sum_{k=2}^n (-1)^{k+1} S_k(A_1, \dots, A_{n+1}) + (-1)^{n+2} S_{n+1}(A_1, \dots, A_{n+1}) = \\
& = \sum_{k=1}^{n+1} (-1)^{k+1} S_k(A_1, \dots, A_{n+1}),
\end{aligned}$$

co kończy dowód twierdzenia.

Wzór (2.3) nazywamy **wzorem włączeń i wyłączeń**.

Inny dowód. Przeglądamy kolejne składniki sumy stojącej po prawej stronie równości i przy każdym elemencie iloczynu $\bigcap_{j \in T} A_j$ rysujemy znak plus lub minus w zależności

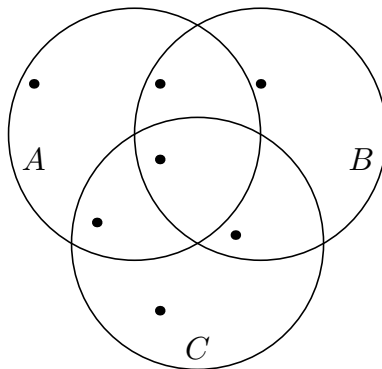
od tego, czy liczba $\left| \bigcap_{j \in T} A_j \right|$ występowała w sumie ze znakiem plus czy minus. Inaczej mówiąc, jeśli zbiór T ma nieparzystą liczbę elementów, to rysujemy znak plus; jeśli zaś zbiór T ma parzystą liczbę elementów, to rysujemy znak minus.

Zilustrujemy tę procedurę (w przypadku sumy trzech zbiorów $A \cup B \cup C$) serią rysunków. Dowodzimy równość

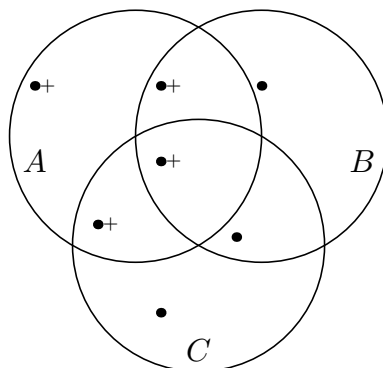
$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Przeglądamy składniki sumy po prawej stronie i rysujemy znaki plus kolejno przy każdym elemencie zbiorów A , B i C , potem znaki minus przy każdym elemencie zbiorów $A \cap B$, $A \cap C$ i $B \cap C$, wreszcie znaki plus przy każdym elemencie zbioru $A \cap B \cap C$.

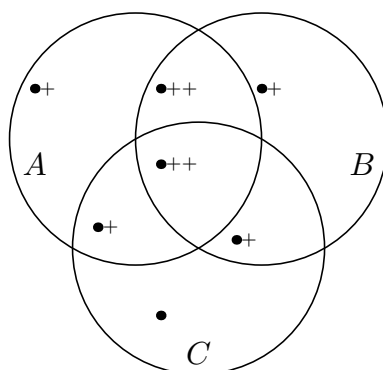
Rysunek 1: zbiory A , B i C wraz z zaznaczonymi przykładowymi elementami (po jednym elemencie w każdej składowej).



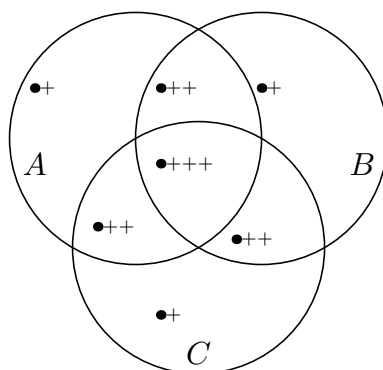
Rysunek 2: przy każdym elemencie zbioru A rysujemy znak plus



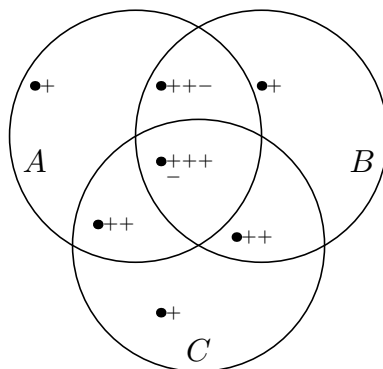
Rysunek 3: przy każdym elemencie zbioru B rysujemy znak plus



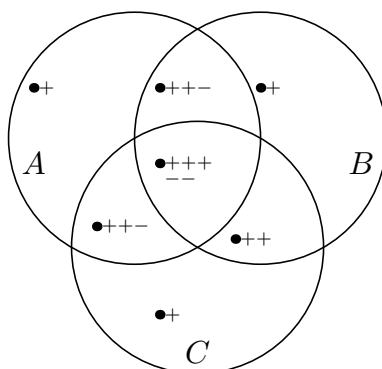
Rysunek 4: przy każdym elemencie zbioru C rysujemy znak plus



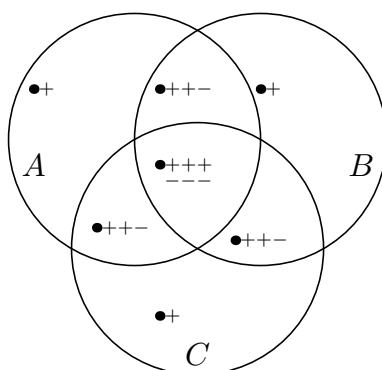
Rysunek 5: przy każdym elemencie zbioru $A \cap B$ rysujemy znak minus



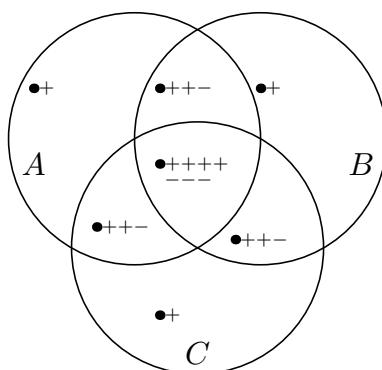
Rysunek 6: przy każdym elemencie zbioru $A \cap C$ rysujemy znak minus



Rysunek 7: przy każdym elemencie zbioru $B \cap C$ rysujemy znak minus



Rysunek 8: przy każdym elemencie zbioru $A \cap B \cap C$ rysujemy znak plus



Zauważamy, że przy każdym elemencie sumy $A \cup B \cup C$ liczba narysowanych plusów jest o jeden większa od liczby narysowanych minusów: przy elementach należących do jednego zbioru narysowaliśmy tylko jeden plus, przy elementach należących do dwóch zbiorów narysowaliśmy dwa plusy i jeden minus, wreszcie przy elementach należących do wszystkich trzech zbiorów narysowaliśmy cztery plusy i trzy minusy. To daje równość

$$(\text{liczba plusów}) - (\text{liczba minusów}) = |A \cup B \cup C|.$$

Nietrudno przy tym zauważyć, że w każdym z siedmiu powyższych kroków liczba narysowanych znaków była równa liczbie elementów rozpatrywanego zbioru. Stąd dostajemy równość

$$(\text{liczba plusów}) - (\text{liczba minusów}) = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|,$$

z której wynika równość (2.2).

Powróćmy do dowodu twierdzenia 2.1. Znów zauważamy, że prawa strona równości (2.3) jest różnicą między liczbą plusów i liczbą minusów. Wystarczy zatem pokazać, że przy każdym elemencie sumy zbiorów $A_1 \cup \dots \cup A_n$ narysowaliśmy o jeden plus więcej. Niech $x \in A_1 \cup \dots \cup A_n$. Niech następnie

$$M = \{j : x \in A_j\}.$$

Inaczej mówiąc, $x \in A_j$ wtedy i tylko wtedy, gdy $j \in M$. Oznaczmy $m = |M|$; oczywiście $m > 0$. Niech teraz $T \in P_k(n)$ i popatrzmy na zbiór $\bigcap_{j \in T} A_j$; jest to jeden ze zbiorów występujących po prawej stronie równości (2.3). Jeśli $T \setminus M \neq \emptyset$, to oczywiście mamy $x \notin \bigcap_{j \in T} A_j$. Przypuśćmy zatem, że $T \subseteq M$. Wtedy przy elemencie x rysowaliśmy znak plus lub minus, w zależności od parzystości k : plus dla nieparzystych k , minus dla parzystych k . Dla danego k liczba takich zbiorów T jest równa $\binom{m}{k}$. Liczby plusów i minusów narysowanych przy x są zatem równe

$$\text{liczba plusów} = \sum_{2 \nmid k} \binom{m}{k}.$$

$$\text{liczba minusów} = \sum_{k > 0, 2 \mid k} \binom{m}{k},$$

skąd dostajemy

$$\text{liczba plusów} - \text{liczba minusów} = \sum_{k=1}^m (-1)^{k+1} \binom{m}{k}.$$

Z równości (przypominamy, że $m > 0$)

$$\sum_{k=0}^m (-1)^k \binom{m}{k} = 0$$

wynika, że

$$\binom{m}{0} + \sum_{k=1}^m (-1)^k \binom{m}{k} = 0,$$

czyli

$$1 = - \sum_{k=1}^m (-1)^k \binom{m}{k} = \sum_{k=1}^m (-1)^{k+1} \binom{m}{k}.$$

Stąd wynika, że przy elemencie x narysowaliśmy o jeden plus więcej. Tak jest dla każdego elementu x sumy $A_1 \cup \dots \cup A_n$. To zaś oznacza, że suma po prawej stronie równości będzie równa liczbie elementów sumy $A_1 \cup \dots \cup A_n$, co kończy dowód.

3. Liczba funkcji z jednego zbioru skończonego na drugi zbiór skończony

Twierdzenie 2.2. Dane są dwa zbiory skończone A i B . Niech $|A| = m$ i $|B| = n$. Wtedy

$$|\{f \in A^B : f \text{ jest „na”}\}| = \sum_{k=0}^m (-1)^k \binom{m}{k} (m-k)^n. \quad (2.4)$$

Dowód. Bez zmniejszenia ogólności możemy przyjąć, że $A = [m]$ i $B = [n]$. Definiujemy zbiory $A_1, \dots, A_m$ w następujący sposób:

$$A_j = \{f \in A^B : j \notin R_f\}$$

dla $j = 1, 2, \dots, m$. Inaczej mówiąc

$$A_j = (A \setminus \{j\})^B.$$

Korzystając ze wzoru włączeń i wyłączeń otrzymujemy

$$|A_1 \cup \dots \cup A_m| = \sum_{k=1}^m (-1)^{k+1} \sum_{T \in P_k(m)} \left| \bigcap_{j \in T} A_j \right|.$$

Niech zatem $T \in P_k(m)$. Wtedy

$$\bigcap_{j \in T} A_j = \bigcap_{j \in T} (A \setminus \{j\})^B = (A \setminus T)^B,$$

skąd otrzymujemy

$$\left| \bigcap_{j \in T} A_j \right| = |(A \setminus T)^B| = (m-k)^n.$$

Zatem

$$|A_1 \cup \dots \cup A_m| = \sum_{k=1}^m (-1)^{k+1} \sum_{T \in P_k(m)} (m-k)^n = \sum_{k=1}^m (-1)^{k+1} \binom{m}{k} (m-k)^n.$$

Do zakończenia dowodu wystarczy zauważyć, że suma zbiorów $A_1 \cup \dots \cup A_m$ składa się z tych funkcji $f : B \rightarrow A$, które nie są „na”. Zatem

$$\{f \in A^B : f \text{ jest „na”}\} = A^B \setminus (A_1 \cup \dots \cup A_m),$$

czyli

$$\begin{aligned}
 |\{f \in A^B : f \text{ jest „na”}\}| &= m^n - |A_1 \cup \dots \cup A_m| = \\
 &= m^n - \sum_{k=1}^m (-1)^{k+1} \binom{m}{k} (m-k)^n = \\
 &= m^n + \sum_{k=1}^m (-1)^k \binom{m}{k} (m-k)^n = \\
 &= \sum_{k=0}^m (-1)^k \binom{m}{k} (m-k)^n,
 \end{aligned}$$

c. b. d. o.

4. Liczba nieporządków

Permutacją zbioru skończonego A nazywamy funkcję różnowartościową $\pi : A \rightarrow A$ przekształcającą zbiór A na siebie. **Punktem stałym** permutacji π nazywamy taki element a zbioru A , dla którego $\pi(a) = a$. **Nieporządkiem** nazywamy permutację bez punktów stałych. Zbiór wszystkich permutacji zbioru A oznaczmy symbolem $S(A)$, a zbiór nieporządków zbioru A symbolem $D(A)$.

Powyższa definicja permutacji nie jest identyczna z definicją przyjętą w wykładzie pierwszym. Pokażemy teraz, że w pewnym sensie te dwie definicje opisują te same obiekty kombinatoryczne. Przypuśćmy zatem, że mamy dany zbiór skończony A . Ustalmy pewne uporządkowanie tego zbioru:

$$A = \{a_1, a_2, \dots, a_n\}.$$

Niech $\pi : A \rightarrow A$ będzie permutacją zbioru A w sensie powyższej definicji. Przekształcenie π możemy wtedy utożsamić z ciągiem $(\pi(a_1), \pi(a_2), \dots, \pi(a_n))$ elementów zbioru A . Oczywiście ten ciąg jest różnowartościowy, a więc jest permutacją zbioru A w sensie definicji z wykładu pierwszego. Zwróćmy uwagę na to, że utożsamienie przekształcenia π z ciągiem elementów zbioru A jest zależne od przyjętego na początku uporządkowania zbioru A . Zauważmy też, że w przypadku, gdy $A = [n]$, obie definicje pokrywają się.

Niech wreszcie D_n oznacza liczbę nieporządków zbioru n -elementowego, to znaczy np. $D_n = D([n])$ dla $n > 0$. Przyjmujemy ponadto $D_0 = 1$.

Twierdzenie 2.3 Niech $|A| = n > 0$. Wtedy

$$D_n = |D(A)| = n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}. \quad (2.5)$$

Dowód. Definiujemy zbiory $A_1, \dots, A_n$ w następujący sposób:

$$A_j = \{\pi \in S(A) : \pi(j) = j\}$$

dla $j = 1, \dots, n$. Mamy wówczas

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|.$$

Niech teraz $T \in P_k(n)$. Wówczas

$$\bigcap_{j \in T} A_j = \bigcap_{j \in T} \{\pi : \pi(j) = j\} = \{\pi : \forall j \in T (\pi(j) = j)\} = \{\pi : \pi|_T = \text{id}\}.$$

Stąd wynika, że

$$\left| \bigcap_{j \in T} A_j \right| = (n - k)!$$

Zatem

$$\begin{aligned} |A_1 \cup \dots \cup A_n| &= \sum_{k=1}^n (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right| = \sum_{k=1}^n (-1)^{k+1} \sum_{T \in P_k(n)} (n - k)! = \\ &= \sum_{k=1}^n (-1)^{k+1} \binom{n}{k} \cdot (n - k)! = \sum_{k=1}^n (-1)^{k+1} \cdot \frac{n!}{k! \cdot (n - k)!} \cdot (n - k)! = \\ &= \sum_{k=1}^n (-1)^{k+1} \cdot \frac{n!}{k!}. \end{aligned}$$

Następnie zauważamy, że suma zbiorów $A_1 \cup \dots \cup A_n$ składa się z tych permutacji, które mają co najmniej jeden punkt stały. Zatem

$$D(A) = S(A) \setminus (A_1 \cup \dots \cup A_n),$$

skąd wynika, że

$$\begin{aligned} |D(A)| &= n! - |A_1 \cup \dots \cup A_n| = n! - \sum_{k=1}^n (-1)^{k+1} \cdot \frac{n!}{k!} = \\ &= n! + \sum_{k=1}^n (-1)^k \cdot \frac{n!}{k!} = \sum_{k=0}^n (-1)^k \cdot \frac{n!}{k!} = \\ &= n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}. \end{aligned}$$

To kończy dowód twierdzenia.

Z powyższego twierdzenia wyprowadzimy wniosek dotyczący prawdopodobieństwa wylosowania nieporządku. Przypuśćmy, że losujemy permutację ustalonego zbioru n -elementowego A i pytamy o to, jakie jest prawdopodobieństwo tego, że wylosujemy nieporządek. Zbiorem zdarzeń elementarnych Ω w tym przypadku jest zbiór $S(A)$ wszystkich permutacji zbioru A ; przyjmujemy, że wylosowanie każdej permutacji jest jednakowo prawdopodobne. Interesuje nas prawdopodobieństwo zdarzenia $D(A) \subseteq \Omega$. To prawdopodobieństwo jest równe

$$P(D(A)) = \frac{|D(A)|}{n!} = \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

Zauważmy, że

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

skąd wynika, że dla dużych n rozważane prawdopodobieństwo jest w przybliżeniu równe $e^{-1} \approx 0,367879$ (już dla $n = 9$ uzyskujemy dokładność przybliżenia 6 cyfr po przecinku).

5. Uogólnienie wzoru włączeń i wyłączeń

Przypuśćmy, że mamy dane zbiory skończone $A_1, \dots, A_n \subseteq X$, gdzie X jest ustalonym zbiorem skończonym. Przyjmiemy, że

$$\bigcap_{j \in \emptyset} A_j = X.$$

Korzystając z tej umowy, możemy wysłowić zasadę włączeń i wyłączeń w inny sposób. Zastanówmy się, ile elementów zbioru X nie należy do żadnego ze zbiorów $A_1, \dots, A_n$. Otóż mamy

$$\begin{aligned} |X \setminus (A_1 \cup \dots \cup A_n)| &= |X| - \sum_{k=1}^n (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right| = \\ &= \left| \bigcup_{j \in \emptyset} A_j \right| + \sum_{k=1}^n (-1)^k \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right| = \\ &= \sum_{k=0}^n (-1)^k \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \end{aligned}$$

Niech nadal $A_1, \dots, A_n \subseteq X$. Przyjmiemy wtedy oznaczenie:

$$D_r(X, A_1, \dots, A_n) = \{x \in X : |\{i \in [n] : x \in A_i\}| = r\},$$

gdzie $0 \leq r \leq n$. Inaczej mówiąc, $D_r(X, A_1, \dots, A_n)$ jest zbiorem tych elementów zbioru X , które należą do zbiorów A_i dla dokładnie r indeksów i . Jeśli zbiory $A_1, \dots, A_n$ są ponumerowane bez powtórzeń, to $D_r(X, A_1, \dots, A_n)$ jest zbiorem tych elementów zbioru X , które należą do dokładnie r zbiorów spośród $A_1, \dots, A_n$. W dalszym ciągu, będziemy pisać w skrócie, że element zbioru X należy do dokładnie r zbiorów spośród $A_1, \dots, A_n$, mając na myśli to, że istnieje dokładnie r indeksów i takich, że ten element należy do zbioru A_i .

Pokazaliśmy przed chwilą, że

$$|D_0(X, A_1, \dots, A_n)| = \sum_{k=0}^n (-1)^k \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.6)$$

Tę równość można uogólnić.

Twierdzenie 2.4 Niech $A_1, \dots, A_n$ będą skończonymi podzbiórmi zbioru skończonego X . Wówczas dla dowolnego $r = 0, 1, \dots, n$ mamy

$$|D_r(X, A_1, \dots, A_n)| = \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.7)$$

Dowód. Niech $R \in P_r(n)$. Wyznamy liczbę tych $x \in X$, które mają własność:

$$x \in A_j \quad \text{wtedy i tylko wtedy, gdy} \quad j \in R.$$

Inaczej mówiąc, wyznaczmy liczbę tych $x \in X$, które należą dokładnie do tych zbiorów A_j , dla których $j \in R$.

Niech

$$B = \bigcap_{j \in R} A_j \quad \text{oraz} \quad B_j = B \cap A_j$$

dla $j \notin R$. Naszym celem jest wyznaczenie liczby elementów zbioru

$$\bigcap_{j \notin R} (B \setminus B_j),$$

czyli obliczenie $D_0(B, B_{i_1}, \dots, B_{i_{n-r}})$, gdzie $[n] \setminus R = \{i_1, \dots, i_{n-r}\}$.

Ze wzoru (2.6) wynika, że

$$\begin{aligned} |D_0(B, B_{i_1}, \dots, B_{i_{n-r}})| &= \sum_{k=0}^{n-r} (-1)^k \sum_{T \in P_k([n] \setminus R)} \left| \bigcap_{j \in T} B_j \right| = \\ &= \sum_{k=0}^{n-r} \sum_{T \in P_k([n] \setminus R)} (-1)^k \left| \bigcap_{j \in T} (A_j \cap B) \right| = \\ &= \sum_{k=0}^{n-r} \sum_{T \in P_k([n] \setminus R)} (-1)^k \left| \bigcap_{j \in T} \left(A_j \cap \bigcap_{i \in R} A_i \right) \right| = \\ &= \sum_{k=0}^{n-r} \sum_{T \in P_k([n] \setminus R)} (-1)^k \left| \left(\bigcap_{i \in R} A_i \right) \cap \left(\bigcap_{j \in T} A_j \right) \right| = \\ &= \sum_{k=0}^{n-r} \sum_{T \in P_k([n] \setminus R)} (-1)^k \left| \bigcap_{j \in T \cup R} A_j \right| = \\ &= \sum_{k=0}^{n-r} \sum_{\substack{T \in P_{k+r}([n]) \\ R \subseteq T}} (-1)^k \left| \bigcap_{j \in T} A_j \right| = \\ &= \sum_{k=r}^n \sum_{\substack{T \in P_k([n]) \\ R \subseteq T}} (-1)^{k-r} \left| \bigcap_{j \in T} A_j \right| = \\ &= \sum_{\substack{T \\ R \subseteq T \subseteq [n]}} (-1)^{|T|-r} \left| \bigcap_{j \in T} A_j \right|. \end{aligned}$$

Dla ustalonego zbioru R obliczyliśmy, ile jest takich $x \in X$, które należą do dokładnie tych zbiorów A_j , dla których $j \in R$. Teraz chcemy obliczyć, ile jest takich x , które należą do dokładnie r zbiorów A_j (dokładniej: chcemy obliczyć, ile jest takich x , dla których $|\{i \in [n] : x \in A_i\}| = r$). W tym celu musimy zsumować otrzymane liczby dla wszystkich r -elementowych podzbiorów R zbioru $[n]$. Mamy zatem

$$\begin{aligned}
 |D_r(X, A_1, \dots, A_n)| &= \sum_{R \in P_r(n)} \sum_{\substack{T \subseteq [n] \\ |T|=r}} (-1)^{|T|-r} \left| \bigcap_{j \in T} A_j \right| = \\
 &= \sum_{T \in P_{\geq r}(n)} \sum_{R \in P_r(T)} (-1)^{|T|-r} \left| \bigcap_{j \in T} A_j \right| = \\
 &= \sum_{T \in P_{\geq r}(n)} \binom{|T|}{r} \cdot (-1)^{|T|-r} \left| \bigcap_{j \in T} A_j \right| = \\
 &= \sum_{k=r}^n \sum_{T \in P_k(n)} \binom{k}{r} \cdot (-1)^{k-r} \left| \bigcap_{j \in T} A_j \right| = \\
 &= \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|,
 \end{aligned}$$

co kończy dowód twierdzenia.

6. Liczba permutacji mających r punktów stałych

W tym paragrafie obliczymy, ile jest permutacji zbioru n -elementowego mających dokładnie r punktów stałych. Niech

$$D_r(A) = \{\pi \in S(A) : |\{i \in A : \pi(i) = i\}| = r\}.$$

W szczególności $D_0(A) = D(A)$.

Twierdzenie 2.5 Niech $|A| = n$ i niech $0 \leq r \leq n$. Wtedy

$$|D_r(A)| = \frac{n!}{r!} \cdot \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}. \quad (2.8)$$

Dowód. Sposób I. Wybieramy najpierw zbiór r punktów stałych permutacji, a następnie permutujemy pozostałe elementy tak, by nie utworzyć nowego punktu stałego; inaczej mówiąc permutacja pozostałych elementów jest nieporządkiem. Stąd wynika wzór

$$D_r(A) = \binom{n}{r} \cdot D_{n-r} = \frac{n!}{r! \cdot (n-r)!} \cdot (n-r)! \cdot \sum_{k=0}^{n-r} \frac{(-1)^k}{k!} = \frac{n!}{r!} \cdot \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}.$$

Sposób II. Korzystamy z twierdzenia 2.4. Definiujemy zbiory $A_1, \dots, A_n$ w następujący sposób:

$$A_j = \{\pi \in S(A) : \pi(j) = j\}$$

dla $j = 1, \dots, n$. Tak jak w dowodzie twierdzenia 2.3 stwierdzamy, że dla $T \subseteq [n]$ zachodzi równość

$$\left| \bigcap_{j \in T} A_j \right| = (n - k)!$$

Z twierdzenia 2.4 otrzymujemy teraz

$$\begin{aligned} |D_r(A)| &= D_r(S(A), A_1, \dots, A_n) = \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right| = \\ &= \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{T \in P_k(n)} (n - k)! = \\ &= \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \binom{n}{k} (n - k)! = \\ &= \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \frac{n!}{k! \cdot (n - k)!} \cdot (n - k)! = \\ &= \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \frac{n!}{k!} = \\ &= \sum_{k=r}^n (-1)^{k-r} \cdot \frac{k!}{r! \cdot (k - r)!} \cdot \frac{n!}{k!} = \\ &= \sum_{k=r}^n (-1)^{k-r} \cdot \frac{n!}{r! \cdot (k - r)!} = \\ &= \frac{n!}{r!} \cdot \sum_{k=r}^n (-1)^{k-r} \cdot \frac{1}{(k - r)!} = \\ &= \frac{n!}{r!} \cdot \sum_{k=0}^{n-r} (-1)^k \cdot \frac{1}{k!}, \end{aligned}$$

co kończy dowód twierdzenia.

7. Średnia liczba punktów stałych

Niech $|A| = n$. Przypuśćmy, że wybieramy losowo jedną permutację ze zbioru $S(A)$. Oznaczmy przez p_r prawdopodobieństwo tego, że wylosowana permutacja będzie miała dokładnie r punktów stałych. Z twierdzenia 2.5 wynika, że

$$p_r = \frac{D_r(A)}{n!} = \frac{1}{r!} \cdot \sum_{k=0}^{n-r} (-1)^k \cdot \frac{1}{k!}.$$

Niech zmienna losowa X będzie określona wzorem

$$X(\pi) = |\{j \in A : \pi(j) = j\}|.$$

Zatem $X(\pi)$ jest liczbą punktów stałych permutacji π . W tym paragrafie obliczymy wartość średnią zmiennej X .

Z definicji wartości średniej mamy

$$E(X) = \sum_{r=0}^n r \cdot p_r.$$

Mamy zatem

$$\begin{aligned} E(X) &= \sum_{r=0}^n r \cdot p_r = \sum_{r=1}^n r \cdot p_r = \sum_{r=1}^n r \cdot \frac{1}{r!} \cdot \sum_{k=0}^{n-r} (-1)^k \cdot \frac{1}{k!} = \\ &= \sum_{r=1}^n \frac{1}{(r-1)!} \cdot \sum_{k=0}^{n-r} (-1)^k \cdot \frac{1}{k!} = \sum_{r=1}^n \sum_{k=0}^{n-r} \frac{(-1)^k}{(r-1)! \cdot k!}. \end{aligned}$$

Korzystamy teraz ze wzoru

$$\sum_{r=1}^n \sum_{k=0}^{n-r} a_{r,k} = \sum_{j=1}^n \sum_{r=1}^j a_{r,j-r}.$$

Mamy zatem

$$\begin{aligned} E(X) &= \sum_{r=1}^n \sum_{k=0}^{n-r} \frac{(-1)^k}{(r-1)! \cdot k!} = \sum_{j=1}^n \sum_{r=1}^j \frac{(-1)^{j-r}}{(r-1)! \cdot (j-r)!} = \\ &= \sum_{j=1}^n \sum_{r=1}^j \frac{(-1)^{j-r} \cdot (j-1)!}{(j-1)! \cdot (r-1)! \cdot (j-r)!} = \sum_{j=1}^n \sum_{r=1}^j \frac{(-1)^{j-r}}{(j-1)!} \cdot \frac{(j-1)!}{(r-1)! \cdot (j-r)!} = \\ &= \sum_{j=1}^n \sum_{r=1}^j \frac{(-1)^{j-r}}{(j-1)!} \cdot \binom{j-1}{r-1} = \sum_{j=1}^n \sum_{r=0}^{j-1} \frac{(-1)^{j-r-1}}{(j-1)!} \cdot \binom{j-1}{r} = \\ &= \sum_{j=1}^n \sum_{r=0}^{j-1} \frac{(-1)^{j+r-1}}{(j-1)!} \cdot \binom{j-1}{r} = \sum_{j=1}^n \frac{(-1)^{j-1}}{(j-1)!} \cdot \sum_{r=0}^{j-1} (-1)^r \cdot \binom{j-1}{r} \\ &= \sum_{j=0}^{n-1} \frac{(-1)^j}{j!} \cdot \sum_{r=0}^j (-1)^r \cdot \binom{j}{r}. \end{aligned}$$

Korzystamy teraz z równości

$$\sum_{r=0}^j (-1)^r \cdot \binom{j}{r} = \begin{cases} 1 & \text{jeśli } j = 0, \\ 0 & \text{jeśli } j > 0. \end{cases}$$

Stąd ostatecznie

$$E(X) = \sum_{j=0}^{n-1} \frac{(-1)^j}{j!} \cdot \sum_{r=0}^j (-1)^r \cdot \binom{j}{r} = \frac{(-1)^0}{0!} = 1.$$

Średnią liczbę punktów stałych permutacji można obliczyć znacznie prościej, korzystając z następującej własności wartości średniej zmiennych losowych:

$$E(X_1 + \dots + X_n) = E(X_1) + \dots + E(X_n).$$

Zdefiniujmy teraz n zmiennych losowych $X_1, \dots, X_n$:

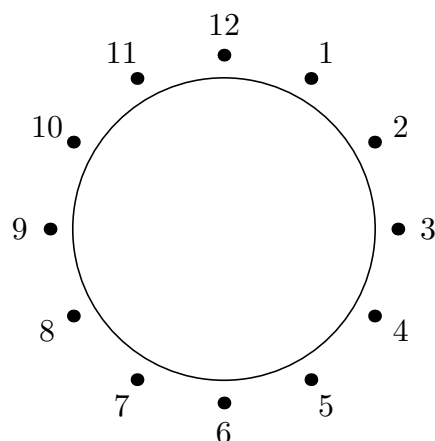
$$X_i(\pi) = \begin{cases} 1 & \text{jeśli } \pi(i) = i, \\ 0 & \text{jeśli } \pi(i) \neq i. \end{cases}$$

Nietrudno zauważyć, że wtedy $X = X_1 + \dots + X_n$, gdzie X jest zmienną losową zdefiniowaną wyżej. Następnie łatwo obliczyć, że $E(X_i) = P(X = 1) = \frac{1}{n}$. Stąd dostajemy

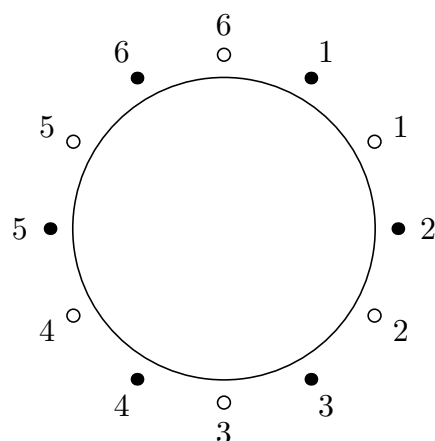
$$E(X) = E(X_1) + \dots + E(X_n) = n \cdot \frac{1}{n} = 1.$$

8. Problem par małżeńskich

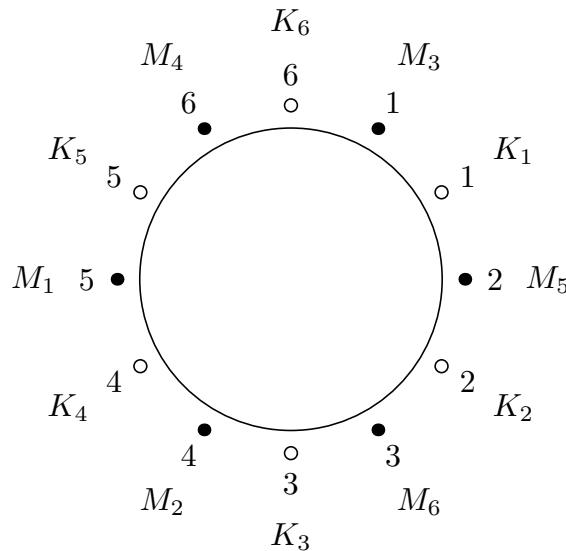
W tym paragrafie rozwiążemy następujący problem pochodzący od Lucasa (*le problème des ménages*). Dany jest okrągły stół, wokół którego mamy posadzić na numerowanych miejscach n par małżeńskich w taki sposób, by panie i panowie siedzieli naprzemian i by żadna pani nie siedziała obok swojego męża. Lucas pytał o to, na ile sposobów możemy te osoby posadzić wokół stołu z zachowaniem podanych reguł. Popatrzmy najpierw na przykład. Oto okrągły stół z 12 miejscami (a więc tutaj $n = 6$):



Przed wszystkim widzimy, że panie muszą zająć albo miejsca parzyste, albo nieparzyste. Ponumerujmy więc oddzielnie liczbami od 1 do 6 miejsca parzyste i nieparzyste:



Najpierw posadzimy panie. Ich miejsca możemy wybrać na $2 \cdot n!$ sposobów: musimy zdecydować, czy wybieramy miejsca parzyste, czy nieparzyste, a następnie na wybranych miejscach mamy $n!$ możliwości posadzenia n pań. Ponumerujmy panie: $K_1, K_2, \dots, K_n$, przy czym przyjmujemy, że pani K_i siedzi na miejscu i . Dla ustalenia uwagi przypuścimy, że panie posadziliśmy na miejscach parzystych, czyli białych na rysunku drugim. Ponumerujmy następnie panów: $M_1, M_2, \dots, M_n$, przy czym zakładamy, że pan M_i jest mężem pani K_i . Przykładowy sposób posadzenia n panów widzimy na następnym rysunku:



Widzimy, że usadzenie panów jest zgodne z wymaganiami, jeśli spełnione są następujące warunki:

- pan M_1 nie siedzi na żadnym z miejsc 1 i 2,
- pan M_2 nie siedzi na żadnym z miejsc 2 i 3,
- pan M_3 nie siedzi na żadnym z miejsc 3 i 4,
- pan M_4 nie siedzi na żadnym z miejsc 4 i 5,
- pan M_5 nie siedzi na żadnym z miejsc 5 i 6,
- pan M_6 nie siedzi na żadnym z miejsc 6 i 1.

Ogólnie dla n par warunki te możemy sformułować w trzech punktach:

- żaden z panów M_i (dla $i = 1, \dots, n$) nie może siedzieć na miejscu i ,
- żaden z panów M_i (dla $i = 1, \dots, n-1$) nie może siedzieć na miejscu $i+1$,
- pan M_n nie może siedzieć na miejscu 1,

Niech teraz $\pi(i)$ oznacza numer miejsca, na którym siedzi pan M_i . Naszym celem jest znalezienie liczby $\mu(n)$ permutacji $\pi \in S([n])$, spełniających następujące warunki:

- 1) $\pi(i) \neq i$ dla $i = 1, \dots, n$,
- 2) $\pi(i) \neq i+1$ dla $i = 1, \dots, n-1$,
- 3) $\pi(n) \neq 1$.

Liczba $M(n)$ wszystkich możliwych sposobów posadzenia n par małżeńskich będzie równa

$$M(n) = 2 \cdot n! \cdot \mu(n). \quad (2.9)$$

Definiujemy $2n$ zbiorów:

$$\begin{aligned} A_{2i-1} &= \{\pi \in S([n]) : \pi(i) = i\} \quad \text{dla } i = 1, \dots, n, \\ A_{2i} &= \{\pi \in S([n]) : \pi(i) = i + 1\} \quad \text{dla } i = 1, \dots, n - 1, \\ A_{2n} &= \{\pi \in S([n]) : \pi(n) = 1\}. \end{aligned}$$

Wówczas

$$\mu(n) = |S([n]) \setminus (A_1 \cup \dots \cup A_{2n})| = D_0(S([n]), A_1, \dots, A_{2n}) = \sum_{k=0}^{2n} (-1)^k \sum_{T \in P_k(2n)} \left| \bigcap_{j \in T} A_j \right|$$

Niech $T \in P_k(2n)$. Chcemy obliczyć

$$\left| \bigcap_{j \in T} A_j \right|.$$

Zauważmy, że

$$\bigcap_{j \in T} A_j = \emptyset,$$

wtedy i tylko wtedy, gdy spełniony jest co najmniej jeden z trzech warunków:

- 1) $2i - 1, 2i \in T$ dla pewnego $i = 1, \dots, n$,
- 2) $2i, 2i + 1 \in T$ dla pewnego $i = 1, \dots, n - 1$,
- 3) $1, 2n \in T$.

Przypuśćmy bowiem, że

$$\pi \in \bigcap_{j \in T} A_j$$

oraz spełniony jest warunek pierwszy dla pewnego i . Wtedy $\pi \in A_{2i-1} \cap A_{2i}$, czyli $\pi(i) = i$ oraz $\pi(i) = i + 1$, co jest niemożliwe. Podobnie, jeśli spełniony jest warunek drugi dla pewnego i , to $\pi \in A_{2i} \cap A_{2i+1}$, czyli $\pi(i) = i + 1$ oraz $\pi(i + 1) = i + 1$. To także jest niemożliwe. Wreszcie, jeśli $1, 2n \in T$, to $\pi \in A_1 \cap A_{2n}$, czyli $\pi(1) = 1$ oraz $\pi(n) = 1$, co także jest niemożliwe. Na odwrót, jeśli żaden z tych trzech warunków nie jest spełniony, czyli w zbiorze T nie występują dwie kolejne liczby (liczby $2n$ i 1 traktujemy tu jako liczby kolejne), to w permutacji π mamy ustalone k wartości. Takie permutacje istnieją i jest ich $(n - k)!$. Zauważmy, że wtedy oczywiście $k \leq n$.

Wprowadźmy na użytek tego dowodu następujące oznaczenia. Oznaczmy przez $g(n, k)$ liczbę takich zbiorów $B \in P_k(n)$, że:

- a) jeśli $i \in B$, to $i + 1 \notin B$ dla $i = 1, \dots, n - 1$,
- b) jeśli $n \in B$, to $1 \notin B$.

Oznaczmy następnie przez $h(n, k)$ liczbę zbiorów $B \in P_k(n)$ spełniających tylko powyższy warunek a):

- a) jeśli $i \in B$, to $i + 1 \notin B$ dla $i = 1, \dots, n - 1$,

Wtedy

$$\mu(n) = \sum_{k=0}^n (-1)^k \cdot (n-k)! \cdot g(2n, k). \quad (2.10)$$

Naszym celem jest zatem obliczenie $g(2n, k)$.

Lemat 2.6. $h(n, k) = \binom{n-k+1}{k}$.

Dowód. Sposób I. Mamy policzyć, ile jest k -elementowych podzbiorów zbioru $[n]$ nie zawierających dwóch kolejnych liczb. Każdy k -elementowy podzbiór zbioru $[n]$ jest zbiorem wartości dokładnie jednej funkcji rosnącej $f : [k] \rightarrow [n]$. Warunek, że ten podzbiór nie zawiera dwóch kolejnych liczb jest równoważny następującej własności funkcji f :

$$f(i+1) - f(i) \geq 2 \quad \text{dla } i = 1, 2, \dots, n-1. \quad (*)$$

Dla dowolnej funkcji $f : [k] \rightarrow [n]$ definiujemy funkcję $g : [k] \rightarrow [n-k+1]$ wzorem

$$g(i) = f(i) - i + 1$$

dla $i = 1, 2, \dots, k$. Mamy zatem

$$\begin{aligned} g(1) &= f(1), \\ g(2) &= f(2) - 1, \\ g(3) &= f(3) - 2, \\ &\dots \dots \\ g(k-1) &= f(k-1) - (k-2), \\ g(k) &= f(k) - (k-1). \end{aligned}$$

Nietrudno zauważyć, że funkcja f spełnia warunek $(*)$ wtedy i tylko wtedy, gdy funkcja g jest rosnąca. Zatem funkcji $f : [k] \rightarrow [n]$ spełniających warunek $(*)$ jest tyle, ile funkcji rosnących $g : [k] \rightarrow [n-k+1]$, a więc $\binom{n-k+1}{k}$.

Sposób II. Rozumowanie będziemy ilustrować przykładem, w którym $n = 13$ i $k = 4$. Narysujmy w jednej linii $n-k$ kółeczek.

○ ○ ○ ○ ○ ○ ○ ○ ○ ○

Tworzą one $n-k+1$ (w naszym przykładzie $n-k+1 = 10$) wolnych miejsc: jedno przed wszystkimi kółeczkami, $n-k-1$ miejsc między kolejnymi kółeczkami i jedno na końcu, za wszystkimi kółeczkami. Z tych $n-k+1$ miejsc wybierzmy k miejsc (w naszym przykładzie będzie to miejsce pierwsze, miejsce między trzecim i czwartym kółkiem, miejsce między siódmym i ósmym kółkiem oraz miejsce między ósmym i dziewiątym kółkiem) i wstawmy w nie czarne kółka:

● ○ ○ ○ ● ○ ○ ○ ○ ● ○ ● ○

Mamy razem n kółek, w tym k czarnych. Sposób wstawiania gwarantuje, że żadne dwa czarne kółka nie będą stały obok siebie. Taki ciąg kółek koduje podzbiór zbioru $[n]$:

$$\{i \in [n] : \text{na } i\text{-tym miejscu stoi czarne kółko}\}.$$

W naszym przykładzie jest to zbiór $\{1, 5, 10, 12\}$. Zauważmy wreszcie, że czarne kółka możemy wstawić na $\binom{n-k+1}{k}$ sposobów, co kończy dowód lematu.

Lemat 2.7. $g(n, k) = \frac{n}{n-k} \cdot \binom{n-k}{k}$.

Dowód. Zliczamy zbiory $B \in P_k(n)$ spełniające warunki a) i b).

Najpierw zajmujemy się takimi zbiorami B , że $1 \in B$. Wtedy $2 \notin B$ oraz $n \notin B$. Ponadto zbiór $B \setminus \{1\} \in P_{k-1}(\{3, \dots, n-1\})$ spełnia warunek a). Stąd wynika, że istnieje $h(n-3, k-1)$ takich zbiorów B .

Zajmijmy się następnie takimi zbiorami B , że $1 \notin B$. Wtedy zbiór $B \in P_k(\{2, \dots, n\})$ spełnia warunek a). Istnieje zatem $h(n-1, k)$ takich zbiorów B . Zatem

$$\begin{aligned} g(n, k) &= h(n-3, k-1) + h(n-1, k) = \\ &= \binom{n-k-1}{k-1} + \binom{n-k}{k} = \\ &= \frac{k}{n-k} \cdot \binom{n-k}{k} + \binom{n-k}{k} = \\ &= \frac{n}{n-k} \cdot \binom{n-k}{k}, \end{aligned}$$

c. b. d. o.

Twierdzenie 2.8. Liczba sposobów posadzenia n par małżeńskich przy okrągłym stole jest równa

$$M(n) = 2 \cdot n! \cdot \sum_{k=0}^n (-1)^k \cdot \frac{2n}{2n-k} \cdot \binom{2n-k}{k} \cdot (n-k)! \quad (2.11)$$

Dowód. Z równości (2.9) i (2.10) wynika, że liczba sposobów posadzenia n par małżeńskich przy okrągłym stole jest równa

$$M(n) = 2 \cdot n! \cdot \mu(n) = 2 \cdot n! \cdot \sum_{k=0}^n (-1)^k \cdot (n-k)! \cdot g(2n, k).$$

Korzystając z lematu 2.7 otrzymujemy

$$M(n) = 2 \cdot n! \cdot \sum_{k=0}^n (-1)^k \cdot \frac{2n}{2n-k} \cdot \binom{2n-k}{k} \cdot (n-k)!,$$

c. b. d. o.

9. Sumy potęg liczb naturalnych

Przypomnijmy z wykładu 1 oznaczenie

$$S_k(n) = \sum_{j=1}^n j^k = 1^k + \dots + n^k,$$

gdzie $n, k \geq 1$. Z wykładu 1 wiemy, że

$$\begin{aligned} S_0(n) &= n, \\ S_1(n) &= \binom{n+1}{2} = \frac{n(n+1)}{2}, \\ S_2(n) &= \frac{1}{4} \cdot \binom{2n+2}{3} = \frac{n(n+1)(2n+1)}{6}, \\ S_3(n) &= \binom{n+1}{2}^2 = S_1(n)^2 = \frac{n^2(n+1)^2}{4}. \end{aligned}$$

Wyprowadzimy teraz pewien wzór ogólny. Będzie to wzór rekurencyjny, pozwalający obliczyć $S_k(n)$, jeśli są znane wszystkie $S_j(n)$ dla $j < k$.

Twierdzenie 2.9. Jeśli $n, k \geq 1$, to

$$n^k = \sum_{j=1}^k (-1)^{j+1} \binom{k}{j} S_{k-j}(n). \quad (2.12)$$

Zanim udowodnimy to twierdzenie, przyjrzymy się jego początkowym przypadkom i pokażemy, jak z niego można otrzymać wzory na $S_k(n)$ dla $k \leq 3$. Oczywiście

$$S_0(n) = 1^0 + \dots + n^0 = n.$$

Teraz, korzystając z twierdzenia 2.9 dla $k = 2$ mamy

$$n^2 = \sum_{j=1}^2 (-1)^{j+1} \binom{2}{j} S_{2-j}(n) = \binom{2}{1} S_1(n) - \binom{2}{2} S_0(n) = 2S_1(n) - n,$$

skąd otrzymujemy

$$2S_1(n) = n^2 + n = n(n+1),$$

czyli

$$S_1(n) = \frac{n(n+1)}{2}.$$

Następnie, dla $k = 3$ mamy

$$\begin{aligned} n^3 &= \sum_{j=1}^3 (-1)^{j+1} \binom{3}{j} S_{3-j}(n) = \binom{3}{1} S_2(n) - \binom{3}{2} S_1(n) + \binom{3}{3} S_0(n) = \\ &= 3S_2(n) - 3 \cdot \frac{n(n+1)}{2} + n, \end{aligned}$$

skąd dostajemy

$$\begin{aligned} 3S_2(n) &= n^3 + 3 \cdot \frac{n(n+1)}{2} - n = \frac{2n^3 + 3n(n+1) - 2n}{2} = \\ &= \frac{2n^3 + 3n^2 + 3n - 2n}{2} = \frac{n(2n^2 + 3n + 1)}{2} = \\ &= \frac{n(n+1)(2n+1)}{2}, \end{aligned}$$

czyli

$$S_2(n) = \frac{n(n+1)(2n+1)}{6}.$$

Wreszcie dla $n = 4$ mamy

$$\begin{aligned} n^4 &= \sum_{j=1}^4 (-1)^{j+1} \binom{4}{j} S_{4-j}(n) = \\ &= \binom{4}{1} S_3(n) - \binom{4}{2} S_2(n) + \binom{4}{3} S_1(n) - \binom{4}{4} S_0(n) = \\ &= 4S_3(n) - 6 \cdot \frac{n(n+1)(2n+1)}{6} + 4 \cdot \frac{n(n+1)}{2} - n = \\ &= 4S_3(n) - n(n+1)(2n+1) + 2n(n+1) - n, \end{aligned}$$

skąd wynika, że

$$\begin{aligned} 4S_3(n) &= n^4 + n(n+1)(2n+1) - 2n(n+1) + n = \\ &= n \cdot (n^3 + (n+1)(2n+1) - 2(n+1) + 1) = \\ &= n \cdot ((n^3 + 1) + (n+1)(2n+1-2)) = \\ &= n \cdot ((n+1)(n^2 - n + 1) + (n+1)(2n-1)) = \\ &= n(n+1)(n^2 - n + 1 + 2n - 1) = n(n+1)(n^2 + n) = \\ &= n^2(n+1)^2, \end{aligned}$$

czyli

$$S_3(n) = \frac{n^2(n+1)^2}{4}.$$

Udowodnimy teraz twierdzenie 2.9.

Dowód. Weźmy zbiór

$$X = [n]^k = \{(x_1, \dots, x_k) : x_1, \dots, x_k \in [n]\}.$$

Wtedy oczywiście $|X| = n^k$. Definiujemy teraz następujące podzbiory zbioru X :

$$A_m = \{(x_1, \dots, x_k) \in X : \forall i (x_i \leq x_m)\}$$

dla $m = 1, \dots, k$. Inaczej mówiąc, do zbioru A_m należą te ciągi, w których największy wyraz znajduje się na m -tym miejscu. Oczywiście ciągi mające największy wyraz na kilku miejscach, należą do kilku takich zbiorów A_m . Na przykład, jeśli $n = 5$ i $k = 7$, to $(1, 3, 4, 2, 5, 4, 2) \in A_5$ oraz $(1, 3, 4, 2, 1, 4, 2) \in A_3 \cap A_6$. Ogólnie, niech $T \in P_j(k)$, gdzie $1 \leq j \leq k$. Wtedy

$$\bigcap_{m \in T} A_m = \bigcup_{l=1}^n \{(x_1, \dots, x_k) \in X : \forall m \in T (x_m = l) \text{ oraz } \forall m \in [k] \setminus T (x_m \leq l)\}.$$

Zauważmy następnie, że

$$|\{(x_1, \dots, x_k) \in X : \forall m \in T (x_m = l) \text{ oraz } \forall m \in [k] \setminus T (x_m \leq l)\}| = l^{k-j}$$

oraz zbiory

$$\{(x_1, \dots, x_k) \in X : \forall m \in T (x_m = l) \text{ oraz } \forall m \in [k] \setminus T (x_m \leq l)\}$$

dla różnych l są rozłączne. Zatem

$$\left| \bigcap_{m \in T} A_j \right| = \sum_{l=1}^n l^{k-j} = S_{k-j}(n).$$

Wreszcie

$$X = A_1 \cup \dots \cup A_k,$$

a więc z zasady włączeń i wyłączeń otrzymujemy

$$\begin{aligned} |X| &= \sum_{j=1}^k (-1)^{j+1} \sum_{T \in P_j(k)} \left| \bigcap_{m \in T} A_m \right| = \\ &= \sum_{j=1}^k (-1)^{j+1} \sum_{T \in P_j(k)} S_{k-j}(n) = \\ &= \sum_{j=1}^k (-1)^{j+1} \binom{k}{j} S_{k-j}(n), \end{aligned}$$

czyli

$$n^k = \sum_{j=1}^k (-1)^{j+1} \binom{k}{j} S_{k-j}(n),$$

c. b. d. o.

10. Dwie tożsamości

Rozważania tego paragrafu będą w zasadzie powtórzeniem rozważań z paragrafu 3. Zajmiemy się funkcjami $f : [n] \rightarrow [m]$ i będziemy chcieli policzyć funkcje f spełniające dla pewnego k warunek $[k] \subseteq R_f$. Definiujemy zbiory $A_1, \dots, A_k$ w następujący sposób:

$$A_j = \{f \in [m]^{[n]} : j \notin R_f\}$$

dla $j = 1, \dots, k$. Korzystając ze wzoru włączeń i wyłączeń, podobnie jak w paragrafie 3, otrzymujemy

$$\begin{aligned} |A_1 \cup \dots \cup A_k| &= \sum_{j=1}^k (-1)^{j+1} \sum_{T \in P_j(k)} \left| \bigcap_{i \in T} A_i \right| = \sum_{j=1}^k (-1)^{j+1} \sum_{T \subseteq P_j(k)} (m-j)^n = \\ &= \sum_{j=1}^k (-1)^{j+1} \binom{k}{j} (m-j)^n. \end{aligned}$$

Funkcje, które nas interesują, tworzą zbiór $[m]^{[n]} \setminus (A_1 \cup \dots \cup A_k)$. Zatem liczba takich funkcji jest równa

$$m^n - \sum_{j=1}^k (-1)^{j+1} \binom{k}{j} (m-j)^n = \sum_{j=0}^k (-1)^j \binom{k}{j} (m-j)^n.$$

W szczególności, jeśli $k = n$ oraz $m \geq n$, to istnieje $n!$ takich funkcji. Zatem

$$\sum_{j=0}^n (-1)^j \binom{n}{j} (m-j)^n = n! \quad \text{dla } m \geq n. \quad (2.13)$$

Zdefiniujmy teraz wielomian $W(x)$ wzorem

$$W(x) = \sum_{k=0}^n (-1)^k \binom{n}{k} (x-k)^n.$$

Jest to wielomian stopnia co najwyżej n . Z tożsamości (2.13) wynika jednak, że tę samą wartość $n!$ przyjmuje on w nieskończenie wielu punktach:

$$W(m) = n! \quad \text{dla } m \geq n.$$

Stąd wynika, że ten wielomian jest wielomianem stałym, czyli

$$\sum_{k=0}^n (-1)^k \binom{n}{k} (x-k)^n = n! \quad (2.14)$$

Z rozumowaniem, które przeprowadziliśmy, pozwalającym przejść od tożsamości udowodnionej dla liczb naturalnych do równości wielomianów, spotkamy się jeszcze w następnych wykładach.

11. Nierówności Bonferroniego

Udowodnimy teraz dwie nierówności, zwane **nierównościami Bonferroniego**. Oto one:

$$|A_1 \cup \dots \cup A_n| \geq \sum_{k=1}^{2r} (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right| \quad (2.15)$$

oraz

$$|A_1 \cup \dots \cup A_n| \leq \sum_{k=1}^{2r+1} (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.16)$$

Powtarzamy drugi dowód zasady włączeń i wyłączeń polegający na przeglądaniu kolejnych składników sumy stojącej po prawej stronie nierówności i rysowaniu przy każdym elemencie iloczynu $\bigcap_{j \in T} A_j$ znaku plus lub minus w zależności od tego, czy liczba $\left| \bigcap_{j \in T} A_j \right|$

występuje w sumie ze znakiem plus czy minus. Inaczej mówiąc, jeśli zbiór T ma nieparzystą liczbę elementów, to rysujemy znak plus; jeśli zaś zbiór T ma parzystą liczbę elementów, to rysujemy znak minus.

Tak jak w poprzednim dowodzie zauważamy, że prawa strona równości (2.3) jest różnicą między liczbą plusów i liczbą minusów. Musimy zatem oszacować różnicę między liczbą plusów i minusów narysowanych przy każdym elemencie sumy zbiorów $A_1 \cup \dots \cup A_n$.

Zajmiemy się najpierw nierównością (2.15). Mamy teraz pokazać, że przy każdym elemencie sumy zbiorów $A_1 \cup \dots \cup A_n$ narysowaliśmy co najwyżej o jeden plus więcej. Niech $x \in A_1 \cup \dots \cup A_n$. Tak jak poprzednio, niech

$$M = \{j : x \in A_j\}.$$

Inaczej mówiąc, $x \in A_j$ wtedy i tylko wtedy, gdy $j \in M$. Oznaczmy $m = |M|$; oczywiście $m > 0$. Niech teraz $T \in P_k(n)$ i popatrzmy na zbiór $\bigcap_{j \in T} A_j$; jest to jeden ze zbiorów występujących po prawej stronie równości (2.3). Jeśli $T \setminus M \neq \emptyset$, to oczywiście mamy $x \notin \bigcap_{j \in T} A_j$. Przypuśćmy zatem, że $T \subseteq M$. Wtedy przy elemencie x rysowaliśmy znak plus lub minus, w zależności od parzystości k : plus dla nieparzystych k , minus dla parzystych k . Dla danego k liczba takich zbiorów T jest równa $\binom{m}{k}$. Liczby plusów i minusów narysowanych przy x są zatem równe

$$\begin{aligned} \text{liczba plusów} &= \sum_{k=1}^r \binom{m}{2k}, \\ \text{liczba minusów} &= \sum_{k=1}^r \binom{m}{2k-1}, \end{aligned}$$

skąd dostajemy

$$\text{liczba plusów} - \text{liczba minusów} = \sum_{k=1}^{2r} (-1)^{k+1} \binom{m}{k}.$$

Tym razem korzystamy z równości (1.27) (przypominamy, że $m > 0$):

$$\sum_{k=0}^{2r} (-1)^k \binom{m}{k} = (-1)^{2r} \binom{m-1}{2r} = \binom{m-1}{2r}.$$

Mamy teraz dwie możliwości. Jeśli $m-1 < 2r$, czyli $m \leq 2r$ (tzn. element x należy do co najwyżej $2r$ zbiorów A_j), to tak jak poprzednio

$$\text{liczba plusów} - \text{liczba minusów} = 0.$$

Jeśli zaś $m > 2r$, to

$$\binom{m-1}{2r} \geq 1$$

skąd wynika, że

$$\binom{m}{0} + \sum_{k=1}^{2r} (-1)^k \binom{m}{k} \geq 1,$$

czyli

$$\sum_{k=1}^{2r} (-1)^k \binom{m}{k} \geq 0.$$

Zatem

$$\sum_{k=1}^{2r} (-1)^{k+1} \binom{m}{k} = - \sum_{k=1}^{2r} (-1)^k \binom{m}{k} \leq 0.$$

Stąd wynika, że przy elemencie x narysowaliśmy co najwyżej tyle plusów, ile minusów. Zatem dla każdego elementu x sumy $A_1 \cup \dots \cup A_n$ w obu przypadkach narysowaliśmy co najwyżej o jeden plus więcej, co dowodzi nierówności (2.15). Dowód nierówności (2.16) jest analogiczny i pozostawimy go jako ćwiczenie.

Z powyższego dowodu wynika, że jeśli każdy element sumy $A_1 \cup \dots \cup A_n$ należy do co najwyżej $2r$ zbiorów A_j , to nierówność (2.15) staje się równością. Jeśli natomiast istnieje co najmniej jeden element należący do więcej niż $2r$ zbiorów A_j , to nierówność (2.15) jest ostra. Podobnie jest z nierównością (2.16). Jeśli każdy element sumy $A_1 \cup \dots \cup A_n$ należy do co najwyżej $2r + 1$ zbiorów A_j , to mamy równość; w przeciwnym przypadku nierówność jest ostra.

Spis tożsamości kombinatorycznych

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (2.1)$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \quad (2.2)$$

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.3)$$

$$|\{f \in A^B : f \text{ jest „na”}\}| = \sum_{k=0}^m (-1)^k \binom{m}{k} (m-k)^n. \quad (2.4)$$

$$|D(A)| = n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}. \quad (2.5)$$

$$|D_0(X, A_1, \dots, A_n)| = \sum_{k=0}^n (-1)^k \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.6)$$

$$|D_r(X, A_1, \dots, A_n)| = \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.7)$$

$$|D_r(A)| = \frac{n!}{r!} \cdot \sum_{k=0}^{n-r} \frac{(-1)^k}{k!}. \quad (2.8)$$

$$M(n) = 2 \cdot n! \cdot \mu(n). \quad (2.9)$$

$$\mu(n) = \sum_{k=0}^n (-1)^k \cdot (n-k)! \cdot g(2n, k). \quad (2.10)$$

$$M(n) = 2 \cdot n! \cdot \sum_{k=0}^n (-1)^k \cdot \frac{2n}{2n-k} \cdot \binom{2n-k}{k} \cdot (n-k)! \quad (2.11)$$

$$n^k = \sum_{j=1}^k (-1)^{j+1} \binom{k}{j} S_{k-j}(n). \quad (2.12)$$

$$\sum_{j=0}^n (-1)^j \binom{n}{j} (m-j)^n = n! \quad \text{dla } m \geq n. \quad (2.13)$$

$$\sum_{k=0}^n (-1)^k \binom{n}{k} (x-k)^n = n! \quad (2.14)$$

$$|A_1 \cup \dots \cup A_n| \geq \sum_{k=1}^{2m} (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.15)$$

$$|A_1 \cup \dots \cup A_n| \leq \sum_{k=1}^{2m+1} (-1)^{k+1} \sum_{T \in P_k(n)} \left| \bigcap_{j \in T} A_j \right|. \quad (2.16)$$

RÓWNANIA REKURENCYJNE

1. Ciągi arytmetyczne i geometryczne

Z najprostszymi równaniami rekurencyjnymi zetknęliśmy się już w szkole. Zaczniemy od przypomnienia definicji ciągu arytmetycznego. Niech będą dane dwie liczby rzeczywiste a i r . **Ciągiem arytmetycznym** nazywamy ciąg (a_n) liczb rzeczywistych określony wzorami

$$a_0 = a, \quad a_{n+1} = a_n + r \quad \text{dla } n \geq 0.$$

Ze szkoły znamy też **wzór ogólny** (lub **wzór jawny**) ciągu arytmetycznego (a_n) :

$$a_n = a + nr$$

dla $n = 0, 1, 2, \dots$

W podobny sposób definiujemy ciągi geometryczne. Załóżmy, że dane są liczby rzeczywiste a i q . **Ciągiem geometrycznym** nazywamy ciąg (a_n) liczb rzeczywistych zdefiniowany wzorami

$$a_0 = a, \quad a_{n+1} = a_n q \quad \text{dla } n \geq 0.$$

Znów wzór ogólny ciągu geometrycznego (a_n) jest znany ze szkoły:

$$a_n = aq^n$$

dla $n = 0, 1, 2, \dots$

2. Wieże Hanoi

Znaczenie równań rekurencyjnych w kombinatoryce polega na tym, że wielokrotnie umiemy dość łatwo znaleźć rozwiązanie rekurencyjne zadania kombinatorycznego, podczas gdy znalezienie wzoru ogólnego nie jest oczywiste. Z drugiej strony, znamy wiele metod otrzymywania wzorów ogólnych z równań rekurencyjnych. Kilka takich metod poznamy w tym i następnym wykładzie. Zaczniemy od przykładu: zadania o tzw. wieżach Hanoi.

Łamigłówka o nazwie „Wieże Hanoi” wygląda w następujący sposób. Mamy trzy pałeczki. Na jedną z nich nadziano 64 krążki w kolejności od największego na dole do najmniejszego na górze. Należy przenieść wszystkie krążki z jednej pałeczki na drugą, przy czym wolno za każdym razem przenosić tylko jeden krążek i nie wolno kłaść większego krążka na mniejszy. W czasie przenoszenia wolno kłaść krążki na wszystkich trzech pałeczkach. Ile najmniej ruchów (tzn. pojedynczych przeniesień krążków) potrzeba, by przenieść wszystkie 64 krążki?

Oznaczmy przez H_n najmniejszą liczbę ruchów, które należy wykonać by przenieść n krążków z jednej pałeczki na inną. Jest przy tym obojętne, z której pałeczki na którą przenosimy te krążki. Również jest obojętne, czy na tych pałeczkach już leżą jakieś krążki, byle były one większe od wszystkich krążków, które przenosimy. Oczywiście $H_0 = 0$. Przypuśćmy, że umiemy przenieść n krążków w minimalnej liczbie H_n ruchów. Chcemy teraz przenieść $n+1$ krążków z pierwszej pałeczki na drugą. W którymś momencie będziemy musieli przenieść największy krążek, leżący na samym dole na pierwszej

pałeczce. Oczywiście musimy przedtem zdjąć z niego wszystkie mniejsze krążki. Nie mogą one też leżeć na drugiej pałeczce, bo tam mamy położyć największy krążek. Musimy zatem przenieść n krążków z pierwszej pałeczki na trzecią. Wykonamy w tym celu H_n ruchów. Następnie przenosimy największy krążek (to jest jeden ruch) i wreszcie przenosimy n krążków z trzeciej pałeczki na drugą (tu znów mamy H_n ruchów). Razem wykonamy więc $2 \cdot H_n + 1$ ruchów. Widzimy, że z jednej strony jest to minimalna liczba ruchów, które musimy wykonać, a z drugiej, że ta liczba ruchów jest też wystarczająca. Zatem otrzymujemy równanie rekurencyjne:

$$H_0 = 0, \quad H_{n+1} = 2 \cdot H_n + 1 \quad \text{dla } n \geq 0.$$

Obliczmy kilka początkowych wyrazów ciągu (H_n) :

$$\begin{aligned} H_0 &= 0, \\ H_1 &= 2H_0 + 1 = 1, \\ H_2 &= 2H_1 + 1 = 3, \\ H_3 &= 2H_2 + 1 = 7, \\ H_4 &= 2H_3 + 1 = 15 \end{aligned}$$

i tak dalej. Łatwo domyślamy się wzoru ogólnego:

$$H_n = 2^n - 1$$

dla $n = 0, 1, 2, \dots$. Możemy teraz sprawdzić przez indukcję, że ten odgadnięty wzór ogólny jest poprawny.

3. Równania rekurencyjne liniowe pierwszego rzędu o stałych współczynnikach

Niech będą dane liczby rzeczywiste a , b i c . Przypuśćmy następnie, że ciąg (a_n) został określony za pomocą równania rekurencyjnego

$$a_0 = a, \quad a_{n+1} = b \cdot a_n + c \quad \text{dla } n \geq 0.$$

Ciąg (H_n) określony wyżej otrzymamy przyjmując $a = 0$, $b = 2$ i $c = 1$. Przyjmijmy ponadto, że $b \neq 1$ (w przeciwnym razie mielibyśmy do czynienia z ciągiem arytmetycznym). Obliczmy kilka początkowych wyrazów ciągu (a_n) :

$$\begin{aligned} a_0 &= a, \\ a_1 &= ba_0 + c = ab + c, \\ a_2 &= ba_1 + c = ab^2 + bc + c, \\ a_3 &= ba_2 + c = ab^3 + b^2c + bc + c, \\ a_4 &= ba_3 + c = ab^4 + b^3c + b^2c + bc + c, \\ a_5 &= ba_4 + c = ab^5 + b^4c + b^3c + b^2c + bc + c \end{aligned}$$

i tak dalej. Znów domyślamy się wzoru ogólnego:

$$a_n = ab^n + c(1 + b + b^2 + \dots + b^{n-1}) = ab^n + c \cdot \frac{b^n - 1}{b - 1}$$

dla $n = 0, 1, 2, \dots$. Sprawdzimy przez indukcję, że ten wzór jest poprawny.

Dla $n = 0$ mamy

$$a_0 = ab^0 + c \cdot \frac{b^0 - 1}{b - 1} = a.$$

Przypuśćmy następnie, że nasz wzór jest spełniony dla pewnego n i obliczmy a_{n+1} :

$$\begin{aligned} a_{n+1} &= ba_n + c = b \cdot \left(ab^n + c \cdot \frac{b^n - 1}{b - 1} \right) + c = ab^{n+1} + c \cdot \frac{b^{n+1} - b}{b - 1} + c = \\ &= ab^{n+1} + c \cdot \frac{b^{n+1} - b + b - 1}{b - 1} = ab^{n+1} + c \cdot \frac{b^{n+1} - 1}{b - 1}, \end{aligned}$$

co kończy dowód indukcyjny.

Wzór ogólny tego ciągu można wyznaczyć też w inny sposób, wprowadzając ciąg pomocniczy (b_n) zdefiniowany wzorem

$$b_n = a_{n+1} - a_n$$

dla $n = 0, 1, 2, \dots$. Wówczas

$$b_{n+1} = a_{n+2} - a_{n+1} = (ba_{n+1} + c) - (ba_n + c) = b \cdot (a_{n+1} - a_n) = b \cdot b_n,$$

skąd dostajemy

$$b_n = b_0 \cdot b^n$$

dla $n = 0, 1, 2, \dots$. Zatem

$$a_{n+1} = a_n + b_0 \cdot b^n$$

dla $n = 0, 1, 2, \dots$. Wypiszmy n początkowych równości:

$$\begin{aligned} a_1 &= a_0 + b_0 \cdot b^0, \\ a_2 &= a_1 + b_0 \cdot b^1, \\ a_3 &= a_2 + b_0 \cdot b^2, \\ a_{n-1} &= a_{n-2} + b_0 \cdot b^{n-2}, \\ a_n &= a_{n-1} + b_0 \cdot b^{n-1}. \end{aligned}$$

Po dodaniu stronami tych nierówności i skróceniu występujących po obu stronach wyrazów $a_1, a_2, \dots, a_{n-1}$, otrzymamy

$$\begin{aligned} a_n &= a_0 + b_0 \cdot (b^0 + b^1 + b^2 + \dots + b^{n-1}) = a_0 + b_0 \cdot \frac{b^n - 1}{b - 1} = \\ &= a + (ab + c - a) \cdot \frac{b^n - 1}{b - 1} = a + a(b - 1) \cdot \frac{b^n - 1}{b - 1} + c \cdot \frac{b^n - 1}{b - 1} = \\ &= a + a(b^n - 1) + c \cdot \frac{b^n - 1}{b - 1} = ab^n + c \cdot \frac{b^n - 1}{b - 1}. \end{aligned}$$

4. Równania rekurencyjne liniowe pierwszego rzędu o zmiennych współczynnikach

Rozwiążemy najpierw zadanie o tzw. sortowaniu przez łączenie. Mamy 2^n monet, każda innej wagi. Dysponujemy wagą szalkową bez odważników. Naszym zadaniem będzie ułożenie wszystkich monet w kolejności od najcięższej do najlżejszej. Będziemy to robić w następujący sposób. Najpierw podzielimy monety na dwie części po 2^{n-1} monet. Następnie każdą z tych części uporządkujemy od najcięższej do najlżejszej. Potem porównamy najcięższe monety z obu części i cięższą z nich odłożymy jako najcięższą ze wszystkich. Potem porównamy najcięższe monety obu części (jedna z tych części jest teraz mniejsza, ubyłła z niej jedna moneta). Cięższą monetę odkładamy na bok jako drugą z kolei. I tak dalej. Trzeba jeszcze wyjaśnić, w jaki sposób porządkujemy obie części. Otóż zrobimy to w taki sam sposób. Każdą z tych części podzielimy znów na dwie części, uporządkujemy je i połączymy ze sobą. Każdą z tych mniejszych części znów porządkujemy tak samo: dzielimy na dwie części i potem łączymy ze sobą. I tak dalej. Wreszcie dojdziemy do części liczących tylko dwie monety i wtedy wystarczy jedno ważenie, by taką małą część uporządkować. Ile potrzeba ważeń, by za pomocą tej metody uporządkować wszystkie monety?

Oznaczmy przez P_n maksymalną liczbę ważeń potrzebnych do uporządkowania 2^n monet w sposób opisany w zadaniu. Oczywiście $P_0 = 0$. Jeśli bowiem mamy 2^0 , czyli 1 monetę, to nie musimy nic ważyć. Przypuśćmy teraz, że umiemy już uporządkować 2^n monet za pomocą P_n ważeń. Spróbujmy zatem uporządkować 2^{n+1} monet. Najpierw dzielimy je na dwie części, po 2^n monet każda. Następnie porządkujemy każdą z tych części. Do uporządkowania każdej części potrzebujemy P_n ważeń. Wreszcie musimy połączyć obie części. Zauważamy więc, że każde ważenie pozwala nam odłożyć na bok, jako kolejną, tylko jedną monetę. Do uporządkowania wszystkich 2^{n+1} monet będziemy więc potrzebowali co najwyżej $2^{n+1} - 1$ ważeń. (Czasami to łączenie może zakończyć się wcześniej, gdy przy odkładaniu monet na bok jedną z części wyczerpiemy dużo wcześniej niż drugą; na pewno jednak nie będziemy potrzebowali większej liczby ważeń.) Łączna maksymalna liczba ważeń potrzebnych do uporządkowania wszystkich 2^{n+1} monet wynosi więc $2 \cdot P_n + 2^{n+1} - 1$.

Ciąg liczb (P_n) jest zatem określony wzorami: rekurencyjnymi

$$P_0 = 0, \quad P_{n+1} = 2 \cdot P_n + 2^{n+1} - 1 \quad \text{dla } n \geq 0.$$

Znów obliczmy kilka początkowych wyrazów ciągu (P_n) :

$$\begin{aligned} P_0 &= 0, \\ P_1 &= 2 \cdot 0 + 2^1 - 1 = 1, \\ P_2 &= 2 \cdot 1 + 2^2 - 1 = 5, \\ P_3 &= 2 \cdot 5 + 2^3 - 1 = 17, \\ P_4 &= 2 \cdot 17 + 2^4 - 1 = 49, \\ P_5 &= 2 \cdot 49 + 2^5 - 1 = 129, \\ P_6 &= 2 \cdot 129 + 2^6 - 1 = 321 \end{aligned}$$

i tak dalej. Tu domyslenie się wzoru ogólnego jest trudniejsze. Można jednak zauważyć, że

$$P_0 - 1 = -1 = (-1) \cdot 2^0,$$

$$P_1 - 1 = 0 = 0 \cdot 2^1,$$

$$P_2 - 1 = 4 = 1 \cdot 2^2,$$

$$P_3 - 1 = 16 = 2 \cdot 2^3,$$

$$P_4 - 1 = 48 = 3 \cdot 2^4,$$

$$P_5 - 1 = 128 = 4 \cdot 2^5,$$

$$P_6 - 1 = 320 = 5 \cdot 2^6$$

i tak dalej. Widzimy już wzór ogólny

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

dla $n = 0, 1, 2, \dots$. Sprawdzenie poprawności tego wzoru przez indukcję jest prostym ćwiczeniem.

5. Metoda czynnika sumacyjnego

Równanie rekurencyjne otrzymane w ostatnim paragrafie można rozwiązać w sposób następujący. Rozważmy ciąg (Q_n) określony wzorem

$$Q_n = \frac{P_n}{2^n} \quad \text{dla } n \geq 0.$$

Wówczas oczywiście $Q_0 = 0$. Podzielmy teraz obie strony równania

$$P_{n+1} = 2 \cdot P_n + 2^{n+1} - 1$$

przez 2^{n+1} . Otrzymamy

$$\frac{P_{n+1}}{2^{n+1}} = \frac{P_n}{2^n} + 1 - \frac{1}{2^{n+1}},$$

czyli

$$Q_{n+1} = Q_n + 1 - \frac{1}{2^{n+1}}$$

dla $n = 0, 1, 2, \dots$. Wypiszmy teraz otrzymane zależności dla początkowych wartości n :

$$Q_1 = Q_0 + 1 - \frac{1}{2^1},$$

$$Q_2 = Q_1 + 1 - \frac{1}{2^2},$$

$$Q_3 = Q_2 + 1 - \frac{1}{2^3},$$

$$Q_4 = Q_3 + 1 - \frac{1}{2^4},$$

...

$$Q_{n-1} = Q_{n-2} + 1 - \frac{1}{2^{n-1}},$$

$$Q_n = Q_{n-1} + 1 - \frac{1}{2^n}.$$

Dodajemy teraz te równości stronami i po skróceniu jednakowych składników występujących po obu stronach, otrzymujemy

$$Q_n = Q_0 + n - \frac{1}{2^1} - \frac{1}{2^2} - \frac{1}{2^3} - \dots - \frac{1}{2^n}.$$

Mnożymy obie strony przez 2^n , otrzymując

$$P_n = n \cdot 2^n - (1 + 2 + 4 + \dots + 2^{n-1}) = n \cdot 2^n - (2^n - 1) = (n - 1) \cdot 2^n + 1.$$

Powstaje pytanie, w jaki sposób dobieramy na początku ciąg (Q_n) i liczbę, przez którą dzielimy obie strony równania rekurencyjnego. Popatrzmy zatem na ten problem nieco ogólniej. Przypuśćmy, że mamy dane trzy ciągi (a_n) , (b_n) i (c_n) oraz, że ciąg (t_n) jest określony wzorami rekurencyjnymi

$$t_0 = t, \quad a_n t_{n+1} = b_n t_n + c_n \quad \text{dla } n \geq 0.$$

Wybieramy następnie ciąg (s_n) (tzw. **czynnik sumacyjny**) o tej własności, że

$$a_n s_n = b_{n+1} s_{n+1}$$

dla $n = 0, 1, 2, \dots$. Następnie mnożymy obie strony równania

$$a_n t_{n+1} = b_n t_n + c_n$$

przez s_n :

$$a_n s_n t_{n+1} = b_n s_n t_n + c_n s_n,$$

czyli

$$b_{n+1} s_{n+1} t_{n+1} = b_n s_n t_n + c_n s_n$$

dla $n = 0, 1, 2, \dots$. Określamy teraz ciąg (u_n) wzorem

$$u_n = b_n s_n t_n$$

dla $n = 0, 1, 2, \dots$ i wypisujemy n początkowych równań:

$$u_1 = u_0 + c_0 s_0,$$

$$u_2 = u_1 + c_1 s_1,$$

$$u_3 = u_2 + c_2 s_2,$$

$$\dots \quad \dots$$

$$u_n = u_{n-1} + c_{n-1} s_{n-1}.$$

Dodajemy stronami otrzymane równości i po skróceniu dostajemy

$$u_n = u_0 + \sum_{k=0}^{n-1} c_k s_k,$$

czyli

$$t_n = \frac{1}{b_n s_n} \cdot \left(b_0 s_0 t + \sum_{k=0}^{n-1} c_k s_k \right)$$

dla $n = 0, 1, 2, \dots$

W naszym przykładzie mieliśmy $a_n = 1$, $b_n = 2$ oraz $c_n = 2^{n+1} - 1$. Dobieraliśmy czynnik sumacyjny s_n tak, by $a_n s_n = b_{n+1} s_{n+1}$, czyli $s_n = 2s_{n+1}$. W tym momencie wybór

$$s_n = \frac{1}{2^n}$$

jest już naturalny.

6. Równania rekurencyjne liniowe pierwszego rzędu o zmiennych współczynnikach – c. d.

W ostatnim przykładzie mieliśmy do czynienia z ciągiem zdefiniowanym za pomocą równania rekurencyjnego liniowego postaci

$$t_0 = t, \quad a_n t_{n+1} = b_n t_n + c_n \quad \text{dla } n \geq 0,$$

w którym ciągi (a_n) i (b_n) były stałe i tylko wyrazy ciągu (c_n) zależały od n . Znamy jednak dobrze ciąg zdefiniowany rekurencyjnie, w którym współczynnik b_n zależy od n . Jest to silnia:

$$0! = 1, \quad (n+1)! = (n+1) \cdot n! \quad \text{dla } n \geq 0.$$

W tym paragrafie przyjrzymy się zastosowaniu metody czynnika sumacyjnego do znalezienia wzoru ogólnego dla ciągu zdefiniowanego podobnymi wzorami. Przypuśćmy, że ciąg (a_n) jest zdefiniowany wzorami

$$a_0 = 1, \quad a_{n+1} = (n+1) \cdot a_n + 1 \quad \text{dla } n \geq 1.$$

Definiujemy ciąg (b_n) wzorem

$$b_n = \frac{a_n}{n!}$$

dla $n = 0, 1, 2, \dots$. Następnie dzielimy obie strony równania

$$a_{n+1} = (n+1) \cdot a_n + 1$$

przez $(n+1)!$. Otrzymujemy

$$\frac{a_{n+1}}{(n+1)!} = \frac{a_n}{n!} + \frac{1}{n!}$$

dla $n = 0, 1, 2, \dots$, czyli

$$b_{n+1} = b_n + \frac{1}{(n+1)!}$$

dla $n = 0, 1, 2, \dots$. Podobnie jak w poprzednich paragrafach otrzymujemy stąd

$$b_n = b_0 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!},$$

czyli

$$a_n = n! \cdot \left(\frac{1}{0!} + \frac{1}{1!} + \dots + \frac{1}{n!} \right)$$

dla $n = 0, 1, 2, \dots$. Dla dużych n mamy zatem $a_n \approx n! \cdot e$.

7. Suma odwrotności współczynników dwumianowych

Metodę czynnika sumacyjnego możemy zastosować także do obliczenia następujących dwóch sum. Oznaczmy:

$$S_n = \sum_{k=0}^n \frac{1}{\binom{n}{k}}, \quad T_n = \sum_{k=0}^n \frac{k}{\binom{n}{k}}$$

dla $n = 0, 1, 2, \dots$. Wtedy:

$$T_n = \sum_{k=0}^n \frac{n-k}{\binom{n}{k}} = n \cdot S_n - T_n, \quad \text{czyli} \quad T_n = \frac{n}{2} \cdot S_n.$$

Następnie:

$$\begin{aligned} S_n &= 1 + \sum_{k=1}^n \frac{1}{\binom{n}{k}} = 1 + \sum_{k=1}^n \frac{1}{\frac{n}{k} \binom{n-1}{k-1}} = 1 + \frac{1}{n} \cdot \sum_{k=1}^n \frac{k}{\binom{n-1}{k-1}} = \\ &= 1 + \frac{1}{n} \cdot \sum_{k=0}^n \frac{k+1}{\binom{n-1}{k}} = 1 + \frac{1}{n} \cdot (S_{n-1} + T_{n-1}) = \\ &= 1 + \frac{1}{n} \cdot S_{n-1} + \frac{1}{n} \cdot T_{n-1} = 1 + \frac{1}{n} \cdot S_{n-1} + \frac{n-1}{2n} \cdot S_{n-1} = \\ &= \frac{n+1}{2n} \cdot S_{n-1} + 1 \end{aligned}$$

dla $n = 1, 2, 3, \dots$. Mamy zatem równanie rekurencyjne postaci $S_n = a_n S_{n-1} + 1$, gdzie $a_n = \frac{n+1}{2n}$. Takie równania umiemy rozwiązywać za pomocą czynnika sumacyjnego. Dobieramy czynnik s_n tak, by były spełnione równości $s_n a_n = s_{n-1}$ dla wszystkich $n \geq 1$. Przyjmujemy

$$s_0 = 1 \quad \text{oraz} \quad s_n = \frac{s_{n-1}}{a_n} \quad \text{dla } n \geq 1.$$

Wtedy otrzymujemy:

$$s_n S_n = s_n a_n S_{n-1} + s_n$$

czyli

$$s_n S_n = s_{n-1} S_{n-1} + s_n$$

dla $n = 1, 2, 3, \dots$. Przyjmując następnie $U_n = s_n S_n$, otrzymujemy równanie rekurencyjne

$$U_0 = 1, \quad U_n = U_{n-1} + s_n \quad \text{dla } n \geq 1.$$

To równanie rekurencyjne oczywiście ma rozwiązanie w postaci sumy:

$$U_n = U_0 + \sum_{k=1}^n s_k$$

dla $n = 0, 1, 2, \dots$. Nietrudno zauważyć, że czynniki sumacyjne s_n są równe

$$s_n = \frac{s_0}{a_1 a_2 \cdot \dots \cdot a_n} = \frac{1}{a_1 a_2 \cdot \dots \cdot a_n} = \prod_{k=1}^n \frac{2k}{k+1} = \frac{2^n}{n+1}$$

dla $n = 1, 2, 3, \dots$. Ponadto $s_0 = 1$. Stąd otrzymujemy

$$U_n = 1 + \sum_{k=1}^n \frac{2^k}{k+1} = \sum_{k=0}^n \frac{2^k}{k+1}$$

dla $n = 0, 1, 2, \dots$. Ostatecznie:

$$S_n = \frac{1}{s_n} \cdot \sum_{k=0}^n \frac{2^k}{k+1} = \frac{n+1}{2^n} \cdot \sum_{k=0}^n \frac{2^k}{k+1} = \frac{n+1}{2^{n+1}} \cdot \sum_{k=0}^n \frac{2^{k+1}}{k+1} = \frac{n+1}{2^{n+1}} \cdot \sum_{k=1}^{n+1} \frac{2^k}{k}$$

oraz

$$T_n = \frac{n(n+1)}{2^{n+2}} \cdot \sum_{k=1}^{n+1} \frac{2^k}{k}$$

dla $n = 0, 1, 2, \dots$

8. Co trzeci współczynnik dwumianowy

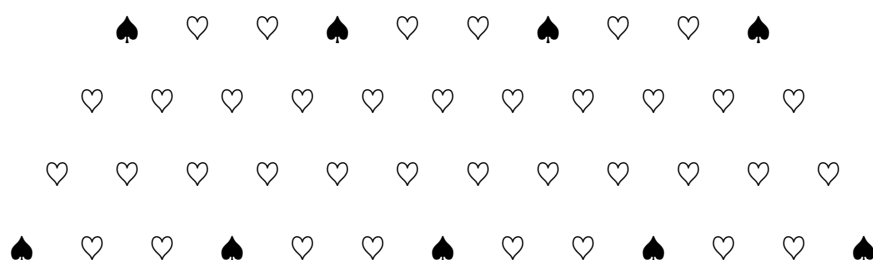
W tym paragrafie obliczymy sumę

$$S_n = \sum_{k=0}^n \binom{3n}{3k} = \sum_{3|k} \binom{3n}{k}$$

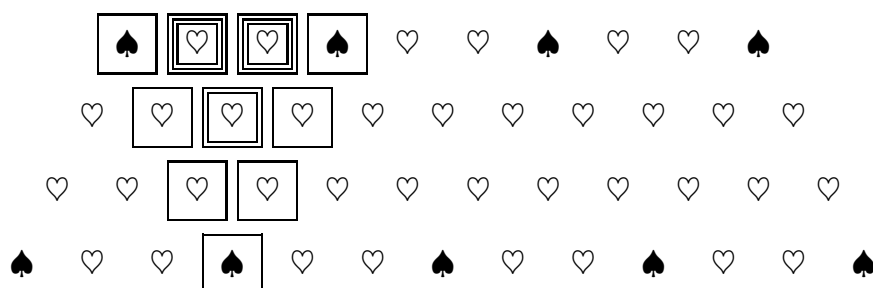
dla $n = 0, 1, 2, \dots$. W drugiej sumie wskaźnik k przebiega wszystkie liczby podzielne przez 3, dla których dodawany składnik jest niezerowy. Przypominamy tu, że każdy wiersz trójkąta Pascala traktujemy jako składający się z nieskończenie wielu współczynników dwumianowych, wśród których jest tylko skończenie wiele różnych od zera. Tej umowy będziemy się trzymać we wszystkich rozważanych dalej sumach. Przystąpimy teraz do ułożenia równania rekurencyjnego dla ciągu (S_n) .

Przyjrzymy się dokładnie strukturze trójkąta Pascala. Mamy obliczyć sumę co trzeciego wyrazu w co trzecim wierszu tego trójkąta. Pamiętamy, że każdy wyraz trójkąta Pascala jest sumą dwóch wyrazów stojących bezpośrednio nad nim, z jego lewej i prawej strony. Te wyrazy z kolei są sumami wyrazów stojących wyżej itd. Spróbujemy wyrazić sumę co trzeciego wyrazu wiersza o numerze $3n + 3$ za pomocą analogicznej sumy wyrazów

wiersza o numerze $3n$. Popatrzmy w tym celu na przykładowy fragment trójkąta Pascala (wiersze od $n = 9$ do $n = 12$):



Na powyższym rysunku nie wpisaliśmy liczb. Zaznaczyliśmy tylko miejsca, na których się znajdują dwoma znakami: ♠ i ♥. Okazuje się bowiem, że dla uzyskania równania rekurencyjnego zupełnie nie jest istotne, jakie liczby dodajemy, ale ważne jest to, na jakich miejscach się one znajdują. I tak symbolem ♠ są oznaczone te miejsca w trójkącie Pascala, gdzie znajdują się liczby, które będziemy sumować. Symbolem ♥ oznaczone są wszystkie pozostałe miejsca w tym trójkącie. Teraz popatrzmy, jak liczby stojące na miejscach ♠ najniższego wiersza powstają z liczb stojących w wierszu położonym najwyżej na naszym rysunku:



Symbole ♠ i ♥ są teraz w ramkach. Pojedyncza ramka oznacza, że dana liczba była użyta jeden raz do obliczenia odpowiedniej liczby dolnego wiersza. Takimi są na przykład liczby drugiego wiersza od dołu. Jednak w trzecim wierszu od dołu pojawia się już liczba, która została użyta dwa razy: po jednym razie do obliczenia każdej z obramowanych liczb drugiego wiersza od dołu. W najwyższym wierszu naszego rysunku niektóre liczby mają nawet trzy ramki: te, które były potrzebne do obliczenia liczby w podwójnej ramce niższego rzędu. Tak samo będzie dla każdej interesującej nas liczby najniższego rzędu. Możemy to zapisać w postaci wzoru:

$$\binom{3n+3}{3k} = \binom{3n}{3k-3} + 3 \cdot \binom{3n}{3k-2} + 3 \cdot \binom{3n}{3k-1} + \binom{3n}{3k}$$

Nietrudno teraz dostrzec zależność rekurencyjną (przyjmujemy, że sumowanie rozciąga się na wszystkie niezerowe wyrazy danej sumy):

$$S_{n+1} = 2 \cdot \sum_{3|k} \binom{3n}{k} + 3 \cdot \sum_{3 \nmid k} \binom{3n}{k} = 3 \cdot \sum_k \binom{3n}{k} - \sum_{3|k} \binom{3n}{k} = 3 \cdot 2^{3n} - S_n$$

dla $n = 0, 1, 2, \dots$

Wzór ten możemy otrzymać też za pomocą bezpośrednich obliczeń:

$$\begin{aligned}
 \binom{3n+3}{3k} &= \binom{3n+2}{3k-1} + \binom{3n+2}{3k} = \\
 &= \binom{3n+1}{3k-2} + \binom{3n+1}{3k-1} + \binom{3n+1}{3k-1} + \binom{3n+1}{3k} = \\
 &= \binom{3n+1}{3k-2} + 2 \cdot \binom{3n+1}{3k-1} + \binom{3n+1}{3k} = \\
 &= \binom{3n}{3k-3} + \binom{3n+1}{3k-2} + 2 \cdot \binom{3n}{3k-2} + 2 \cdot \binom{3n}{3k-1} + \binom{3n}{3k-1} + \binom{3n}{3k} = \\
 &= \binom{3n}{3k-3} + 3 \cdot \binom{3n}{3k-2} + 3 \cdot \binom{3n}{3k-1} + \binom{3n}{3k}
 \end{aligned}$$

Stąd wynika, że (pamiętamy, że sumowanie rozciąga się na wszystkie niezerowe wyrazy danej sumy):

$$S_{n+1} = \sum_k \binom{3n+3}{3k} = \sum_k \binom{3n}{3k-3} + 3 \cdot \sum_k \binom{3n}{3k-2} + 3 \cdot \sum_k \binom{3n}{3k-1} + \sum_k \binom{3n}{3k}.$$

Teraz należy zauważyć, że

$$\sum_k \binom{3n}{3k-3} = \sum_k \binom{3n}{3k}.$$

W obu sumach występują bowiem te same składniki niezerowe $\binom{3n}{k}$ wiersza o numerze $3n$: te mianowicie, dla których liczba k jest podzielna przez 3. Mamy zatem

$$\begin{aligned}
 S_{n+1} &= \sum_k \binom{3n+3}{3k} = \\
 &= 2 \cdot \sum_k \binom{3n}{3k-3} + 3 \cdot \sum_k \binom{3n}{3k-2} + 3 \cdot \sum_k \binom{3n}{3k-1} = \\
 &= 3 \cdot \sum_k \binom{3n}{k} - \sum_{3|k} \binom{3n}{k} = \\
 &= 3 \cdot 2^{3n} - S_n
 \end{aligned}$$

dla $n = 0, 1, 2, \dots$

Nietrudno zauważyć, że $S_0 = 1$. Pozostaje nam wyprowadzenie wzoru ogólnego na S_n ze wzorów rekurencyjnych

$$S_0 = 1, \quad S_{n+1} = 3 \cdot 2^{3n} - S_n = 3 \cdot 8^n - S_n \quad \text{dla } n \geq 0.$$

Możemy to osiągnąć bardzo prosto wyrażając S_{n+2} za pomocą S_n :

$$S_{n+2} = 3 \cdot 8^{n+1} - S_{n+1} = 3 \cdot 8^{n+1} - 3 \cdot 8^n + S_n,$$

czyli

$$S_{n+2} = S_n + 21 \cdot 8^n.$$

Teraz już łatwo zauważyć, że dla liczby nieparzystej n mamy

$$S_n = S_1 + 21 \cdot (8^1 + 8^3 + \dots + 8^{n-2})$$

i ze wzoru na sumę ciągu geometrycznego otrzymujemy

$$S_n = 2 + 21 \cdot \frac{8^n - 8}{8^2 - 1} = 2 + \frac{8^n - 8}{3} = \frac{8^n - 2}{3}.$$

Dla n parzystych skorzystamy ze wzoru rekurencyjnego:

$$S_n = 3 \cdot 8^{n-1} - S_{n-1} = 3 \cdot 8^{n-1} - \frac{8^{n-1} - 2}{3} = \frac{9 \cdot 8^{n-1} - 8^{n-1} + 2}{3} = \frac{8^n + 2}{3}.$$

Łącząc razem otrzymane wzory dla n parzystych i n nieparzystych dostajemy wzór

$$S_n = \sum_{k=0}^n \binom{3n}{3k} = \frac{8^n + 2 \cdot (-1)^n}{3}.$$

Równanie rekurencyjne

$$S_0 = 1, \quad S_{n+1} = 3 \cdot 8^n - S_n \quad \text{dla } n \geq 0$$

można rozwiązać też za pomocą czynnika sumacyjnego. Zdefiniujmy ciąg (T_n) wzorem:

$$T_n = (-1)^n \cdot S_n$$

dla $n = 0, 1, 2, \dots$ i pomnóżmy obie strony równania

$$S_{n+1} = 3 \cdot 8^n - S_n$$

przez $(-1)^{n+1}$. Otrzymamy

$$(-1)^{n+1} \cdot S_{n+1} = 3 \cdot (-1)^{n+1} \cdot 8^n + (-1)^n \cdot S_n,$$

czyli

$$T_{n+1} = T_n - 3 \cdot (-1)^n \cdot 8^n = T_n - 3 \cdot (-8)^n.$$

Stąd już łatwo stwierdzimy, że (pamiętając, że $T_0 = 1$):

$$\begin{aligned} T_n &= T_0 - 3 \cdot (-8)^0 - 3 \cdot (-8)^1 - \dots - 3 \cdot (-8)^{n-1} = \\ &= T_0 - 3 \cdot (1 + (-8)^1 + (-8)^2 + \dots + (-8)^{n-1}) = \\ &= T_0 - 3 \cdot \frac{(-8)^n - 1}{-8 - 1} = 1 + \frac{(-8)^n - 1}{3} = \frac{(-8)^n + 2}{3}. \end{aligned}$$

Ponieważ $T_n = (-1)^n \cdot S_n$, więc

$$S_n = (-1)^n \cdot \frac{(-8)^n + 2}{3} = \frac{8^n + 2 \cdot (-1)^n}{3}$$

dla $n = 0, 1, 2, \dots$

Dowód kombinatoryczny. Równanie rekurencyjne

$$S_0 = 1, \quad S_{n+1} = 3 \cdot 8^n - S_n \quad \text{dla } n \geq 0$$

można też otrzymać za pomocą rozumowania kombinatorycznego. Mamy bowiem

$$S_n = |\{A \subseteq [3n] : 3 \mid |A|\}|$$

dla $n = 0, 1, 2, \dots$. Możemy teraz zastanowić się, jak wyglądają podzbiory zbioru $[3n+3]$ o liczbie elementów podzielnej przez 3. Te podzbiory możemy pogrupować w cztery zbiory:

- 1) $A \subseteq [3n]$, gdzie $3 \mid |A|$,
- 2) $A = B \cup \{3n+1, 3n+2, 3n+3\}$, gdzie $B \subseteq [3n]$ i $3 \mid |B|$,
- 3) $A = B \cup \{3n+1\}$ lub $A = B \cup \{3n+2\}$ lub $A = B \cup \{3n+3\}$, gdzie $B \subseteq [3n]$ i $|B| \equiv 2 \pmod{3}$,
- 4) $A = B \cup \{3n+1, 3n+2\}$ lub $A = B \cup \{3n+1, 3n+3\}$ lub $A = B \cup \{3n+2, 3n+3\}$, gdzie $B \subseteq [3n]$ i $|B| \equiv 1 \pmod{3}$.

W pierwszej i drugiej grupie mamy po S_n zbiorów, w trzeciej i czwartej mamy łącznie $3 \cdot (2^{3n} - S_n)$ zbiorów. Stąd otrzymujemy równanie

$$S_{n+1} = 2S_n + 3 \cdot 2^{3n} - 3S_n = 3 \cdot 8^n - S_n.$$

Rozwiązanie algebraiczne. Zadanie obliczenia sumy S_n można rozwiązać metodami algebry. W tym celu weźmy zespolony pierwiastek trzeciego stopnia z jedności:

$$\varepsilon^3 = 1.$$

Wtedy ε jest pierwiastkiem równania $x^3 - 1 = 0$, czyli $(x-1)(x^2 + x + 1) = 0$. Stąd wynika, że nierzeczywisty pierwiastek tego równania spełnia równanie

$$\varepsilon^2 + \varepsilon + 1 = 0.$$

Obliczymy teraz dwoma sposobami sumę

$$(1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n}.$$

Najpierw skorzystamy ze wzoru dwumianowego Newtona:

$$\begin{aligned} & (1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n} = \\ &= \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{0 \cdot k} + \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{1 \cdot k} + \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{2 \cdot k} = \\ &= \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0 + \varepsilon^k + \varepsilon^{2k}). \end{aligned}$$

Popatrzmy teraz, jak wyglądają sumy

$$1 + \varepsilon^k + \varepsilon^{2k}$$

dla różnych k . Oczywiście dla liczb k podzielnych przez 3 dodajemy do siebie trzy jedynki. Zatem suma jest równa 3. Niech teraz $k = 3l + 1$. Wtedy

$$1 + \varepsilon^k + \varepsilon^{2k} = 1 + \varepsilon^{3l} \cdot \varepsilon + \varepsilon^{6l} \cdot \varepsilon^2 = 1 + \varepsilon + \varepsilon^2 = 0.$$

Podobnie dla $k = 3l + 2$ stwierdzimy, że ta suma równa jest 0. Zatem, kontynuując przerwane obliczenia, dostajemy

$$\sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0 + \varepsilon^k + \varepsilon^{2k}) = \sum_{k=0}^n 3 \binom{3n}{3k} = 3 \cdot \sum_{k=0}^n \binom{3n}{3k}.$$

Następnie obliczymy tę samą sumę bez odwoływania się do wzoru Newtona. Mamy wtedy:

$$\begin{aligned} (1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n} &= \\ &= (1 + 1)^{3n} + (1 + \varepsilon)^{3n} + (1 + \varepsilon^2)^{3n} = \\ &= 2^{3n} + (-\varepsilon^2)^{3n} + (-\varepsilon)^{3n} = \\ &= 2^{3n} + (-1)^{3n} \varepsilon^{6n} + (-1)^{3n} \varepsilon^{3n} = \\ &= 2^{3n} + (-1)^n (\varepsilon^3)^n + (-1)^n (\varepsilon^3)^n = \\ &= 2^{3n} + (-1)^n + (-1)^n = \\ &= 2^{3n} + 2 \cdot (-1)^n. \end{aligned}$$

W tym dowodzie korzystaliśmy z oczywistych równości:

$$(-1)^{3n} = (-1)^n, \quad 1 + \varepsilon = -\varepsilon^2, \quad 1 + \varepsilon^2 = -\varepsilon.$$

Porównując wyniki obu obliczeń, otrzymamy:

$$3 \cdot \sum_{k=0}^n \binom{3n}{3k} = 8^n + 2 \cdot (-1)^n,$$

czyli ostatecznie

$$\sum_{k=0}^n \binom{3n}{3k} = \frac{8^n + 2 \cdot (-1)^n}{3}.$$

9. Nieporządki

W tym paragrafie rozwiążemy znane nam już zadanie o liczbie nieporządków. Mamy zadanie:

- Piszemy n listów i adresujemy n kopert. Na ile sposobów możemy włożyć te listy do kopert tak, by żaden list nie trafił do właściwej koperty?

Ponumerujemy listy i koperty liczbami od 1 do n ; zakładamy przy tym, że list o numerze k powinien trafić do koperty o numerze k . Popatrzmy teraz na ciąg numerów listów włożonych do kopert: a_1 jest numerem listu włożonego do koperty z numerem 1, a_2 jest numerem listu w kopercie z numerem 2 i tak dalej. Ogólnie a_k jest numerem listu włożonego do koperty o numerze k . Oczywiście ciąg liczb $(a_1, a_2, \dots, a_n)$ jest permutacją zbioru liczb od 1 do n . Będziemy używać znanego oznaczenia permutacji: permutację $(a_1, a_2, \dots, a_{n-1}, a_n)$ oznaczamy symbolem

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ a_1 & a_2 & \dots & a_{n-1} & a_n \end{pmatrix}$$

wskazując w ten sposób w górnym wierszu numery kopert i pod nimi w dolnym wierszu numery listów, które trafiły do kolejnych kopert.

Przypomnijmy, że liczba k jest **punktem stałym** permutacji $(a_1, \dots, a_n)$, jeśli $a_k = k$, tzn. jeśli liczba a_k stoi na swoim, tzn. k -tym miejscu. Interesuje nas liczba **nieporządków**, czyli tych permutacji, które nie mają punktów stałych, tzn. permutacji $(a_1, \dots, a_k)$ takich, że żadna liczba a_k nie stoi na swoim miejscu:

$$D_n = |\{(a_1, \dots, a_n) : \forall k (a_k \neq k)\}|.$$

Przyjrzyjmy się, w jaki sposób możemy pogrupować nieporządki. Popatrzmy na n -tą kopertę. Mógł do niej trafić jeden z $n-1$ listów: każdy z wyjątkiem n -tego. Niech zatem będzie to list o numerze k . Mamy teraz dwa przypadki.

Przypadek 1. List o numerze n trafił do koperty z numerem k . Inaczej mówiąc, listy z numerami n i k „zamieniły się” kopertami. Mamy więc sytuację:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & k & \dots & n-1 & n \\ a_1 & a_2 & a_3 & \dots & n & \dots & a_{n-1} & k \end{pmatrix}$$

Oczywiście wtedy pozostałe listy (a jest ich $n-2$) muszą też być „wymieszane”, czyli ich numery muszą tworzyć nieporządek zbioru pozostałych liczb:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & k-1 & k+1 & \dots & n-1 \\ a_1 & a_2 & a_3 & \dots & a_{k-1} & a_{k+1} & \dots & a_{n-1} \end{pmatrix}.$$

Tak włożyć te $n-2$ listy do kopert można na D_{n-2} sposobów. Inaczej mówiąc, istnieją D_{n-2} nieporządki n liczb, w których na n tym miejscu stoi dana liczba k i na k -tym miejscu stoi liczba n . Uwzględniając liczbę możliwych k (jest ich $n-1$) widzimy, że w tym przypadku mamy łącznie $(n-1)D_{n-2}$ sposobów włożenia listów do kopert.

Popatrzmy na przykład. Przypuśćmy, że listy o numerach 5 i 2 zamieniły się miejscami. Istnieją 2 nieporządki zbioru liczb $\{1, 3, 4\}$:

$$\begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 3 & 4 \\ 4 & 3 & 1 \end{pmatrix}.$$

Z nich powstają 2 nieporządki liczb od 1 do 5, w których 2 i 5 zamieniły się miejscami:

$$\begin{pmatrix} 1 & 3 & 4 \\ 3 & 4 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 3 & 4 \\ 4 & 3 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

Przypadek 2. List o numerze n trafił do koperty z numerem l , przy czym $k \neq l$. Mamy więc sytuację:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & l & \dots & n-1 & n \\ a_1 & a_2 & a_3 & \dots & n & \dots & a_{n-1} & k \end{pmatrix}.$$

Wtedy na chwilę przekładamy listy: list o numerze n wkładamy do właściwej (tzn. n -tej) koperty, a list o numerze k wkładamy do koperty z numerem l (czyli zamieniamy miejscami k -ty i n -ty list):

$$\begin{pmatrix} 1 & 2 & 3 & \dots & l & \dots & n-1 & n \\ a_1 & a_2 & a_3 & \dots & k & \dots & a_{n-1} & n \end{pmatrix}.$$

Po tej zamianie mamy jeden list (o numerze n) we właściwej kopercie i pozostałe $n-1$ listów dokładnie wymieszanych, tzn. ich numery tworzą nieporządek $n-1$ liczb od 1 do $n-1$:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & l & \dots & n-1 \\ a_1 & a_2 & a_3 & \dots & k & \dots & a_{n-1} \end{pmatrix}.$$

Odwrotnie, jeśli mamy nieporządek liczb od 1 do $n-1$, to wkładamy list z numerem n do n -tej koperty, a następnie zamieniamy listy z numerami k i n , otrzymując nieporządek n numerów listów. Mamy D_{n-1} nieporządków liczb od 1 do $n-1$ i z każdego takiego nieporządku dostajemy jeden nieporządek n liczb, w którym na miejscu n -tym stoi liczba k . Uwzględniając liczbę możliwych k , dostajemy w tym przypadku $(n-1)D_{n-1}$ sposobów włożenia listów.

Popatrzmy na przykład. Istnieje 9 nieporządków liczb od 1 do 4:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Z każdego z tych dziewięciu nieporządków otrzymamy jeden nieporządek liczb od 1 do

5, w którym na miejscu piątym stoi liczba 2:

$$\begin{array}{lll}
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}, \\
 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} & \longrightarrow & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix},
 \end{array}$$

Łącznie mamy w obu przypadkach $(n-1) \cdot (D_{n-2} + D_{n-1})$ sposobów włożenia listów. Ponieważ $D_1 = 0$ oraz $D_2 = 1$, więc otrzymujemy równanie rekurencyjne:

$$D_1 = 0, \quad D_2 = 1, \quad D_n = (n-1) \cdot (D_{n-2} + D_{n-1}) \quad \text{dla } n > 2.$$

Zwróćmy uwagę na to, że otrzymaliśmy równanie rekurencyjne **drugiego rzędu**: do obliczenia kolejnego wyrazu ciągu musimy znać dwa poprzednie wyrazy. Zajmiemy się teraz poszukiwaniem wzoru ogólnego na liczbę nieporządków.

Definiujemy nowy ciąg:

$$E_n = D_n - nD_{n-1}$$

dla $n \geq 2$. Wtedy mamy:

$$E_n = D_n - nD_{n-1} = -(D_{n-1} - (n-1)D_{n-2}) = -E_{n-1}.$$

Ciąg (E_n) jest więc ciągiem geometrycznym o ilorazie -1 , którego początkowym wyrazem jest E_2 . Mamy zatem

$$E_n = E_2 \cdot (-1)^{n-2}.$$

Ponieważ $E_2 = D_2 - 2D_1 = 1$, więc ostatecznie otrzymujemy

$$E_n = (-1)^n,$$

czyli

$$D_n = nD_{n-1} + (-1)^n.$$

Otrzymane nowe równanie rekurencyjne ciągu (D_n) umiemy już rozwiązać metodą czynnika sumacyjnego. Podzielmy obie strony ostatniego równania przez $n!$:

$$\frac{D_n}{n!} = \frac{nD_{n-1}}{n!} + \frac{(-1)^n}{n!},$$

czyli

$$\frac{D_n}{n!} = \frac{D_{n-1}}{(n-1)!} + \frac{(-1)^n}{n!}.$$

Definiujemy ciąg (G_n) wzorem

$$G_n = \frac{D_n}{n!}$$

dla $n = 1, 2, 3, \dots$. Wtedy

$$G_n = G_{n-1} + \frac{(-1)^n}{n!},$$

skąd łatwo wynika, że

$$G_n = G_1 + \frac{(-1)^2}{2!} + \frac{(-1)^3}{3!} + \frac{(-1)^4}{4!} + \dots + \frac{(-1)^n}{n!}.$$

Ponieważ $G_1 = 0$, więc ostatni wzór możemy zapisać w postaci

$$G_n = 1 + \frac{(-1)^1}{1!} + \frac{(-1)^2}{2!} + \frac{(-1)^3}{3!} + \dots + \frac{(-1)^n}{n!}.$$

Stąd otrzymujemy ostatecznie

$$D_n = n! \left(1 + \frac{(-1)^1}{1!} + \frac{(-1)^2}{2!} + \frac{(-1)^3}{3!} + \dots + \frac{(-1)^n}{n!} \right) = n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}$$

dla $n = 1, 2, 3, \dots$. Dla dużych n mamy znane już przybliżenie $D_n \approx n! \cdot e^{-1} \approx 0,367879n$.

10. Sortowanie szybkie

Analizując średni czas działania algorytmu tzw. sortowania szybkiego (ang. quicksort) dochodzimy do następującego równania rekurencyjnego:

$$C_0 = 0, \quad C_n = n - 1 + \frac{2}{n} \cdot \sum_{k=0}^{n-1} C_k \quad \text{dla } n \geq 1.$$

Zauważmy, że każdy wyraz C_n (dla $n \geq 1$) ciągu określonego tym równaniem zależy od wszystkich wyrazów poprzednich. Pierwszym krokiem na drodze do znalezienia wzoru ogólnego będzie zmniejszenie rzędu rekurencji. Pomnożmy obie strony równania

$$C_n = n - 1 + \frac{2}{n} \cdot \sum_{k=0}^{n-1} C_k$$

przez n . Otrzymamy równanie

$$nC_n = n(n-1) + 2 \sum_{k=0}^{n-1} C_k.$$

Podstawmy w tym równaniu $n+1$ w miejsce n :

$$(n+1)C_{n+1} = n(n+1) + 2 \sum_{k=0}^n C_k.$$

Następnie odejmijmy stronami otrzymane równania:

$$(n+1)C_{n+1} - nC_n = n(n+1) - n(n-1) + 2C_n,$$

czyli

$$(n+1)C_{n+1} = (n+2)C_n + 2n.$$

Otrzymaliśmy równanie rekurencyjne liniowe pierwszego rzędu, które możemy rozwiązać metodą czynnika sumacyjnego. Podzielmy teraz obie strony otrzymanego równania przez $(n+1)(n+2)$

$$\frac{C_{n+1}}{n+2} = \frac{C_n}{n+1} + \frac{2n}{(n+1)(n+2)}$$

i wprowadźmy ciąg pomocniczy (D_n) określony wzorem

$$D_n = \frac{C_n}{n+1}$$

dla $n = 0, 1, 2, \dots$. Mamy wówczas

$$D_{n+1} = D_n + \frac{2n}{(n+1)(n+2)} = D_n + \frac{4}{n+2} - \frac{2}{n+1}$$

dla $n = 0, 1, 2, \dots$. Stąd dostajemy

$$D_n = D_0 + \sum_{k=0}^{n-1} \frac{4}{k+2} - \sum_{k=0}^{n-1} \frac{2}{k+1}.$$

Ponieważ $C_0 = 0$, więc $D_0 = 0$. Przyjmijmy następnie oznaczenie

$$H_0 = 0, \quad H_n = \sum_{k=1}^n \frac{1}{k} \quad \text{dla } n \geq 0.$$

Liczby H_n nazywamy **liczbami harmonicznymi**. Wówczas

$$\sum_{k=0}^{n-1} \frac{4}{k+2} = 4 \cdot \sum_{k=2}^{n+1} \frac{1}{k} = 4 \cdot (H_{n+1} - 1)$$

oraz

$$\sum_{k=0}^{n-1} \frac{2}{k+1} = 2 \cdot \sum_{k=1}^n \frac{1}{k} = 2H_n.$$

Stąd wynika, że

$$D_n = 4(H_{n+1} - 1) - 2H_n = 2H_{n+1} + 2(H_{n+1} - H_n) - 4 = 2H_{n+1} + \frac{2}{n+1} - 4.$$

Ponieważ $H_{n+1} = H_n + \frac{1}{n+1}$, więc

$$D_n = 2H_n + \frac{4}{n+1} - 4 = 2H_n - \frac{4n}{n+1}.$$

Stąd ostatecznie otrzymujemy

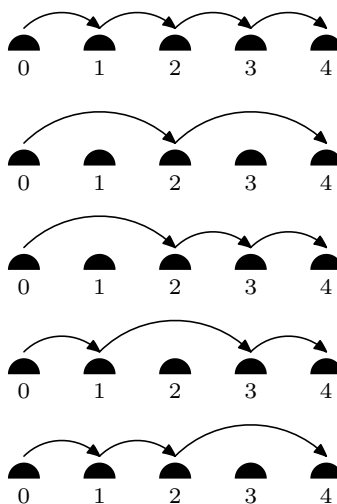
$$C_n = (n+1)D_n = 2(n+1)H_n - 4n$$

dla $n = 0, 1, 2, \dots$

11. Ciąg Fibonacciego

Ciąg liczb Fibonacciego pojawił się po raz pierwszy w książce Leonarda z Pizy (zwanego Fibonaccim) *Liber abaci* przy okazji zadania o rozmnażaniu królików. Zobaczmy teraz inne zadanie kombinatoryczne prowadzące do tego samego ciągu.

Zadanie. Żaba skacze z kamienia na kamień. Kamienie leżą jeden za drugim i są ponumerowane liczbami naturalnymi od zera; żaba startuje z kamienia zerowego. W jednym skoku potrafi ona przeskoczyć z jednego kamienia na następny lub o dwa kamienie dalej. Żaba może wykonywać po sobie skoki różnych długości. Na przykład, na czwarty kamień może dostać się skacząc cztery razy na odległość jednego kamienia lub skacząc dwa razy, za każdym razem na odległość dwóch kamieni, lub też skacząc raz na odległość dwóch kamieni i dwa razy na odległość jednego kamienia. Tę ostatnią możliwość może zrealizować na trzy sposoby, skok podwójny może być pierwszym, drugim lub trzecim skokiem. Oto możliwe drogi żaby na czwarty kamień:

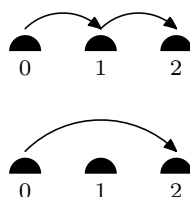


Łącznie ma więc pięć różnych sposobów dostania się na czwarty kamień. A ile istnieje sposobów dostania się na n -ty kamień?

Oznaczmy przez F_n liczbę dróg żaby na n -ty kamień. Oczywiście $F_1 = 1$. Na kamień z numerem 1 żaba może dostać się tylko w jeden sposób – ma wykonać jeden pojedynczy skok:



Następnie $F_2 = 2$. Na kamień z numerem 2 żaba może dostać się dwoma sposobami – wykonać dwa skoki pojedyncze lub jeden podwójny:



Zobaczmy teraz, na ile sposobów żaba może się dostać na kamień o numerze $n + 2$. Ma ona F_n różnych dróg na kamień o numerze n i F_{n+1} dróg na kamień o numerze $n + 1$. Ponieważ ostatni skok żaby jest skokiem podwójnym z kamienia o numerze n lub pojedynczym z kamienia o numerze $n + 1$, więc łącznie istnieje $F_n + F_{n+1}$ dróg żaby na kamień $n + 2$. A więc $F_{n+2} = F_{n+1} + F_n$. Zatem na trzeci kamień żaba może dostać się na $1 + 2 = 3$ sposoby, na czwarty na $2 + 3 = 5$ sposobów i tak dalej. Zauważmy, że jeśli przyjmiemy $F_0 = 1$ (co jest całkiem naturalne: istnieje jeden sposób dostania się na kamień o numerze 0, mianowicie nie robić nic), to okaże się, że $F_2 = F_0 + F_1$. Zatem ciąg (F_n) jest określony wzorami

$$F_0 = 1, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n \quad \text{dla } n \geq 0.$$

Otrzymane równanie rekurencyjne jest równaniem drugiego rzędu; widzieliśmy już takie równania przy okazji nieporządków. Jest to tzw. równanie liniowe (kolejny wyraz jest kombinacją liniową poprzednich) jednorodne (nie ma „wyrazu wolnego”) o stałych współczynnikach (w powyższym wzorze są one równe 1). Istnieje dość prosta metoda znajdowania wzoru ogólnego dla ciągów określonych równaniami liniowymi jednorodnymi o stałych współczynnikach. W następnym paragrafie pokażemy tę metodę dla ciągów określonych takimi równaniami drugiego rzędu.

12. Równania rekurencyjne liniowe jednorodne drugiego rzędu o stałych współczynnikach

Mówimy, że ciąg (t_n) liczb zespolonych spełnia równanie rekurencyjne liniowe, jednorodne o stałych współczynnikach, jeśli istnieją liczby $a_k, a_{k-1}, \dots, a_1, a_0$ takie, że $a_k \neq 0$, $a_0 \neq 0$ oraz dla wszystkich liczb naturalnych n zachodzi równość

$$a_k \cdot t_{n+k} + a_{k-1} \cdot t_{n+k-1} + \dots + a_1 \cdot t_{n+1} + a_0 \cdot t_n = 0. \quad (4.1)$$

Mówimy też, że to równanie rekurencyjne jest równaniem rzędu k .

Jeśli ciąg liczb zespolonych (t_n) spełnia równanie rekurencyjne rzędu k , to każdy wyraz tego ciągu, począwszy od a_k , jest jednoznacznie określony za pomocą k poprzednich wyrazów. Na przykład, dla ciągu określonego równaniem (4.1) mamy

$$t_{n+k} = -\frac{a_{k-1}}{a_k} \cdot t_{n+k-1} - \dots - \frac{a_1}{a_k} \cdot t_{n+1} - \frac{a_0}{a_k} \cdot t_n. \quad (4.2)$$

Jeśli będziemy znali pierwsze k wyrazów tego ciągu, to za pomocą równości (4.2) będziemy mogli wyznaczyć wszystkie następne wyrazy tego ciągu. Zauważmy również, że z warunku $a_k \neq 0$ wynika, iż możemy ograniczyć się do rozpatrywania równań rekurencyjnych postaci (4.1), w których $a_k = 1$. Wystarczy bowiem obie strony naszego równania rekurencyjnego podzielić przez a_k , by otrzymać równanie równoważne.

Zauważamy następnie, że jeśli dwa ciągi liczb zespolonych (t_n) i (u_n) spełniają równanie rekurencyjne (4.1), to ciąg (v_n) określony wzorem

$$v_n = c \cdot t_n + d \cdot u_n$$

(dla $n = 0, 1, 2, \dots$) też spełnia to równanie. Mianowicie

$$\begin{aligned} a_k v_{n+k} + a_{k-1} \cdot v_{n+k-1} + \dots + a_1 \cdot v_{n+1} + a_0 \cdot v_n &= \\ &= c \cdot (a_k t_{n+k} + a_{k-1} \cdot t_{n+k-1} + \dots + a_1 \cdot t_{n+1} + a_0 \cdot t_n) + \\ &+ d \cdot (a_k u_{n+k} + a_{k-1} \cdot u_{n+k-1} + \dots + a_1 \cdot u_{n+1} + a_0 \cdot u_n) = \\ &= c \cdot 0 + d \cdot 0 = 0. \end{aligned}$$

Stąd wynika, że ciągi liczb zespolonych spełniające równanie rekurencyjne (4.1) tworzą podprzestrzeń liniową przestrzeni wszystkich ciągów o wyrazach zespolonych. Ponieważ wyrazy $t_0, t_1, \dots, t_{k-1}$ wyznaczają jednoznacznie cały ciąg, więc ta podprzestrzeń ma wymiar k . Stąd wynika, że jeśli znajdziemy k liniowo niezależnych rozwiązań równania (4.1), to każde rozwiązanie równania będzie pewną kombinacją liniową tych k rozwiązań. W przypadku $k = 2$ chcemy zatem znaleźć dwa liniowo niezależne rozwiązania.

Nietrudno zauważyć, że równania rekurencyjne jednorodne rzędu 1 definiują ciągi geometryczne:

$$t_{n+1} = q \cdot t_n.$$

Próbujemy znaleźć ciągi geometryczne spełniające równanie rzędu 2. Przypuśćmy więc, że mamy dany ciąg liczb zespolonych (t_n) spełniający równanie

$$t_{n+2} + a \cdot t_{n+1} + b \cdot t_n = 0. \quad (4.3)$$

Szukamy takiego ilorazu q , różnego od zera, by ciąg określony wzorem $t_n = q^n$ spełniał równanie (4.3). Ten iloraz q musiałby zatem spełniać równanie:

$$q^{n+2} + aq^{n+1} + bq^n = 0,$$

czyli

$$q^2 + aq + b = 0. \quad (4.4)$$

A zatem, jeśli liczba q jest ilorazem ciągu geometrycznego spełniającego równanie rekurencyjne (4.3), to jest ona pierwiastkiem równania kwadratowego (4.4). Nietrudno zauważyć, że i na odwrót, jeśli liczba q jest pierwiastkiem równania kwadratowego (4.4), to ciąg geometryczny określony wzorem $t_n = q^n$ spełnia równanie rekurencyjne (4.3). Równanie

$$x^2 + ax + b = 0 \quad (4.5)$$

jest zwykle nazywane **równaniem charakterystycznym** równania rekurencyjnego (4.3). Mamy teraz dwa przypadki w zależności od liczby rozwiązań równania charakterystycznego.

Przypadek 1. Równanie charakterystyczne (4.5) ma dwa różne pierwiastki (rzeczywiste lub zespolone) q_1 i q_2 . Wtedy mamy dwa ciągi geometryczne spełniające równanie (4.3). Rozwiązanie ogólne równania rekurencyjnego (4.3) ma zatem postać

$$t_n = c \cdot q_1^n + d \cdot q_2^n$$

dla $n = 0, 1, 2, \dots$. Współczynniki c i d wyznaczamy z układu równań otrzymanego przez wstawienie $n = 0$ i $n = 1$ do rozwiązania ogólnego. Przyjmując $n = 0$, otrzymujemy równanie

$$c + d = t_0.$$

Przyjmując $n = 1$, otrzymujemy równanie

$$q_1 c + q_2 d = t_1.$$

Układ równań

$$\begin{cases} c + d = t_0 \\ q_1 c + q_2 d = t_1 \end{cases}$$

zawsze ma rozwiązanie, gdyż

$$\begin{vmatrix} 1 & 1 \\ q_1 & q_2 \end{vmatrix} = q_2 - q_1 \neq 0.$$

Zatem dwa początkowe wyrazy ciągu (t_n) pozwalają wyznaczyć jednoznacznie liczby c i d , a więc określają jednoznacznie cały ciąg (t_n) .

Popatrzmy na kilka przykładów. Rozwiążmy najpierw równanie rekurencyjne

$$t_0 = 3, \quad t_1 = 7, \quad t_{n+2} - 5t_{n+1} + 6t_n = 0 \quad \text{dla } n \geq 0.$$

Równanie charakterystyczne $x^2 - 5x + 6 = 0$ ma dwa pierwiastki rzeczywiste $x_1 = 2$ oraz $x_2 = 3$. Stąd wynika, że ciąg (t_n) jest określony wzorem ogólnym

$$t_n = c \cdot 2^n + d \cdot 3^n$$

dla $n = 0, 1, 2, \dots$. Współczynniki c i d wyznaczamy z układu równań powstałego przez podstawienie $n = 0$ i $n = 1$:

$$\begin{cases} c + d = 3 \\ 2c + 3d = 7 \end{cases}$$

Rozwiązując ten układ równań, otrzymujemy $c = 2$ i $d = 1$. Zatem

$$t_n = 2^{n+1} + 3^n$$

dla $n = 0, 1, 2, \dots$

Możemy teraz wyznaczyć wzór ogólny dla ciągu liczb Fibonacciego. Równanie rekurencyjne ciągu F_n ma postać

$$F_0 = 1, \quad F_1 = 1, \quad F_{n+2} - F_{n+1} - F_n = 0 \quad \text{dla } n \geq 0.$$

Jego równanie charakterystyczne

$$x^2 - x - 1 = 0$$

ma dwa pierwiastki

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad \text{oraz} \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

Zatem rozwiązanie ogólne rozważanego równania rekurencyjnego ma postać

$$F_n = c \cdot \alpha^n + d \cdot \beta^n$$

dla pewnych współczynników c i d . Współczynniki te wyznaczamy z układu równań

$$\begin{cases} c + d = 1 \\ \alpha c + \beta d = 1 \end{cases}$$

Ten układ równań ma następujące rozwiązanie:

$$c = \frac{\alpha}{\sqrt{5}}, \quad d = -\frac{\beta}{\sqrt{5}}.$$

Stąd otrzymujemy

$$F_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right).$$

Otrzymany wzór ogólny jest nazywany **wzorem Bineta**.

Rozwiążmy jeszcze jedno równanie rekurencyjne

$$t_0 = 1, \quad t_1 = 4, \quad t_{n+2} - 2t_{n+1} + 2t_n = 0 \quad \text{dla } n \geq 0.$$

Równanie charakterystyczne $x^2 - 2x + 2 = 0$ ma dwa pierwiastki zespolone

$$x_1 = 1 + i \quad \text{oraz} \quad x_2 = 1 - i.$$

Stąd wynika, że ciąg (t_n) jest określony wzorem ogólnym

$$t_n = c \cdot (1 + i)^n + d \cdot (1 - i)^n$$

dla $n = 0, 1, 2, \dots$. Współczynniki c i d wyznaczamy z układu równań powstałego przez podstawienie $n = 0$ i $n = 1$:

$$\begin{cases} c + d = 2 \\ (1 + i)c + (1 - i)d = 2 \end{cases}$$

Rozwiązując ten układ równań, otrzymujemy

$$c = \frac{1 - 3i}{2} \quad \text{oraz} \quad d = \frac{1 + 3i}{2}.$$

Zatem

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

dla $n = 0, 1, 2, \dots$

Jest oczywiste, że ciąg (t_n) ma wyrazy rzeczywiste (nawet całkowite). Otrzymany wzór odwołuje się jednak do liczb urojonych. Okazuje się, że dość łatwo możemy z powyższych wzorów zespolonych otrzymać postać rzeczywistą rozwiązania. Mamy bowiem

$$\begin{aligned} 1 + i &= \sqrt{2} \cdot \left(\cos \frac{\pi}{4} + i \cdot \sin \frac{\pi}{4} \right), \\ 1 - i &= \sqrt{2} \cdot \left(\cos \frac{\pi}{4} - i \cdot \sin \frac{\pi}{4} \right). \end{aligned}$$

Ze wzoru de Moivre'a otrzymujemy

$$\begin{aligned} t_n &= \frac{1 - 3i}{2} \cdot (1 + i)^n + \frac{1 + 3i}{2} \cdot (1 - i)^n = \\ &= \frac{1 - 3i}{2} \cdot (\sqrt{2})^n \cdot \left(\cos \frac{n\pi}{4} + i \cdot \sin \frac{n\pi}{4} \right) + \frac{1 + 3i}{2} \cdot (\sqrt{2})^n \cdot \left(\cos \frac{n\pi}{4} - i \cdot \sin \frac{n\pi}{4} \right) = \\ &= \frac{(\sqrt{2})^n}{2} \cdot \left((1 - 3i) \left(\cos \frac{n\pi}{4} + i \cdot \sin \frac{n\pi}{4} \right) + (1 + 3i) \left(\cos \frac{n\pi}{4} - i \cdot \sin \frac{n\pi}{4} \right) \right) = \\ &= (\sqrt{2})^n \cdot \left(\cos \frac{n\pi}{4} + 3 \sin \frac{n\pi}{4} \right). \end{aligned}$$

Pokażemy teraz, że tę postać rzeczywistą możemy uzyskać także nieco inną metodą.

Rozpatrujemy zatem przypadek, gdy równanie charakterystyczne (4.5) ma współczynniki rzeczywiste, ale nie ma pierwiastków rzeczywistych (czyli ma dwa sprzężone pierwiastki zespolone). Oznacza to, że w równaniu (4.5) mamy $a^2 < 4b$. Stąd wynika, że $b > 0$. Niech więc $b = r^2$. Wtedy

$$\left(\frac{a}{2r} \right)^2 = \frac{a^2}{4b} < 1.$$

Zatem

$$\left| \frac{a}{2r} \right| < 1.$$

Stąd wynika, że istnieje liczba φ taka, że

$$\frac{a}{2r} = -\cos \varphi.$$

Równanie rekurencyjne (4.3) przyjmuje teraz postać

$$t_{n+2} - 2r \cos \varphi \cdot t_{n+1} + r^2 t_n = 0. \quad (4.6)$$

Można teraz sprawdzić, że ciąg (t_n) określony wzorem

$$t_n = r^n (c \cdot \cos n\varphi + d \cdot \sin n\varphi)$$

(dla $n = 0, 1, 2, \dots$) jest rozwiązaniem ogólnym równania (4.6). W dowodzie korzysta się z następujących tożsamości trygonometrycznych:

$$2 \cos \alpha \cos \beta = \cos(\alpha + \beta) + \cos(\alpha - \beta)$$

oraz

$$2 \cos \alpha \sin \beta = \sin(\alpha + \beta) + \sin(\beta - \alpha).$$

Szczegóły tego dowodu pozostawiamy jako ćwiczenie.

Przypadek 2. Równanie charakterystyczne (4.5) ma jeden pierwiastek podwójny q . Mamy wtedy tylko jeden ciąg geometryczny (q^n) spełniający równanie rekurencyjne (4.3). Potrzebne jest drugie rozwiązanie. Sprawdźmy, że takim drugim rozwiązaniem jest ciąg liczb postaci $n \cdot q^n$. Mianowicie równanie charakterystyczne naszego równania rekurencyjnego ma postać

$$x^2 + ax + b = 0.$$

Takie równanie ma jeden pierwiastek podwójny, gdy $a^2 = 4b$ i ten pierwiastek jest równy

$$x = -\frac{a}{2}.$$

Ponieważ q jest tym pierwiastkiem podwójnym, więc

$$2q + a = 0.$$

Teraz sprawdzamy, że ciąg (nq^n) spełnia równanie rekurencyjne (4.3):

$$t_{n+2} + at_{n+1} + bt_n = 0,$$

czyli

$$(n+2)q^{n+2} + a(n+1)q^{n+1} + bnq^n = 0.$$

Przekształcamy to równanie w sposób równoważny:

$$\begin{aligned}
 4(n+2)q^{n+2} + 4a(n+1)q^{n+1} + 4bnq^n &= 0, \\
 4(n+2)q^{n+2} + 4a(n+1)q^{n+1} + a^2nq^n &= 0, \\
 q^n \cdot (4(n+2)q^2 + 4a(n+1)q + a^2n) &= 0, \\
 q^n \cdot (n(4q^2 + 4aq + a^2) + 4q(2q + a)) &= 0, \\
 q^n \cdot (n(2q + a)^2 + 4q(2q + a)) &= 0, \\
 q^n \cdot (2q + a) \cdot (n(2q + a) + 4q) &= 0.
 \end{aligned}$$

Ostatnie równanie jest spełnione, gdyż

$$2q + a = 0.$$

Teraz mamy już dwa niezależne rozwiązania równania rekurencyjnego (4.3):

$$t_n = q^n \quad \text{oraz} \quad t_n = nq^n,$$

a więc mamy rozwiązanie ogólne:

$$t_n = c \cdot q^n + d \cdot nq^n,$$

czyli

$$t_n = (c + dn) \cdot q^n$$

dla $n = 0, 1, 2, \dots$. Współczynniki c i d wyznaczamy – podobnie, jak w przypadku 1 – z układu równań otrzymanego przez podstawienie $n = 0$ i $n = 1$ do wzoru ogólnego:

$$\begin{cases} c = t_0 \\ (c + d)q = t_1 \end{cases}$$

Znów dowolne wartości t_0 i t_1 wyznaczają jednoznacznie współczynniki c i d , a więc tym samym rozwiązanie równania rekurencyjnego.

Popatrzmy na jeden przykład. Rozwiążmy równanie rekurencyjne

$$t_0 = 1, \quad t_1 = 6, \quad t_{n+2} - 4t_{n+1} + 4t_n = 0 \quad \text{dla } n \geq 0.$$

Równanie charakterystyczne $x^2 - 4x + 4 = 0$ ma jeden podwójny pierwiastek rzeczywisty $x = 2$. Stąd wynika, że ciąg (t_n) jest określony wzorem ogólnym

$$t_n = c \cdot 2^n + d \cdot n \cdot 2^n = (c + dn) \cdot 2^n$$

dla $n = 0, 1, 2, \dots$. Współczynniki c i d wyznaczamy z układu równań powstałego przez podstawienie $n = 0$ i $n = 1$:

$$\begin{cases} c = 3 \\ (c + d) \cdot 2 = 6 \end{cases}$$

Rozwiązując ten układ równań, otrzymujemy $c = 1$ i $d = 2$. Zatem

$$t_n = (2n + 1) \cdot 2^n$$

dla $n = 0, 1, 2, \dots$

13. Równania rekurencyjne liniowe jednorodne wyższych rzędów o stałych współczynnikach

Rozpatrzone wyżej dwa przypadki dają w sumie pełną analizę równania rekurencyjnego (4.3) czyli równania liniowego jednorodnego o stałych współczynnikach, rzędu 2. Przypadek ogólny równań jednorodnych wyższych rzędów rozpatruje się podobnie. Dla równania (4.1) w analogiczny sposób definiujemy jego **równanie charakterystyczne**:

$$a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0 = 0. \quad (4.7)$$

Następnie znajdujemy jego wszystkie pierwiastki (uwzględniając pierwiastki zespolone i wielokrotne)

$$r_1, r_2, \dots, r_k.$$

Przypuśćmy najpierw, że wszystkie pierwiastki są różne (tzn. wszystkie mają krotność 1). Wtedy rozwiązanie ogólne ma postać

$$t_n = c_1 r_1^n + c_2 r_2^n + \dots + c_k r_k^n. \quad (4.8)$$

Przypuśćmy następnie, że niektóre pierwiastki równania (4.7) pokrywają się (czyli mamy do czynienia z pierwiastkiem wielokrotnym). Dla ustalenia uwagi, niech na przykład $r_1 = r_2 = \dots = r_l = r$, tzn. r jest pierwiastkiem krotności l . Wtedy zamiast sumy

$$c_1 r_1^n + \dots + c_l r_l^n$$

w rozwiązaniu (4.8) będziemy mieli sumę

$$r^n (c_1 + c_2 n + c_3 n^2 + \dots + c_l n^{l-1}).$$

W taki sam sposób postępujemy dla każdego pierwiastka wielokrotnego, rzeczywistego lub zespolonego. Szczegółowe sformułowanie tego twierdzenia i jego dowód odłożymy do następnego wykładu.

14. Równania rekurencyjne liniowe niejednorodne drugiego rzędu o stałych współczynnikach

Zajmiemy się teraz równaniami niejednorodnymi. Przypuśćmy więc, że mamy równanie niejednorodne rzędu k :

$$a_k \cdot t_{n+k} + a_{k-1} \cdot t_{n+k-1} + \dots + a_1 \cdot t_{n+1} + a_0 \cdot t_n = f(n). \quad (4.9)$$

Zajmiemy się najpierw równaniami, w których funkcja f ma szczególną postać:

$$f(n) = c^n \cdot w(n),$$

gdzie c jest liczbą zespoloną, a $w(n)$ jest wielomianem stopnia d zmiennej n . Wtedy ciąg (t_n) spełnia pewne równanie rekurencyjne jednorodne rzędu $k+d+1$, którego wielomian charakterystyczny ma postać

$$(a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0)(r - c)^{d+1} = 0.$$

Takie równania już potrafimy rozwiązać. Musimy tylko zwrócić uwagę na to, że do rozwiązania tego równania potrzebujemy $k+d+1$ wartości początkowych. Mamy zaś podane tylko k wartości początkowych (bo równanie (4.9) jest rzędu k). Pozostałe $d+1$ wartości musimy sami wyznaczyć z równania (4.9). Pozostaje więc tylko uzasadnić, że równanie (2) rzeczywiście sprowadza się w taki sposób do równania jednorodnego. Nie przeprowadzimy tu dowodu w całej ogólności, ograniczymy się tylko do jednego przypadku, gdy równanie (4.9) jest rzędu 2 i wielomian $w(n)$ jest stopnia 1. Mamy zatem równanie

$$t_{n+2} + at_{n+1} + bt_n = c^n(pn + q). \quad (4.10)$$

Podstawiamy w nim za n kolejno $n+1$ i $n+2$:

$$t_{n+3} + at_{n+2} + bt_{n+1} = c^{n+1}(p(n+1) + q). \quad (4.11)$$

$$t_{n+4} + at_{n+3} + bt_{n+2} = c^{n+2}(p(n+2) + q). \quad (4.12)$$

Następnie mnożymy równanie (4.10) przez c^2 , równanie (4.11) przez $(-2c)$ i dodajemy otrzymane równania do równania (4.12). Nietrudno sprawdzić, że po prawej stronie otrzymamy zero i całe równanie będzie miało postać

$$t_{n+4} + (a - 2c)t_{n+3} + (b - 2ac + c^2)t_{n+2} + (ac^2 - 2bc)t_{n+1} + bc^2t_n = 0. \quad (4.13)$$

Równanie charakterystyczne tego równania rekurencyjnego ma postać

$$x^4 + (a - 2c)x^3 + (b - 2ac + c^2)x^2 + (ac^2 - 2bc)x + bc^2 = 0. \quad (4.14)$$

Teraz wystarczy zauważyć, że lewa strona równania (4.14) rozkłada się na czynniki

$$x^4 + (a - 2c)x^3 + (b - 2ac + c^2)x^2 + (ac^2 - 2bc)x + bc^2 = (x^2 + ax + b)(x - c)^2.$$

Zatem rzeczywiście ciąg (t_n) spełnia równanie rekurencyjne jednorodne, którego równanie charakterystyczne ma żadaną postać.

W podobny sposób można rozwiązać nieco bardziej skomplikowane równania niejednorodne. Jeśli funkcja f w równaniu (4.9) ma postać

$$f(n) = c_1^n \cdot w_1(n) + c_2^n \cdot w_2(n) + \dots,$$

gdzie $w_1(n), w_2(n), \dots$ są wielomianami stopni odpowiednio $d_1, d_2, \dots$, to ciąg (t_n) spełnia równanie rekurencyjne jednorodne, którego równaniem charakterystycznym jest

$$(a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0)(x - c_1)^{d_1+1}(x - c_2)^{d_2+1} \dots$$

Dowód tego stwierdzenia pominiemy.

15. Układy równań rekurencyjnych

Rozwiązanie układów równań rekurencyjnych omówimy na jednym przykładzie. Rozwiążemy układ równań

$$\begin{cases} t_0 = 2 \\ u_0 = 3 \\ t_{n+1} = 6t_n + 4u_n \\ u_{n+1} = t_n + 3u_n \end{cases}$$

Sprowadzimy ten układ równań do jednego równania liniowego drugiego rzędu. Najpierw w równaniu

$$t_{n+1} = 6t_n + 4u_n$$

podstawimy $n + 1$ w miejsce n . Otrzymamy

$$t_{n+2} = 6t_{n+1} + 4u_{n+1} = 6t_{n+1} + 4 \cdot (t_n + 3u_n) = 6t_{n+1} + 4t_n + 12u_n.$$

Teraz podstawiamy $4u_n = t_{n+1} - 6t_n$:

$$t_{n+2} = 6t_{n+1} + 4t_n + 3 \cdot (t_{n+1} - 6t_n) = 6t_{n+1} + 4t_n + 3t_{n+1} - 18t_n = 9t_{n+1} - 14t_n.$$

Otrzymaliśmy równanie rekurencyjne

$$t_{n+2} - 9t_{n+1} + 14t_n = 0.$$

Jego równaniem charakterystycznym jest:

$$x^2 - 9x + 14 = 0,$$

czyli

$$(x - 2)(x - 7) = 0.$$

Stąd wynika, że ciąg (t_n) jest określony wzorem ogólnym

$$t_n = c \cdot 7^n + d \cdot 2^n$$

dla $n = 0, 1, 2, \dots$. Współczynniki c i d obliczamy z układu równań

$$\begin{cases} c + d = t_0 = 2 \\ 7c + 2d = t_1 = 24 \end{cases}$$

Otrzymujemy $c = 4$ i $d = -2$. A więc

$$t_n = 4 \cdot 7^n - 2 \cdot 2^n = 4 \cdot 7^n - 2^{n+1}$$

dla $n = 0, 1, 2, \dots$. Wzór ogólny ciągu (u_n) otrzymujemy z równania $t_{n+1} = 6t_n + 4u_n$:

$$4u_n = t_{n+1} - 6t_n = 4 \cdot 7^{n+1} - 2^{n+2} - 24 \cdot 7^n + 2^{n+1} = 4 \cdot 7^n + 4 \cdot 2^{n+1},$$

czyli

$$u_n = 7^n + 2^{n+1}$$

dla $n = 0, 1, 2, \dots$

Ten układ równań, dzięki wyjątkowemu doborowi współczynników, można też rozwiązać prościej, nie odwołując się do rozwiązywania równań liniowych drugiego rzędu. Załóżmy bowiem, że

$$\begin{cases} t_0 + u_0 = 5 \\ t_{n+1} + u_{n+1} = 7 \cdot (t_n + u_n), \end{cases}$$

skąd dostajemy $t_n + u_n = 5 \cdot 7^n$ dla $n = 0, 1, 2, \dots$. Następnie

$$t_{n+1} = 4(t_n + u_n) + 2t_n = 2t_n + 20 \cdot 7^n.$$

Teraz zauważamy, że

$$t_{n+2} - 7t_{n+1} = 2t_{n+1} + 20 \cdot 7^{n+1} - 14t_n - 20 \cdot 7^{n+1} = 2 \cdot (t_{n+1} - 7t_n).$$

Stąd wynika, że

$$t_{n+1} - 7t_n = (t_1 - 7t_0) \cdot 2^n = (24 - 14) \cdot 2^n = 10 \cdot 2^n.$$

Zatem

$$t_{n+1} = 2t_n + 20 \cdot 7^n = 7t_n + 10 \cdot 2^n,$$

czyli

$$5t_n = 20 \cdot 7^n - 10 \cdot 2^n.$$

Ostatecznie

$$t_n = 4 \cdot 7^n - 2^{n+1}$$

dla $n = 0, 1, 2, \dots$. Wzór ogólny ciągu (u_n) otrzymujemy teraz z równości $t_n + u_n = 5 \cdot 7^n$:

$$u_n = 5 \cdot 7^n - t_n = 5 \cdot 7^n - 4 \cdot 7^n + 2^{n+1} = 7^n + 2^{n+1}$$

dla $n = 0, 1, 2, \dots$

16. Liczby Catalana

Przypomnijmy z wykładu 1, że liczbą Catalana C_n nazywamy liczbę funkcji niemalejących $f : [n] \rightarrow [n]$ spełniających warunek

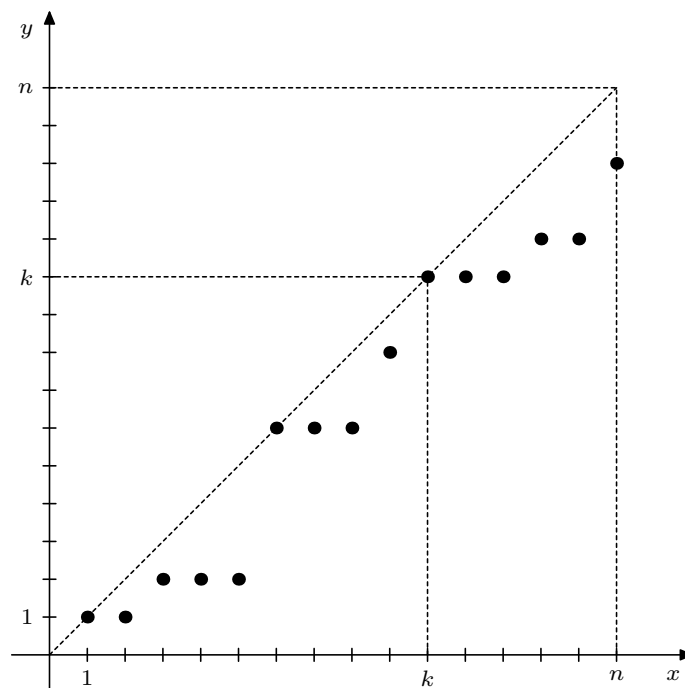
$$f(k) \leq k \quad \text{dla } k = 1, 2, \dots, n.$$

Warunek ten nazwiemy w skrócie **warunkiem Catalana** (spełnionym w zbiorze $[n]$). Przyjmujemy ponadto, że $C_0 = 1$. Poznaliśmy wzór ogólny:

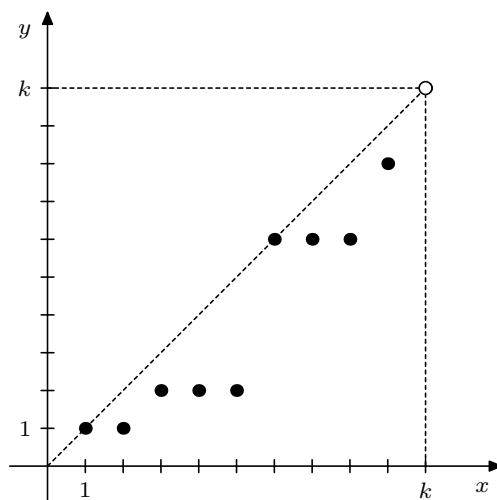
$$C_n = \frac{1}{n+1} \cdot \binom{2n}{n}$$

dla $n = 0, 1, 2, \dots$

W tym paragrafie poznamy równanie rekurencyjne, za pomocą którego można zdefiniować ciąg liczb Catalana. Główny pomysł wyjaśnimy najpierw na wykresie. Niech $f : [n] \rightarrow [n]$ będzie funkcją niemalejącą spełniającą warunek Catalana. Oto wykres takiej funkcji f (na rysunku przyjęto $n = 15$).

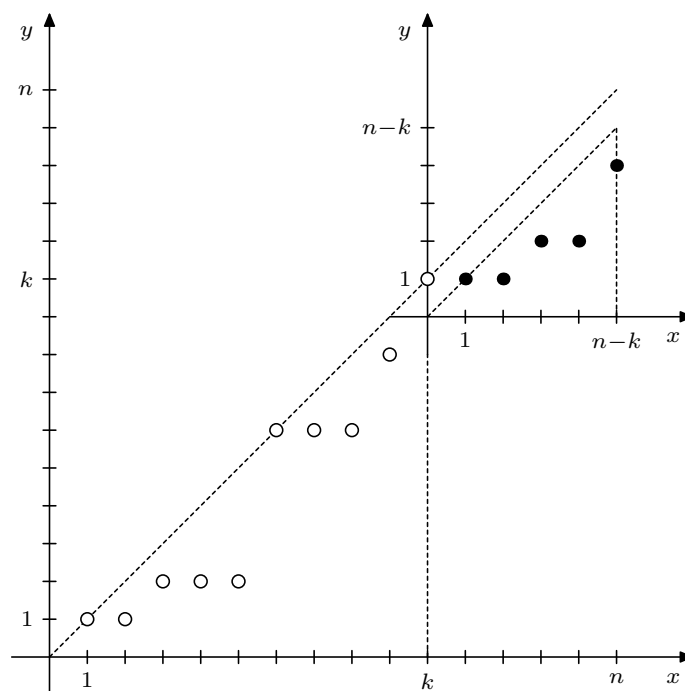


Warunek Catalana oznacza, że punkty tworzące ten wykres nie mogą leżeć ponad prostą o równaniu $y = x$. Niech k będzie największą liczbą x taką, że $f(x) = x$ (na rysunku mamy $k = 10$). Taka liczba istnieje, bo z warunku Catalana wynika, że $f(1) = 1$. Prosta pionowa o równaniu $x = k$ dzieli ten wykres na dwie części: na lewo od niej mamy wykres funkcji niemalejącej $f|_{[k-1] : [k-1] \rightarrow [k-1]}$ spełniającej warunek Catalana (w zbiorze $[k-1]$):



Oczywiście istnieje C_{k-1} takich funkcji. Zastanówmy się teraz, co się dzieje na prawo od prostej $x = k$. Po pierwsze zauważamy, że $f(k+1) = k$. Z warunku Catalana wynika

bowiem, że $f(k+1) \leq k+1$. Z drugiej strony liczba k była największą liczbą x taką, że $f(x) = x$. Zatem $f(k+1) < k+1$. Ponieważ funkcja f jest niemalejąca oraz $f(k) = k$, więc $f(k+1) \geq k$. Łącznie to daje $f(k+1) = k$. Ponieważ dla $x > k$ mamy $f(x) < x$, więc punkty wykresu funkcji f leżące na prawo od prostej $x = k$ nie mogą leżeć nad prostą o równaniu $y = x - 1$. Odpowiednio przesuwając osie układu współrzędnych, otrzymamy wykres pewnej funkcji niemalejącej $g : [n-k] \rightarrow [n-k]$ spełniającej warunek Catalana (w zbiorze $[n-k]$):



Istnieje C_{n-k} takich funkcji. Zatem każdy wykres funkcji niemalejącej $f : [n] \rightarrow [n]$ spełniającej warunek Catalana w zbiorze $[n]$ wyznacza jednoznacznie parę funkcji niemalejących spełniających warunek Catalana: jedną określoną w zbiorze $[k-1]$ i drugą określoną w zbiorze $[n-k]$. Odwrotnie, każda taka para funkcji wyznacza jednoznacznie funkcję f . Musimy bowiem przyjąć $f(k) = k$ i umieścić odpowiednio wysoko wykres drugiej funkcji (wiemy przy tym, jak wysoko: pierwsza wartość jest bowiem równa k). Ponieważ k może być dowolną z liczb od 1 do n , więc otrzymujemy równanie rekurencyjne

$$C_n = \sum_{k=1}^n C_{k-1} \cdot C_{n-k} = \sum_{k=0}^{n-1} C_k \cdot C_{n-k-1}$$

dla $n = 1, 2, 3, \dots$

Podamy teraz ścisłą definicję obu funkcji wyznaczonych przez funkcję f . Pierwszą funkcją jest oczywiście $f \upharpoonright [k-1]$. Drugą funkcję $g : [n-k] \rightarrow [n-k]$ definiujemy wzorem

$$g(x) = f(x+k) - k + 1 \quad \text{dla } x \in [n-k].$$

Oczywiście funkcja g jest niemalejąca. Ponadto

$$g(x) < x + k - k + 1 = x + 1,$$

czyli $g(x) \leq x$. To wynika z określenia liczby k : dla $x \geq 1$ mamy bowiem $f(x+k) < x+k$. Funkcja g spełnia więc rzeczywiście warunek Catalana w zbiorze $[n-k]$. Wyznaczenie wzoru definiującego funkcję f , gdy znane są funkcje $f \mid [k-1]$ i g pozostawiamy jako ćwiczenie.

Podsumowując, liczby Catalana mogą być zdefiniowane następującymi wzorami rekurencyjnymi:

$$C_0 = 1, \quad C_n = \sum_{k=0}^{n-1} C_k C_{n-k-1} \quad \text{dla } n \geq 1.$$

Korzystając z powyższego równania rekurencyjnego obliczymy kilka początkowych liczb Catalana:

$$\begin{aligned} C_0 &= 1, \\ C_1 &= C_0^2 = 1, \\ C_2 &= C_0 C_1 + C_1 C_0 = 2C_0 C_1 = 2, \\ C_3 &= C_0 C_2 + C_1 C_1 + C_2 C_0 = 2 + 1 + 2 = 5, \\ C_4 &= C_0 C_3 + C_1 C_2 + C_2 C_1 + C_3 C_0 = 5 + 2 + 2 + 5 = 14, \\ C_5 &= C_0 C_4 + C_1 C_3 + C_2 C_2 + C_3 C_1 + C_4 C_0 = 14 + 5 + 4 + 5 + 14 = 42. \end{aligned}$$

Pokażemy jeszcze jeden przykład zadania prowadzącego do liczb Catalana. Niech $\bullet$ będzie działaniem niełącznym w pewnym zbiorze A . Wtedy wynik n -krotnego wykonania tego działania na elementach $a_1, a_2, \dots, a_{n+1}$ zależy od rozmieszczenia nawiasów. Na przykład dla $n = 3$ mamy 5 sposobów rozmieszczenia nawiasów, gdy wykonujemy działanie $\bullet$ na elementach $a, b, c, d \in A$:

$$a \bullet (b \bullet (c \bullet d)), \quad a \bullet ((b \bullet c) \bullet d), \quad (a \bullet b) \bullet (c \bullet d), \quad (a \bullet (b \bullet c)) \bullet d, \quad ((a \bullet b) \bullet c) \bullet d.$$

Dla $n = 4$ mamy 14 sposobów rozmieszczenia nawiasów:

$$\begin{array}{llll} a \bullet (b \bullet (c \bullet (d \bullet e))) & (a \bullet b) \bullet (c \bullet (d \bullet e)) & (a \bullet (b \bullet c)) \bullet (d \bullet e) & (a \bullet (b \bullet (c \bullet d))) \bullet e \\ a \bullet (b \bullet ((c \bullet d) \bullet e)) & (a \bullet b) \bullet ((c \bullet d) \bullet e) & ((a \bullet b) \bullet c) \bullet (d \bullet e) & (a \bullet ((b \bullet c) \bullet d)) \bullet e \\ a \bullet ((b \bullet c) \bullet (d \bullet e)) & & & ((a \bullet b) \bullet (c \bullet d)) \bullet e \\ a \bullet ((b \bullet (c \bullet d)) \bullet e) & & & ((a \bullet (b \bullet c)) \bullet d) \bullet e \\ a \bullet (((b \bullet c) \bullet d) \bullet e) & & & (((a \bullet b) \bullet c) \bullet d) \bullet e \end{array}$$

Domyślamy się, że liczba rozmieszczeń nawiasów jest liczbą Catalana. Wykażemy, że tak jest.

Niech B_n będzie liczbą rozmieszczeń nawiasów przy n wykonywanych działaniach. Przyjmujemy, że $B_0 = 1$. Mamy teraz $n \geq 1$ i $n+1$ elementów $a_1, a_2, \dots, a_{n+1}$ zbioru A . Ostatnie działanie, które mamy wykonać dzieli te $n+1$ elementów na dwie grupy:

$$(a_1 \dots a_{k+1}) \bullet (a_{k+2} \dots a_{n+1}).$$

W pierwszej grupie musimy wykonać k działań, w drugiej $n-k-1$ działań. Oczywiście może być $k = 0$, gdy lewa grupa składa się tylko z jednego elementu:

$$a_1 \bullet (a_2 \dots a_{n+1}).$$

W prawej grupie musimy wykonać wtedy $n - 1$ działań. Z drugiej strony lewa grupa może składać się z co najwyżej n elementów; w prawej będzie wtedy tylko jeden element:

$$(a_1 \dots a_n) \bullet a_{n+1}.$$

W lewej grupie mamy wtedy do wykonania $n - 1$ działań, w prawej ani jednego. Podział

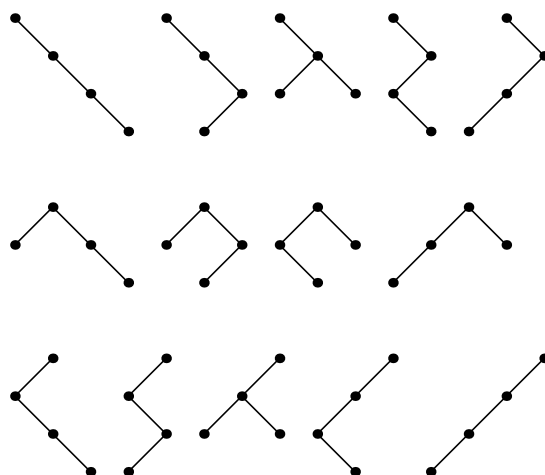
$$(a_1 \dots a_{k+1}) \bullet (a_{k+2} \dots a_{n+1})$$

może być dokonany na $B_k B_n - k - 1$ sposobów: możemy rozmieścić nawiasy w lewej grupie na B_k sposobów i na $B_n - k - 1$ sposobów w prawej. Stąd dostajemy równanie

$$B_n = B_0 B_{n-1} + B_1 B_{n-2} + \dots + B_{n-1} B_0 = \sum_{k=0}^{n-1} B_k B_{n-k-1}$$

dla $n = 1, 2, 3, \dots$. Otrzymaliśmy zatem to samo równanie co w przypadku liczb Catalana. Stąd wynika, że $B_n = C_n$ dla $n = 0, 1, 2, \dots$

Znamy wiele zadań prowadzących do liczb Catalana. Oto jeszcze dwa z nich. Istnieje 14 drzew mających 4 wierzchołki takich, że każdy wierzchołek ma co najwyżej 2 leżące bezpośrednio niżej (można od niego iść w lewo, w prawo, w obie strony lub w żadną):



Ogólnie: istnieje C_n drzew mających n wierzchołków o powyższej własności.

Liczby od 1 do 8 można na 14 sposobów ustawić w tablicy o 4 kolumnach i dwóch wierszach tak, by w każdej kolumnie i w każdym wierszu liczby były ustawione malejąco (licząc od góry i od lewej strony):

$$\begin{bmatrix} 8 & 7 & 6 & 5 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 6 & 4 \\ 5 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 6 & 3 \\ 5 & 4 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 6 & 2 \\ 5 & 4 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 5 & 4 \\ 6 & 3 & 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 7 & 5 & 3 \\ 6 & 4 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 5 & 2 \\ 6 & 4 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 4 & 3 \\ 6 & 5 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 7 & 4 & 2 \\ 6 & 5 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 6 & 5 & 4 \\ 7 & 3 & 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 8 & 6 & 5 & 3 \\ 7 & 4 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 6 & 5 & 2 \\ 7 & 4 & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 6 & 4 & 3 \\ 7 & 5 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 8 & 6 & 4 & 2 \\ 7 & 5 & 3 & 1 \end{bmatrix}$$

Ogólnie: istnieje C_n tablic o n kolumnach i 2 wierszach, w których liczby od 1 do $2n$ są ustawione zgodnie z powyższymi regułami (tzn. w obu wierszach liczby tworzą ciągi malejące, a w każdej kolumnie liczba większa stoi nad mniejszą).

Wykazanie, że w obu powyższych zadaniach poszukiwana liczba (drzew i tablic) jest liczbą Catalana, jest nietrudnym ćwiczeniem.

17. Zadanie olimpijskie

Na zawodach II stopnia XLIII Olimpiady Matematycznej zawodnicy mieli do rozwiązania następujące zadanie:

- Ciągi (x_n) i (y_n) są określone następująco: $x_0 = y_0 = 1$,

$$x_{n+1} = \frac{x_n + 2}{x_n + 1}, \quad y_{n+1} = \frac{y_n^2 + 2}{2y_n} \quad \text{dla } n = 0, 1, 2, \dots$$

Udowodnij, że dla każdej liczby całkowitej $n \geq 0$ zachodzi równość $y_n = x_{2^n - 1}$.

Jedną z metod rozwiązania tego zadania polega na znalezieniu wzorów ogólnych obu ciągów i porównaniu tych wzorów dla odpowiednich indeksów. Wyznaczenie wzoru ogólnego ciągu (x_n) można sprowadzić do równania rekurencyjnego liniowego. Zdefiniujmy bowiem dwa ciągi (a_n) i (b_n) wzorami: $a_0 = b_0 = 1$,

$$a_{n+1} = a_n + 2b_n, \quad b_{n+1} = a_n + b_n \quad \text{dla } n = 0, 1, 2, \dots$$

Wówczas łatwo dowodzimy przez indukcję, że

$$x_n = \frac{a_n}{b_n} \quad \text{dla } n = 0, 1, 2, \dots$$

Podobnie jak w paragrafie 15 sprowadzamy układ równań rekurencyjnych do równania drugiego rzędu

$$a_{n+2} - 2a_{n+1} - a_n = 0.$$

Równanie charakterystyczne $x^2 - 2x - 1 = 0$ ma dwa pierwiastki

$$x_1 = 1 + \sqrt{2}, \quad x_2 = 1 - \sqrt{2}.$$

Stąd łatwo otrzymujemy rozwiązanie ogólne

$$a_n = \frac{(1 + \sqrt{2})^{n+1} + (1 - \sqrt{2})^{n+1}}{2}$$

oraz

$$b_n = \frac{(1 + \sqrt{2})^{n+1} - (1 - \sqrt{2})^{n+1}}{2\sqrt{2}}$$

i ostatecznie otrzymujemy

$$x_n = \frac{a_n}{b_n} = \sqrt{2} \cdot \frac{(1 + \sqrt{2})^{n+1} + (1 - \sqrt{2})^{n+1}}{(1 + \sqrt{2})^{n+1} - (1 - \sqrt{2})^{n+1}}.$$

Uzyskanie wzoru ogólnego dla ciągu (y_n) jest bardziej skomplikowane. Ciąg ten jest bowiem zdefiniowany za pomocą równania nieliniowego i nie widać żadnej ogólnej metody rozwiązywania takich równań rekurencyjnych. Posłużymy się następującym pomysłem. Najpierw obliczamy

$$y_{n+1} - \sqrt{2} = \frac{y_n^2 + 2}{2y_n} - \sqrt{2} = \frac{y_n^2 - 2\sqrt{2}y_n + 2}{2y_n} = \frac{(y_n - \sqrt{2})^2}{2y_n}$$

i podobnie

$$y_{n+1} + \sqrt{2} = \frac{(y_n + \sqrt{2})^2}{2y_n}.$$

Stąd wynika, że

$$\frac{y_{n+1} - \sqrt{2}}{y_{n+1} + \sqrt{2}} = \frac{(y_n - \sqrt{2})^2}{(y_n + \sqrt{2})^2} = \left(\frac{y_n - \sqrt{2}}{y_n + \sqrt{2}} \right)^2.$$

Zdefiniujmy ciąg (c_n) wzorem

$$c_n = \frac{y_n - \sqrt{2}}{y_n + \sqrt{2}}.$$

Wówczas

$$c_{n+1} = c_n^2,$$

skąd wynika, że

$$c_n = c_0^{2^n} = \left(\frac{1 - \sqrt{2}}{1 + \sqrt{2}} \right)^{2^n}.$$

Teraz już łatwo dostajemy

$$y_n = \sqrt{2} \cdot \frac{1 + c_n}{1 - c_n} = \sqrt{2} \cdot \frac{(1 + \sqrt{2})^{2^n} + (1 - \sqrt{2})^{2^n}}{(1 + \sqrt{2})^{2^n} - (1 - \sqrt{2})^{2^n}}.$$

Porównując otrzymane wzory ogólne dostajemy $y_n = x^{2^n - 1}$.

Zadanie można też łatwo rozwiązać bezpośrednio przez indukcję. Najpierw dowodzimy przez indukcję równość pomocniczą:

$$x_{2n+1} = \frac{x_n^2 + 2}{2x_n}$$

dla $n = 0, 1, 2, \dots$. Sprawdzenie warunku początkowego (dla $n = 0$) jest oczywiste. Przyjmijmy więc, że dla pewnego n mamy równość

$$x_{2n+1} = \frac{x_n^2 + 2}{2x_n}$$

i dowodzimy, że

$$x_{2n+3} = \frac{x_{n+1}^2 + 2}{2x_{n+1}}.$$

Przekształcamy najpierw lewą stronę:

$$\begin{aligned} x_{2n+3} &= \frac{x_{2n+2} + 2}{x_{2n+2} + 1} = \frac{\frac{x_{2n+1}+2}{x_{2n+1}+1} + 2}{\frac{x_{2n+1}+2}{x_{2n+1}+1} + 1} = \frac{(x_{2n+1} + 2) + 2(x_{2n+1} + 1)}{(x_{2n+1} + 2) + (x_{2n+1} + 1)} = \\ &= \frac{3x_{2n+1} + 4}{2x_{2n+1} + 3} = \frac{3 \cdot \frac{x_m^2+2}{2x_m} + 4}{2 \cdot \frac{x_m^2+2}{2x_m} + 3} = \frac{3(x_m^2 + 2) + 8x_m}{2(x_m^2 + 2) + 6x_m} = \\ &= \frac{3x_m^2 + 8x_m + 6}{2x_m^2 + 6x_m + 4}. \end{aligned}$$

Następnie przekształcamy prawą stronę:

$$\begin{aligned} \frac{x_{m+1}^2 + 2}{2x_{m+1}} &= \frac{\left(\frac{x_m+2}{x_m+1}\right)^2 + 2}{2 \cdot \frac{x_m+2}{x_m+1}} = \frac{(x_m + 2)^2 + 2(x_m + 1)^2}{2(x_m + 2)(x_m + 1)} = \\ &= \frac{x_m^2 + 4x_m + 4 + 2x_m^2 + 4x_m + 2}{2(x_m^2 + 3x_m + 2)} = \frac{3x_m^2 + 8x_m + 6}{2x_m^2 + 6x_m + 4}. \end{aligned}$$

W ten sposób nasza równość pomocnicza została udowodniona. Teraz dowodzimy przez indukcję, że $y_n = x_{2^n-1}$. Znów sprawdzenie warunku początkowego (dla $n = 0$) jest oczywiste. W kroku indukcyjnym mamy:

$$y_{n+1} = \frac{y_n^2 + 2}{2y_n} = \frac{(x_{2^n-1})^2 + 2}{2x_{2^n-1}} = x_{2(2^n-1)+1} = x_{2^{n+1}-1},$$

co kończy dowód.

18. Zadanie z zawodów matematycznych

Na XXI Austriacko-Polskich Zawodach Matematycznych zawodnicy rozwiązywali następujące zadanie:

- Rozważamy n punktów $P_1, P_2, \dots, P_n$ położonych w tej kolejności na jednej linii prostej. Malujemy każdy z tych punktów na jeden z następujących kolorów: biały, czerwony, zielony, niebieski, fioletowy. Kolorowanie nazwiemy *dopuszczalnym*, jeśli dla dowolnych dwóch kolejnych punktów P_i, P_{i+1} ($i = 1, 2, \dots, n-1$) oba są tego samego koloru lub co najmniej jeden z nich jest biały. Ile jest dopuszczalnych kolorowań?

Najpierw ustalmy terminologię. Powiemy, że punkt jest *kolorowy*, jeśli został pomalowany na kolor różny od białego; w przeciwnym razie nazywamy ten punkt *białym*. Definiujemy dwa ciągi (b_n) i (k_n) w następujący sposób: b_n jest liczbą dopuszczalnych kolorowań n punktów takich, że punkt P_n jest biały, k_n zaś jest liczbą dopuszczalnych kolorowań takich, że punkt P_n jest kolorowy. Wówczas oczywiście

$$b_1 = 1, \quad k_1 = 4.$$

Następnie $b_{n+1} = b_n + k_n$, bo jeśli punkt P_{n+1} jest biały, to kolorowanie poprzednich n punktów jest dowolnym dopuszczalnym kolorowaniem zakończonym punktem białym lub dowolnym kolorowym. Natomiast $k_{n+1} = 4b_n + k_n$, bo jeśli punkt P_{n+1} jest kolorowy, to kolorowanie poprzednich n punktów jest kolorowaniem dopuszczalnym zakończonym punktem białym (i wtedy mamy 4 możliwości wyboru koloru dla P_{n+1}) lub kolorowym tego samego koloru co P_{n+1} .

Układ równań rekurencyjnych

$$b_1 = 1, \quad k_1 = 4, \quad b_{n+1} = b_n + k_n, \quad k_{n+1} = 4b_n + k_n$$

rozwiązujemy tak jak w paragrafie 15, otrzymując ostatecznie liczbę kolorowań dopuszczalnych równą

$$b_n + k_n = b_{n+1} = \frac{3^{n+1} + (-1)^{n+1}}{2}.$$

To zadanie można rozwiązać bez układania równań rekurencyjnych. Nazwijmy *blokiem* ciąg punktów tego samego koloru. Kolorowanie dopuszczalne dzieli punkty $P_1, \dots, P_n$ na k bloków (gdzie $k = 1, 2, \dots, n$), wśród których co drugi jest biały, pozostałe zaś kolorowe. Chcemy policzyć wszystkie sposoby takiego podziału na bloki. Zauważmy najpierw, że istnieje $\binom{n-1}{k-1}$ sposobów podziału n punktów na k bloków, bez uwzględniania kolorów. Musimy bowiem w wolne miejsca między punktami wstawić $k - 1$ kresek oddzielających bloki od siebie. Teraz będziemy rozpatrywać dwa przypadki:

1. Przypuśćmy najpierw, że liczba n jest parzysta: $n = 2m$. Ten przypadek dzielimy na dwa podprzypadki:
 - 1a. Liczba bloków jest parzysta ($k = 2l$, gdzie $l = 1, 2, \dots, m$). Mamy wtedy l bloków białych i l bloków kolorowych. Możemy dla nich wybrać kolory na 4^l sposobów. Uwzględniając to, czy pierwszy blok jest biały, czy kolorowy, mamy w tym przypadku $2 \cdot 4^l$ sposobów wyboru kolorów bloków kolorowych.
 - 1b. Liczba bloków jest nieparzysta ($k = 2l - 1$, gdzie $l = 1, 2, \dots, m$). Jeśli pierwszy blok jest biały, to mamy 4^{l-1} możliwości wyboru kolorów dla bloków kolorowych; jeśli zaś pierwszy blok jest kolorowy, to mamy 4^l możliwości wyboru kolorów. Łącznie mamy w tym przypadku $\frac{5}{4} \cdot 4^l$ możliwości wyboru kolorów.

Łącznie liczba kolorowań dopuszczalnych wynosi w tym przypadku

$$\sum_{l=1}^m \binom{2m-1}{2l-1} \cdot 2 \cdot 4^l + \sum_{l=1}^m \binom{2m-1}{2l-2} \cdot \frac{5}{4} \cdot 4^l.$$

Zauważmy teraz, że

$$2 \cdot 4^l = \frac{9-1}{4} \cdot 2^{2l} = \frac{9+(-1)^{2l-1}}{2} \cdot 2^{2l-1}$$

oraz

$$\frac{5}{4} \cdot 4^l = \frac{9+1}{8} \cdot 2^{2l} = \frac{9+(-1)^{2l-2}}{2} \cdot 2^{2l-2}.$$

Stąd wynika, że w przypadku 1 mamy następującą liczbę kolorowań dopuszczalnych:

$$\begin{aligned}
 & \sum_{l=1}^m \binom{2m-1}{2l-1} \cdot 2 \cdot 4^l + \sum_{l=1}^m \binom{2m-1}{2l-2} \cdot \frac{5}{4} \cdot 4^l = \\
 &= \sum_{l=1}^m \binom{2m-1}{2l-1} \cdot \frac{9 + (-1)^{2l-1}}{2} \cdot 2^{2l-1} + \sum_{l=1}^m \binom{2m-1}{2l-2} \cdot \frac{9 + (-1)^{2l-2}}{2} \cdot 2^{2l-2} = \\
 &= \sum_{l=0}^{2m-1} \binom{2m-1}{l} \cdot \frac{9 + (-1)^l}{2} \cdot 2^l = \\
 &= \frac{9}{2} \cdot \sum_{l=0}^{2m-1} \binom{2m-1}{l} 2^l + \frac{1}{2} \cdot \sum_{l=0}^{2m-1} \binom{2m-1}{l} (-2)^l = \\
 &= \frac{9}{2} \cdot (1+2)^{2m-1} + \frac{1}{2} \cdot (1-2)^{2m-1} = \frac{9 \cdot 3^{2m-1} - 1}{2} = \frac{3^{n+1} - 1}{2}.
 \end{aligned}$$

2. Przypuśćmy następnie, że liczba n jest nieparzysta: $n = 2m + 1$. Ten przypadek znów dzielimy na dwa podprzypadki:

- 2a. Liczba bloków jest parzysta ($k = 2l$, gdzie $l = 1, 2, \dots, m$). Mamy wtedy l bloków białych i l bloków kolorowych. Możemy dla nich wybrać kolory na 4^l sposobów. Uwzględniając to, czy pierwszy blok jest biały, czy kolorowy, mamy w tym przypadku $2 \cdot 4^l$ sposobów wyboru kolorów bloków kolorowych.
- 2b. Liczba bloków jest nieparzysta ($k = 2l - 1$, gdzie $l = 1, 2, \dots, m + 1$). Jeśli pierwszy blok jest biały, to mamy 4^{l-1} możliwości wyboru kolorów dla bloków kolorowych; jeśli zaś pierwszy blok jest kolorowy, to mamy 4^l możliwości wyboru kolorów. Łącznie mamy w tym przypadku $\frac{5}{4} \cdot 4^l$ możliwości wyboru kolorów.

Łącznie liczba kolorowań dopuszczalnych wynosi w tym przypadku

$$\sum_{l=1}^m \binom{2m}{2l-1} \cdot 2 \cdot 4^l + \sum_{l=1}^{m+1} \binom{2m}{2l-2} \cdot \frac{5}{4} \cdot 4^l.$$

Podobnie jak w przypadku 1 pokazujemy, że ta liczba jest równa

$$\frac{3^{n+1} + 1}{2}.$$

W obu przypadkach mamy zatem $\frac{1}{2} \cdot (3^{n+1} + (-1)^{n+1})$ kolorowań dopuszczalnych.

FUNKCJE TWORZĄCE

1. Określenie funkcji tworzących za pomocą szeregów potęgowych

Przypuśćmy, że dany jest ciąg (a_n) liczb zespolonych. **Funkcją tworzącą** dla ciągu (a_n) nazywamy funkcję $A(z)$ określoną za pomocą wzoru

$$A(z) = \sum_{n=0}^{\infty} a_n z^n.$$

Przyjmujemy przy tym, że szereg potęgowy po prawej stronie powyższej równości ma dodatni promień zbieżności r i wtedy funkcja $A(z)$ jest określona wewnątrz koła o środku w zerze i promieniu r . Nie będziemy teraz zajmować się ciągami, dla których rozważany szereg potęgowy ma zerowy promień zbieżności (np. ciągami takimi jak $a_n = n^n$). Z teorii funkcji analitycznych wiadomo, że dla danej funkcji analitycznej $A(z)$ współczynniki definiującego ją szeregu potęgowego są wyznaczone jednoznacznie.

Wykorzystanie funkcji tworzących do znajdowania wzorów ogólnych polega na wykonaniu następujących kroków:

- zdefiniowanie funkcji tworzącej dla danego ciągu określonego rekurencyjnie,
- wykorzystanie równań rekurencyjnych do utworzenia równania na funkcję tworzącą,
- rozwiązanie równania i znalezienie wzoru funkcji tworzącej,
- rozwinięcie znalezionej funkcji tworzącej w szereg potęgowy i porównanie współczynników.

Prześledzimy teraz tę metodę na dwóch przykładach: liczb Fibonacciego i liczb Catalana.

2. Liczby Fibonacciego

Przypomnijmy definicję liczb Fibonacciego:

$$F_0 = F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad \text{dla } n \geq 2.$$

Pokażemy teraz, w jaki sposób można otrzymać wzór ogólny na liczby Fibonacciego, korzystając z tzw. funkcji tworzących.

Definiujemy funkcję tworzącą dla ciągu liczb Fibonacciego wzorem

$$F(x) = \sum_{n=0}^{\infty} F_n z^n.$$

Mamy teraz

$$\begin{aligned} F(x) &= \sum_{n=0}^{\infty} F_n z^n = F_0 + F_1 z + \sum_{n=2}^{\infty} F_n z^n = 1 + z + \sum_{n=0}^{\infty} (F_{n-1} + F_{n-2}) z^n = \\ &= 1 + z + \sum_{n=2}^{\infty} F_{n-1} z^n + \sum_{n=2}^{\infty} F_{n-2} z^n = 1 + z + \sum_{n=1}^{\infty} F_n z^{n+1} + \sum_{n=0}^{\infty} F_n z^{n+2} = \\ &= 1 + z + z \cdot \sum_{n=1}^{\infty} F_n z^n + z^2 \cdot \sum_{n=0}^{\infty} F_n z^n = 1 + z + z \cdot (F(z) - 1) + z^2 \cdot F(z) = \\ &= 1 + z + zF(z) - z + z^2 F(z) = 1 + zF(z) + z^2 F(z). \end{aligned}$$

Otrzymaliśmy równanie

$$F(z) = 1 + zF(z) + z^2F(z),$$

z którego dostajemy wzór na $F(z)$:

$$F(z) \cdot (1 - z - z^2) = 1,$$

czyli

$$F(z) = \frac{1}{1 - z - z^2}.$$

Teraz otrzymaną funkcję tworzącą rozwijamy w szereg potęgowy. W tym celu rozkładamy ułamek

$$\frac{1}{1 - z - z^2}$$

na ułamki proste. Najpierw znajdujemy liczby zespolone α i β takie, że

$$1 - z - z^2 = (1 - \alpha z)(1 - \beta z) = 1 - (\alpha + \beta)z + (\alpha\beta)z^2.$$

W tym celu rozwiązujemy układ równań

$$\begin{cases} \alpha + \beta = 1 \\ \alpha\beta = -1 \end{cases}$$

Otrzymujemy

$$\alpha = \frac{1 + \sqrt{5}}{2} \quad \text{oraz} \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

Następnie szukamy liczb zespolonych c i d takich, że

$$\frac{1}{1 - z - z^2} = \frac{c}{1 - \alpha z} + \frac{d}{1 - \beta z}.$$

Po wymnożeniu otrzymujemy

$$\frac{1}{1 - z - z^2} = \frac{c(1 - \beta z) + d(1 - \alpha z)}{(1 - \alpha z)(1 - \beta z)} = \frac{c + d - (\alpha d + \beta c)z}{1 - z - z^2}.$$

Otrzymujemy następny układ równań:

$$\begin{cases} c + d = 1 \\ \beta c + \alpha d = 0 \end{cases}$$

Rozwiązując ten układ równań, otrzymujemy:

$$c = \frac{\alpha}{\sqrt{5}} \quad \text{oraz} \quad d = -\frac{\beta}{\sqrt{5}}.$$

Mamy zatem

$$F(z) = \frac{\alpha}{\sqrt{5}} \cdot \frac{1}{1 - \alpha z} - \frac{\beta}{\sqrt{5}} \cdot \frac{1}{1 - \beta z}.$$

Korzystamy teraz ze znanego rozwinięcia w szereg potęgowy. Mianowicie dla dowolnej liczby zespolonej γ mamy

$$\frac{1}{1 - \gamma z} = \sum_{n=0}^{\infty} \gamma^n z^n.$$

Stąd dostajemy rozwinięcie funkcji $F(z)$ w szereg potęgowy

$$F(z) = \frac{\alpha}{\sqrt{5}} \cdot \sum_{n=0}^{\infty} \alpha^n z^n - \frac{\beta}{\sqrt{5}} \cdot \sum_{n=0}^{\infty} \beta^n z^n = \sum_{n=0}^{\infty} \frac{\alpha^{n+1} - \beta^{n+1}}{\sqrt{5}} \cdot z^n.$$

Korzystając z jednoznaczności rozwinięcia funkcji analitycznej w szereg potęgowy, dostajemy

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

Otrzymany wzór jest nazywany **wzorem Bineta**.

3. Liczby Catalana

Przypomnijmy, że liczby Catalana C_n spełniają następujące równanie rekurencyjne:

$$C_0 = 1, \quad C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k} = C_0 C_{n-1} + C_1 C_{n-2} + \dots + C_{n-1} C_0 \quad \text{dla } n \geq 1.$$

W szczególności dla początkowych wartości n mamy:

$$\begin{aligned} C_0 &= 1, \\ C_1 &= C_0^2 = 1, \\ C_2 &= C_0 C_1 + C_1 C_0 = 2, \\ C_3 &= C_0 C_2 + C_1 C_1 + C_2 C_0 = 5, \\ C_4 &= C_0 C_3 + C_1 C_2 + C_2 C_1 + C_3 C_0 = 14. \end{aligned}$$

Definiujemy funkcję tworzącą $C(z)$ dla liczb Catalana wzorem

$$C(z) = \sum_{n=0}^{\infty} C_n z^n.$$

Mamy teraz

$$\begin{aligned} (C(z))^2 &= C_0^2 + (C_0 C_1 + C_1 C_0)z + (C_0 C_2 + C_1 C_1 + C_2 C_0)z^2 + \dots = \\ &= C_1 + C_2 z + C_3 z^2 + \dots \end{aligned}$$

Dokładniej:

$$(C(z))^2 = \sum_{n=0}^{\infty} \sum_{k=0}^n C_k C_{n-k} z^n = \sum_{n=0}^{\infty} C_{n+1} z^n.$$

Zatem

$$z \cdot (C(z))^2 = \sum_{n=0}^{\infty} C_{n+1} z^{n+1} = \sum_{n=1}^{\infty} C_n z^n = C(z) - C_0 = C(z) - 1.$$

Otrzymaliśmy więc równanie kwadratowe z niewiadomą $C(z)$:

$$z \cdot (C(z))^2 - C(z) + 1 = 0.$$

Rozwiązując to równanie otrzymujemy

$$C(z) = \frac{1 \pm \sqrt{1-4z}}{2z}.$$

Musimy wiedzieć, jaki znak należy wziąć w liczniku. Wiemy jednak, że $C(0) = C_0 = 1$. Mamy natomiast

$$\lim_{x \rightarrow 0+} \frac{1 + \sqrt{1-4x}}{2x} = +\infty$$

oraz

$$\lim_{x \rightarrow 0} \frac{1 + \sqrt{1-4x}}{2x} = \lim_{x \rightarrow 0} \frac{4x}{2x(1 + \sqrt{1-4x})} = 1.$$

Stąd wynika, że należy wziąć znak minus:

$$C(z) = \frac{1 - \sqrt{1-4z}}{2z}.$$

Teraz musimy rozwinąć funkcję $C(z)$ w szereg potęgowy. Skorzystamy ze wzoru Newtona. W tym celu dla dowolnej liczby rzeczywistej α i dowolnej liczby naturalnej $n \geq 1$ definiujemy

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)(\alpha-2) \cdots (\alpha-n+1)}{n!}.$$

Przyjmujemy ponadto

$$\binom{\alpha}{0} = 1.$$

Wówczas mamy następujący wzór Newtona

$$(1+z)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} z^n,$$

przy czym szereg potęgowy po prawej stronie ma dodatni promień zbieżności (równy 1). Ze wzoru Newtona wynika, że

$$\sqrt{1-4z} = \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} (-4z)^n = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} 4^n z^n,$$

skąd dostajemy

$$1 - \sqrt{1-4z} = - \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} 4^n z^n.$$

Ostatecznie

$$C(z) = -\frac{1}{2} \cdot \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{2}}{n} 4^n z^{n-1} = \frac{1}{2} \cdot \sum_{n=0}^{\infty} (-1)^n \binom{\frac{1}{2}}{n+1} 4^{n+1} z^n.$$

Obliczmy teraz występujące w powyższym wzorze współczynniki dwumianowe:

$$\begin{aligned} \binom{\frac{1}{2}}{n} &= \frac{(1/2) \cdot (1/2 - 1) \cdot (1/2 - 2) \cdot \dots \cdot (1/2 - n + 1)}{n!} = \\ &= \frac{1 \cdot (1 - 2) \cdot (1 - 4) \cdot \dots \cdot (1 - 2n + 2)}{2^n \cdot n!} = \\ &= \frac{(-1)^{n-1} \cdot (2 - 1) \cdot (4 - 1) \cdot \dots \cdot (2n - 3)}{2^n \cdot n!} = \\ &= \frac{(-1)^{n-1} \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n - 3)}{2^n \cdot n!} = \\ &= \frac{(-1)^{n-1} \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n - 3) \cdot 2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n - 2)}{2^n \cdot n! \cdot 2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n - 2)} = \\ &= \frac{(-1)^{n-1} \cdot (2n - 2)!}{2^n \cdot n! \cdot 2^{n-1} \cdot (n - 1)!} = \\ &= \frac{(-1)^{n-1} \cdot (2n - 2)!}{2^{2n-1} \cdot n! \cdot (n - 1)!}. \end{aligned}$$

Stąd

$$\binom{\frac{1}{2}}{n+1} = \frac{(-1)^n \cdot (2n)!}{2^{2n+1} \cdot (n+1)! \cdot n!} = \frac{(-1)^n}{2 \cdot (n+1) \cdot 4^n} \cdot \binom{2n}{n}.$$

Podstawiamy obliczoną wartość współczynnika dwumianowego do wzoru na $C(z)$:

$$C(z) = \frac{1}{2} \cdot \sum_{n=0}^{\infty} (-1)^n \cdot \frac{(-1)^n}{2 \cdot (n+1) \cdot 4^n} \cdot \binom{2n}{n} \cdot 4^{n+1} \cdot z^n = \sum_{n=0}^{\infty} \frac{1}{n+1} \cdot \binom{2n}{n} z^n.$$

Stąd ostatecznie dostajemy

$$C_n = \frac{1}{n+1} \cdot \binom{2n}{n}.$$

4. Wykładnicze funkcje tworzące i liczby Bella

Niech (a_n) będzie nieskończonym ciągiem liczb zespolonych. **Wykładniczą funkcją tworzącą** dla ciągu (a_n) nazywamy funkcję $A(z)$ określoną za pomocą wzoru

$$A(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n.$$

W tym paragrafie wyprowadzimy wzór na wykładniczą funkcję tworzącą dla liczb Bella. Przypomnijmy teraz wzór rekurencyjny dla liczb Bella:

$$B_0 = 1, \quad B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k \quad \text{dla } n \geq 0.$$

Niech $B(z)$ będzie wykładniczą funkcją tworzącą dla liczb Bella:

$$B(z) = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n.$$

Mamy wówczas

$$B(z) = 1 + \sum_{n=1}^{\infty} \frac{B_n}{n!} z^n = 1 + \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} z^{n+1}.$$

Różniczkujemy otrzymany szereg wyraz po wyrazie:

$$\begin{aligned} B'(z) &= \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} \cdot (n+1) z^n = \sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} z^n = \sum_{n=0}^{\infty} \sum_{k=0}^n \binom{n}{k} \cdot B_k \cdot \frac{z^n}{n!} = \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{B_k}{k! \cdot (n-k)!} z^n = \sum_{n=0}^{\infty} \sum_{k=0}^n \left(\frac{B_k}{k!} z^k \cdot \frac{z^{n-k}}{(n-k)!} \right) = \\ &= \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \right) \cdot \left(\sum_{n=0}^{\infty} \frac{z^n}{n!} \right) = B(z) \cdot e^z. \end{aligned}$$

Otrzymaliśmy równanie

$$B'(z) = B(z) \cdot e^z,$$

czyli

$$(\ln B(z))' = e^z.$$

Stąd

$$B(z) = e^{e^z + C}$$

dla pewnej stałej C . Porównując wartości dla $z = 0$, otrzymujemy $C = -1$. Ostatecznie

$$B(z) = e^{e^z - 1}.$$

5. Pierścień szeregów formalnych

Będziemy zajmować się zbiorem wszystkich nieskończonych ciągów o wyrazach zespolonych $\mathbb{P} = \mathbb{C}^{\mathbb{N}}$. Elementy zbioru $\mathbb{P}$ będziemy oznaczać małymi literami greckimi i nazywać **formalnymi szeregami potęgowymi** lub w skrócie **szeregami formalnymi**. Naszym zamysłem jest, by szereg α odpowiadał prawdziwemu szeregowi potęgowemu:

$$\alpha = (a_0, a_1, a_2, \dots, a_n \dots) \quad \text{odpowiada szeregowi} \quad \sum_{n=0}^{\infty} a_n x^n.$$

Pojęcie szeregu **formalnego** związane jest z tym, że nie zwracamy uwagi na zbieżność szeregu. Wszelkie działania na szeregach będziemy traktować czysto formalnie, nie zastanawiając się nad tym, czy rozważane sumy odpowiadają jakimkolwiek liczbom zespolonym. Okaze się, że takie działania będą miały dobrze określony sens algebraiczny oraz szereg formalny α rzeczywiście okaże się nieskończoną sumą elementów postaci $a_n x^n$.

Zdefiniujemy trzy ważne podzbiory $\mathbb{P}$. Niech

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \in \mathbb{P}.$$

Wówczas:

$$\alpha \in \mathbb{P}_{\mathbb{R}} \Leftrightarrow \forall n \in \mathbb{N} (a_n \in \mathbb{R}),$$

$$\alpha \in \mathbb{P}_0 \Leftrightarrow a_0 = 0,$$

$$\alpha \in \mathbb{P}_1 \Leftrightarrow a_0 = 1.$$

Zbiór $\mathbb{P}$ jest więc zbiorem wszystkich szeregów formalnych o wyrazach zespolonych, $\mathbb{P}_{\mathbb{R}}$ jest jego podzbiorem składającym się z szeregów formalnych o wyrazach rzeczywistych, $\mathbb{P}_0$ i $\mathbb{P}_1$ podzbiórami składającymi się z szeregów formalnych, których wyraz wolny jest odpowiednio równy 0 lub 1.

Wprowadzimy teraz działania na szeregach formalnych w taki sposób, by nadały one zbiorowi $\mathbb{P}$ strukturę pierścienia przemiennego bez dzielników zera (czyli tzw. dziedziny całkowitości). Zaczniemy od dodawania szeregów formalnych. Niech

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \quad \text{oraz} \quad \beta = (b_0, b_1, b_2, \dots, b_n, \dots).$$

Sumą $\alpha + \beta$ szeregów formalnych nazwiemy szereg

$$\alpha + \beta = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots, a_n + b_n, \dots).$$

Inaczej mówiąc, szeregi formalne dodajemy „po współrzędnych”. Nietrudno zauważyć, że działanie dodawania szeregów formalnych jest przemienne i łączne:

$$\alpha + \beta = \beta + \alpha \quad \text{oraz} \quad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$

dla dowolnych $\alpha, \beta, \gamma \in \mathbb{P}$. Przyjmijmy następnie

$$\zeta = (0, 0, 0, \dots, 0, \dots)$$

oraz

$$-\alpha = (-a_0, -a_1, -a_2, \dots, -a_n, \dots).$$

Wówczas łatwo sprawdzić, że

$$\alpha + \zeta = \zeta + \alpha = \alpha \quad \text{oraz} \quad \alpha + (-\alpha) = (-\alpha) + \alpha = \zeta.$$

Szereg ζ jest więc zerem, a szereg $-\alpha$ jest szeregiem przeciwnym do szeregu α . Zbiór $\mathbb{P}$ jest zatem grupą abelową ze względu na działanie dodawania. Zdefiniujemy teraz mnożenie szeregów formalnych. Tak jak poprzednio, niech

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \quad \text{oraz} \quad \beta = (b_0, b_1, b_2, \dots, b_n, \dots).$$

Iloczynem $\alpha \cdot \beta$ szeregów formalnych nazwiemy szereg

$$\gamma = (c_0, c_1, c_2, \dots, c_n, \dots)$$

określony wzorami

$$c_0 = a_0 b_0, \quad c_1 = a_0 b_1 + a_1 b_0, \quad c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \dots,$$

czyli ogólnie za pomocą tzw. wzoru Cauchy'ego

$$c_n = \sum_{k=0}^n a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1 + a_n b_0$$

dla $n = 0, 1, 2, \dots$. Wykażemy, że zbiór $\mathbb{P}$ z działaniami dodawania i mnożenia jest pierścieniem przemiennym. Przemienność mnożenia jest oczywista i wynika z przemienności mnożeń we wzorze Cauchy'ego. Pokażemy teraz, że mnożenie szeregów formalnych jest łączne.

Niech dane będą trzy szeregi formalne α , β i γ :

$$\begin{aligned} \alpha &= (a_0, a_1, a_2, \dots, a_n, \dots), \\ \beta &= (b_0, b_1, b_2, \dots, b_n, \dots), \\ \gamma &= (c_0, c_1, c_2, \dots, c_n, \dots). \end{aligned}$$

Chcemy udowodnić, że

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

W tym celu definiujemy następujące szeregi formalne:

$$\begin{aligned} \delta &= \alpha \cdot \beta = (d_0, d_1, d_2, \dots, d_n, \dots), \\ \varepsilon &= \delta \cdot \gamma = (e_0, e_1, e_2, \dots, e_n, \dots), \\ \varphi &= \beta \cdot \gamma = (f_0, f_1, f_2, \dots, f_n, \dots), \\ \eta &= \alpha \cdot \varphi = (h_0, h_1, h_2, \dots, h_n, \dots), \end{aligned}$$

gdzie zgodnie ze wzorem Cauchy'ego mamy

$$d_n = \sum_{k=0}^n a_k b_{n-k}, \quad e_n = \sum_{k=0}^n d_k c_{n-k}, \quad f_n = \sum_{k=0}^n b_k c_{n-k}, \quad h_n = \sum_{k=0}^n a_k f_{n-k}$$

dla $n = 0, 1, 2, \dots$. Naszym celem jest udowodnienie, że $\varepsilon = \eta$, czyli, że $e_n = h_n$ dla $n = 0, 1, 2, \dots$. W tym celu skorzystamy z równości pomocniczej:

$$\sum_{k=0}^n \sum_{l=0}^k p_{k,l} = \sum_{l=0}^n \sum_{k=l}^n p_{k,l} = \sum_{l=0}^n \sum_{k=0}^{n-l} p_{k+l,l} = \sum_{k=0}^n \sum_{l=0}^{n-k} p_{k+l,k}.$$

Dowód tej tożsamości pozostawimy jako ćwiczenie. Mamy teraz:

$$e_n = \sum_{k=0}^n d_k c_{n-k} = \sum_{k=0}^n \left(\sum_{l=0}^k a_l b_{k-l} \right) \cdot c_{n-k} = \sum_{k=0}^n \sum_{l=0}^k a_l b_{k-l} c_{n-k} = \sum_{k=0}^n \sum_{l=0}^{n-k} a_k b_l c_{n-k-l}$$

dla $n = 0, 1, 2, \dots$. Z drugiej strony mamy

$$h_n = \sum_{k=0}^n a_k f_{n-k} = \sum_{k=0}^n a_k \cdot \left(\sum_{l=0}^{n-k} b_l c_{n-k-l} \right) = \sum_{k=0}^n \sum_{l=0}^{n-k} a_k b_l c_{n-k-l} = e_n$$

dla $n = 0, 1, 2, \dots$. W ten sposób dowód łączności mnożenia jest zakończony.

Definiujemy teraz szereg formalny ι wzorem

$$\iota = (i_0, i_1, i_2, \dots, i_n, \dots) = (1, 0, 0, \dots, 0, \dots),$$

czyli

$$i_0 = 1 \quad \text{oraz} \quad i_n = 0$$

dla $n = 1, 2, 3, \dots$. Nietrudno zauważyć teraz, że

$$\iota \cdot \alpha = \alpha \cdot \iota = \alpha$$

dla dowolnego szeregu formalnego α . Szereg ι jest zatem jedynką w zbiorze $\mathbb{P}$. Dowodzimy teraz rozdzielności mnożenia względem dodawania. Niech

$$\begin{aligned} \alpha &= (a_0, a_1, a_2, \dots, a_n, \dots), \\ \beta &= (b_0, b_1, b_2, \dots, b_n, \dots), \\ \gamma &= (c_0, c_1, c_2, \dots, c_n, \dots). \end{aligned}$$

Wówczas równość

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

wynika z równości

$$\sum_{k=0}^n a_k (b_{n-k} + c_{n-k}) = \sum_{k=0}^n a_k b_{n-k} + \sum_{k=0}^n a_k c_{n-k}$$

dla $n = 0, 1, 2, \dots$

Zbiór $\mathbb{P}$ jest zatem pierścieniem przemiennym z jedyneką. Pozostaje wykazać, że jest dziedziną całkowitości. Niech więc $\alpha \neq \zeta$ oraz $\beta \neq \zeta$, gdzie

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \quad \text{oraz} \quad \beta = (b_0, b_1, b_2, \dots, b_n, \dots).$$

Chcemy pokazać, że $\alpha \cdot \beta \neq \zeta$. Niech $\gamma = \alpha \cdot \beta$, gdzie

$$\gamma = (c_0, c_1, c_2, \dots, c_n, \dots).$$

Ponieważ $\alpha \neq \zeta$, więc istnieje liczba n taka, że $a_n \neq 0$. Niech n_0 będzie najmniejszą taką liczbą n :

$$a_{n_0} \neq 0 \quad \text{oraz} \quad a_0 = a_1 = \dots = a_{n_0-1} = 0.$$

Podobnie istnieje liczba m_0 taka, że

$$b_{m_0} \neq 0 \quad \text{oraz} \quad b_0 = b_1 = \dots = b_{m_0-1} = 0.$$

Mamy teraz

$$c_{n_0+m_0} = \sum_{k=0}^{n_0+m_0} a_k b_{n_0+m_0-k} = \sum_{k=0}^{n_0-1} a_k b_{n_0+m_0-k} + a_{n_0} b_{m_0} + \sum_{k=n_0+1}^{n_0+m_0} a_k b_{n_0+m_0-k}.$$

Dla $k = 0, 1, \dots, n_0 - 1$ mamy $a_k = 0$, a więc

$$\sum_{k=0}^{n_0-1} a_k b_{n_0+m_0-k} = 0.$$

Następnie

$$\sum_{k=n_0+1}^{n_0+m_0} a_k b_{n_0+m_0-k} = \sum_{k=1}^{m_0} a_{n_0+k} b_{m_0-k} = \sum_{k=0}^{m_0-1} a_{n_0+m_0-k} b_k.$$

Ponieważ dla $k = 0, 1, \dots, m_0 - 1$ mamy $b_k = 0$, więc

$$\sum_{k=n_0+1}^{n_0+m_0} a_k b_{n_0+m_0-k} = \sum_{k=0}^{m_0-1} a_{n_0+m_0-k} b_k = 0.$$

Zatem

$$c_{n_0+m_0} = a_{n_0} \cdot b_{m_0} \neq 0,$$

co dowodzi, że $\gamma \neq \zeta$. Pierścień $\mathbb{P}$ nie ma zatem dzielników zera, a więc jest dziedziną całkowitości. Zerem tego pierścienia jest szereg formalny ζ , a jedyneką szereg formalny ι . Pokażemy teraz, że ciało liczb zespolonych $\mathbb{C}$ może być traktowane jako podciało pierścienia $\mathbb{P}$.

6. Włożenie $\mathbb{C}$ w $\mathbb{P}$

Definiujemy przekształcenie $h : \mathbb{C} \rightarrow \mathbb{P}$ wzorem

$$h(z) = (z, 0, 0, \dots, 0, \dots).$$

Inaczej mówiąc, $h(z)$ jest szeregiem α_z zdefiniowanym wzorami

$$\alpha_z = (a_0, a_1, a_2, \dots, a_n, \dots),$$

gdzie

$$a_0 = z \quad \text{oraz} \quad a_n = 0$$

dla $n = 1, 2, 3, \dots$. W szczególności $\zeta = h(0)$ oraz $\iota = h(1)$. Przekształcenie h jest oczywiście różnowartościowe. Nietrudno pokazać, że jest ono homomorfizmem $\mathbb{C}$ w $\mathbb{P}$. Utożsamiając liczbę zespoloną z z szeregiem formalnym $h(z)$ możemy przyjąć, że ciało liczb zespolonych jest podciałem pierścienia $\mathbb{P}$. Od tej pory zamiast szeregu formalnego α_z będziemy pisać po prostu z . W szczególności zamiast ζ będziemy pisać 0, a zamiast ι będziemy pisać 1.

Odnotujmy jeszcze jedną własność omawianego włożenia, z której będziemy często korzystać. Niech

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Wówczas dla dowolnej liczby zespolonej z mamy

$$z \cdot \alpha = (za_0, za_1, za_2, \dots, za_n, \dots).$$

Wzór ten wynika natychmiast ze wzoru Cauchy'ego.

7. Rodziny sumowalne

Przypuśćmy, że mamy dany ciąg $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_m, \dots$ szeregów formalnych:

$$\begin{aligned} \alpha_0 &= (a_0^{(0)}, a_1^{(0)}, a_2^{(0)}, \dots, a_n^{(0)}, \dots), \\ \alpha_1 &= (a_0^{(1)}, a_1^{(1)}, a_2^{(1)}, \dots, a_n^{(1)}, \dots), \\ \alpha_2 &= (a_0^{(2)}, a_1^{(2)}, a_2^{(2)}, \dots, a_n^{(2)}, \dots), \\ &\dots \quad \dots \\ \alpha_m &= (a_0^{(m)}, a_1^{(m)}, a_2^{(m)}, \dots, a_n^{(m)}, \dots), \\ &\dots \quad \dots \end{aligned}$$

dla $m = 0, 1, 2, \dots$. Mówimy, że ten ciąg tworzy **rodzinę sumowalną**, jeśli dla każdego n istnieje tylko skończenie wiele liczb m takich, że $a_n^{(m)} \neq 0$. Wówczas dla każdego n definiujemy a_n wzorem

$$a_n = \sum_{m=0}^{\infty} a_n^{(m)}.$$

Suma po prawej stronie ma sens, bo tylko dla skończonego wielu indeksów m sumowany składnik jest różny od zera. Definiujemy teraz

$$\sum_{m=0}^{\infty} \alpha_m = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Inaczej:

$$\sum_{m=0}^{\infty} \alpha_m = \left(\sum_{m=0}^{\infty} a_0^{(m)}, \sum_{m=0}^{\infty} a_1^{(m)}, \sum_{m=0}^{\infty} a_2^{(m)}, \dots, \sum_{m=0}^{\infty} a_n^{(m)}, \dots \right).$$

Zauważmy, że suma rodziny sumowalnej nie zależy od kolejności sumowania. To znaczy, że jeśli mamy dane dwa ciągi szeregów formalnych różniące się tylko kolejnością wyrazów (tzn. jeden jest permutacją drugiego), to sumy obu ciągów będą równe.

8. Szeregi potęgowe

Definiujemy szereg formalny ξ wzorem

$$\xi = (0, 1, 0, 0, 0, \dots, 0, \dots),$$

czyli

$$\xi = (x_0, x_1, x_2, \dots, x_n, \dots),$$

gdzie

$$x_0 = 0, \quad x_1 = 1, \quad x_n = 0 \quad \text{dla } n \geq 2.$$

Nietrudno zauważyć, że

$$\xi^2 = (0, 0, 1, 0, 0, 0, \dots, 0, \dots),$$

$$\xi^3 = (0, 0, 0, 1, 0, 0, \dots, 0, \dots),$$

$$\xi^4 = (0, 0, 0, 0, 1, 0, \dots, 0, \dots)$$

i tak dalej. Ogólnie

$$\xi^m = (x_0, x_1, x_2, \dots, x_n, \dots),$$

gdzie

$$x_n = \begin{cases} 1 & \text{gdy } n = m, \\ 0 & \text{gdy } n \neq m \end{cases}$$

dla $n = 0, 1, 2, \dots$ i $m = 1, 2, 3, \dots$. Przyjmujemy również $\xi^0 = 1$. Przypuśćmy teraz, że dany jest szereg formalny α :

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Przyjmijmy następnie

$$\alpha_0 = a_0 \cdot \xi^0 = (a_0, 0, 0, 0, 0, \dots, 0, \dots),$$

$$\alpha_1 = a_1 \cdot \xi^1 = (0, a_1, 0, 0, 0, \dots, 0, \dots),$$

$$\alpha_2 = a_2 \cdot \xi^2 = (0, 0, a_2, 0, 0, \dots, 0, \dots)$$

i tak dalej. Ogólnie

$$\alpha_m = a_m \cdot \xi^m = (a_0^{(m)}, a_1^{(m)}, a_2^{(m)}, \dots, a_n^{(m)}, \dots),$$

gdzie

$$a_n^{(m)} = \begin{cases} a_n & \text{gdy } n = m, \\ 0 & \text{gdy } n \neq m \end{cases}$$

dla $n, m = 0, 1, 2, \dots$

Nietrudno zauważyć, że rodzina $\alpha_0, \alpha_1, \alpha_2, \dots$ jest sumowalna oraz

$$\alpha = \sum_{m=0}^{\infty} \alpha_m = \sum_{m=0}^{\infty} a_m \cdot \xi^m.$$

Szereg formalny α może więc być traktowany jako suma szeregu potęgowego, w którym współczynnikami przy kolejnych potęgach ξ są wyrazy szeregu formalnego α .

W odróżnieniu od szeregów potęgowych zmiennej zespolonej, nie wolno nam podstawiać w miejsce ξ liczb zespolonych. Otrzymalibyśmy bowiem sumę nieskończenie wielu szeregów formalnych (niekoniecznie sumowalną) lub nieskończenie wielu liczb zespolonych (przy czym szereg nie musiałby być zbieżny). Jedynym wyjątkiem jest podstawienie zera. Formalizuje się to podstawienie za pomocą homomorfizmu $Z : \mathbb{P} \rightarrow \mathbb{C}$ określonego wzorem

$$Z(\alpha) = a_0, \quad \text{gdzie } \alpha = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Sprawdzenie, że przekształcenie Z rzeczywiście jest homomorfizmem, pozostawiamy jako ćwiczenie.

9. Elementy odwracalne pierścienia $\mathbb{P}$

Udowodnimy teraz następujące twierdzenie:

Twierdzenie 5.1. Szereg formalny α jest odwracalny w pierścieniu $\mathbb{P}$ wtedy i tylko wtedy, gdy $a_0 = Z(\alpha) \neq 0$ (czyli wtedy i tylko wtedy, gdy $\alpha \notin \mathbb{P}_0$).

Dowód. Przypuśćmy najpierw, że szereg formalny α jest odwracalny. Niech β będzie takim szeregiem formalnym, że $\alpha \cdot \beta = 1$. Wtedy

$$Z(\alpha) \cdot Z(\beta) = Z(\alpha \cdot \beta) = Z(1) = 1,$$

skąd wynika, że $Z(\alpha) \neq 0$.

Przypuśćmy teraz, że na odwrót, $Z(\alpha) \neq 0$. Niech

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Definiujemy szereg formalny $\beta = (b_0, b_1, b_2, \dots, b_n, \dots)$ w następujący sposób:

$$\begin{aligned} b_0 &= (a_0)^{-1}, \\ b_1 &= (-a_1 b_0) \cdot (a_0)^{-1}, \\ b_2 &= (-a_2 b_0 - a_1 b_1) \cdot (a_0)^{-1}, \\ &\dots \quad \dots \\ b_n &= (-a_n b_0 - a_{n-1} b_1 - \dots - a_1 b_{n-1}) \cdot (a_0)^{-1}, \\ &\dots \quad \dots \end{aligned}$$

Nietrudno teraz zauważyć, że $a_0b_0 = 1$ oraz

$$a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \dots + a_nb_0 = 0,$$

co dowodzi, że $\alpha \cdot \beta = 1$.

Szereg β oznaczamy symbolem α^{-1} i nazywamy **szeregiem odwrotnym** do α . Ponieważ dla dowolnych szeregów formalnych α i β zachodzi równość

$$(\alpha \cdot \beta) \cdot (\alpha^{-1} \cdot \beta^{-1}) = 1,$$

więc mamy równość

$$(\alpha \cdot \beta)^{-1} = \alpha^{-1} \cdot \beta^{-1}.$$

Popatrzmy teraz na przykłady szeregów formalnych odwracalnych. Niech szereg α będzie dany wzorem

$$\alpha = 1 - a\xi = (1, -a, 0, 0, 0, \dots, 0, \dots),$$

gdzie $a \in \mathbb{C}$. Niech następnie

$$\beta = \sum_{n=0}^{\infty} a^n \xi^n = (1, a, a^2, a^3, \dots, a^n, \dots).$$

Ponieważ $Z(\alpha) = Z(\beta) = 1 \neq 0$, więc szeregi α i β są odwracalne. Niech szereg

$$\gamma = (c_0, c_1, c_2, \dots, c_n, \dots)$$

będzie ich iloczynem: $\gamma = \alpha \cdot \beta$. Mamy wówczas

$$c_0 = a_0 \cdot b_0 = 1 \cdot 1 = 1$$

oraz

$$c_n = \sum_{k=0}^n a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} = 1 \cdot a^n + (-a) \cdot a^{n-1} = a^n - a^n = 0$$

dla $n = 1, 2, 3, \dots$. A więc $\alpha \cdot \beta = 1$, czyli

$$(1 - a\xi) \cdot \sum_{n=0}^{\infty} a^n \xi^n = 1.$$

Inaczej mówiąc

$$1 + a\xi + a^2\xi^2 + a^3\xi^3 + \dots + a^n\xi^n + \dots = \sum_{n=0}^{\infty} a^n \xi^n = (1 - a\xi)^{-1}. \quad (5.1)$$

Udowodnimy następnie, że dla dowolnego $d \geq 1$ zachodzi równość

$$(1 - a\xi)^{-d} = \sum_{n=0}^{\infty} \binom{d+n-1}{d-1} a^n \xi^n. \quad (5.2)$$

Tej równości będziemy dowodzić przez indukcję względem d . Dla $d = 1$ mamy pokazać, że

$$(1 - a\xi)^{-1} = \sum_{n=0}^{\infty} \binom{n}{0} a^n \xi^n = \sum_{n=0}^{\infty} a^n \xi^n.$$

To jest dokładnie równość udowodniona wyżej.

W kroku indukcyjnym mamy wykazać, że

$$(1 - a\xi)^{-d-1} = \sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n,$$

czyli

$$(1 - a\xi)^{-d} \cdot (1 - a\xi)^{-1} = \sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n.$$

Z założenia indukcyjnego wiemy, że

$$(1 - a\xi)^{-d} = \sum_{n=0}^{\infty} \binom{d+n-1}{d-1} a^n \xi^n.$$

Musimy zatem udowodnić, że

$$\left(\sum_{n=0}^{\infty} \binom{d+n-1}{d-1} a^n \xi^n \right) \cdot (1 - a\xi)^{-1} = \sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n,$$

czyli

$$\sum_{n=0}^{\infty} \binom{d+n-1}{d-1} a^n \xi^n = \left(\sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n \right) \cdot (1 - a\xi).$$

Przekształcamy prawą stronę:

$$\begin{aligned} \left(\sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n \right) \cdot (1 - a\xi) &= \sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n - \sum_{n=0}^{\infty} \binom{d+n}{d} a^{n+1} \xi^{n+1} = \\ &= \sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n - \sum_{n=1}^{\infty} \binom{d+n-1}{d} a^n \xi^n = \\ &= \sum_{n=0}^{\infty} \binom{d+n}{d} a^n \xi^n - \sum_{n=0}^{\infty} \binom{d+n-1}{d} a^n \xi^n = \\ &= \sum_{n=0}^{\infty} \left(\binom{d+n}{d} - \binom{d+n-1}{d} \right) a^n \xi^n = \\ &= \sum_{n=0}^{\infty} \binom{d+n-1}{d-1} a^n \xi^n, \end{aligned}$$

co kończy dowód indukcyjny.

10. Równania rekurencyjne liniowe jednorodne o stałych współczynnikach – przykład

W tym paragrafie pokażemy na przykładzie, w jaki sposób za pomocą funkcji tworzących możemy otrzymać wzór ogólny ciągu określonego równaniem rekurencyjnym liniowym jednorodnym o stałych współczynnikach. Wybrany przykład będzie pokazywał wszystkie istotne fragmenty dowodu ogólnego, który pokażemy w następnym paragrafie.

Mamy dany ciąg (a_n) zdefiniowany równaniem rekurencyjnym szóstego rzędu:

$$a_{n+6} - 5a_{n+5} - 15a_{n+4} + 85a_{n+3} + 10a_{n+2} - 372a_{n+1} + 360a_n = 0 \quad (5.3)$$

dla $n = 0, 1, 2, \dots$. Poszukujemy rozwiązania ogólnego. Przyjrzyjmy się najpierw równaniu charakterystycznemu naszego równania rekurencyjnego:

$$x^6 - 5x^5 - 15x^4 + 85x^3 + 10x^2 - 372x + 360 = 0$$

lub inaczej

$$(x - 2)^3 \cdot (x + 3)^2 \cdot (x - 5) = 0.$$

Równanie charakterystyczne ma 3 pierwiastki: pierwiastek potrójny $x = 2$, pierwiastek podwójny $x = -3$ i pierwiastek pojedynczy $x = 5$. Pokażemy, że rozwiązanie ogólne równania rekurencyjnego (5.3) ma następującą postać:

$$a_n = (u_0 + u_1n + u_2n^2) \cdot 2^n + (v_0 + v_1n) \cdot (-3)^n + w_0 \cdot 5^n \quad \text{dla } n \geq 0, \quad (5.4)$$

gdzie $u_0, u_1, u_2, v_0, v_1, w_0 \in \mathbb{C}$. Wprowadźmy wygodne oznaczenie: $\mathbb{C}_d[x]$ oznacza zbiór wielomianów zmiennej zespolonej x stopnia mniejszego od d (a więc stopnia co najwyżej $d - 1$). Podobnie $\mathbb{C}_d[\xi]$ oznacza zbiór wielomianów stopnia mniejszego od d zmiennej ξ (jako podzbiór pierścienia wszystkich szeregów formalnych $\mathbb{P}$):

$$\mathbb{C}_d[\xi] = \{\alpha = (a_0, a_1, \dots, a_n, \dots) \in \mathbb{P} : \forall n \geq d (a_n = 0)\}.$$

Wtedy rozwiązanie ogólne równania (5.3) można przedstawić w postaci

$$a_n = u(n) \cdot 2^n + v(n) \cdot (-3)^n + w(n) \cdot 5^n \quad \text{dla } n \geq 0,$$

gdzie $u(x) \in \mathbb{C}_3[x]$, $v(x) \in \mathbb{C}_2[x]$ i $w(x) \in \mathbb{C}_1[x]$. Zwracamy uwagę na związek między krotnościami pierwiastków równania charakterystycznego a stopniami wielomianów $u(x)$, $v(x)$ i $w(x)$.

Będziemy w dalszym ciągu traktować pierścień $\mathbb{P}$ szeregów formalnych jak przestrzeń liniową nad ciałem $\mathbb{C}$. Zdefiniujemy cztery podprzestrzenie przestrzeni $\mathbb{P}$. Oto pierwsza z nich:

$$V_1 = \{\alpha = (a_n) \in \mathbb{P} : a_{n+6} - 5a_{n+5} - 15a_{n+4} + 85a_{n+3} + 10a_{n+2} - 372a_{n+1} + 360a_n = 0\}.$$

W poprzednim wykładzie sprawdziliśmy, że ciągi spełniające równanie rekurencyjne liniowe jednorodne o stałych współczynnikach rzeczywiście tworzą podprzestrzeń liniową przestrzeni wszystkich ciągów o wyrazach zespolonych, a więc przestrzeni $\mathbb{P}$. Ponieważ pierwsze 6 wyrazów ciągu α można dobrać dowolnie, a wszystkie następne są przez nie wyznaczone jednoznacznie, więc

$$V_1 \cong \mathbb{C}^6,$$

czyli

$$\dim V_1 = 6.$$

Przed zdefiniowaniem drugiej podprzestrzeni wybierzmy dwa szeregi formalne:

$$\begin{aligned}\delta &= (1, -5, -15, 85, 10, -372, 360, 0, 0, 0, \dots, 0, \dots) = \\ &= 1 - 5\xi - 15\xi^2 + 85\xi^3 + 10\xi^4 - 372\xi^5 + 360\xi^6 = \\ &= (1 - 2\xi)^3 \cdot (1 + 3\xi)^2 \cdot (1 - 5\xi)\end{aligned}$$

oraz

$$\gamma = \delta^{-1} = (1 - 5\xi - 15\xi^2 + 85\xi^3 + 10\xi^4 - 372\xi^5 + 360\xi^6)^{-1} = (1 - 2\xi)^{-3}(1 + 3\xi)^{-2}(1 - 5\xi)^{-1}.$$

Teraz definiujemy

$$V_2 = \{\alpha \in \mathbb{P} : \exists \pi \in \mathbb{C}_6[\xi] (\alpha = \pi \cdot \gamma)\} = \{\alpha \in \mathbb{P} : \alpha\delta \in \mathbb{C}_6[\xi]\}.$$

Sprawdzenie, że V_2 jest podprzestrzenią $\mathbb{P}$ pozostawimy jako ćwiczenie. Ponieważ elementy V_2 są wyznaczone jednoznacznie przez elementy $\mathbb{C}_6[\xi]$, więc łatwo pokazujemy, że

$$V_2 \cong \mathbb{C}^6,$$

czyli

$$\dim V_2 = 6.$$

Mamy dwie przestrzenie liniowe tego samego wymiaru. Pokażemy, że $V_2 \subseteq V_1$. Przypuśćmy zatem, że mamy dany szereg formalny

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \in V_2.$$

Zatem $\pi = \alpha\delta \in \mathbb{C}_6[\xi]$. Niech zatem

$$\pi = (p_0, p_1, p_2, p_3, p_4, p_5, 0, 0, 0, \dots, 0, \dots),$$

(tzn. $p_n = 0$ dla $n \geq 6$). Mamy zatem równość

$$\begin{aligned}(a_0, a_1, a_2, \dots, a_n, \dots) \cdot (1, -5, -15, 85, 10, -372, 360, 0, 0, 0, \dots, 0, \dots) = \\ = (p_0, p_1, p_2, p_3, p_4, p_5, 0, 0, 0, \dots, 0, \dots).\end{aligned}$$

Stąd wynika, że

$$\begin{aligned} 1 \cdot a_6 - 5 \cdot a_5 - 15 \cdot a_4 + 85 \cdot a_3 + 10 \cdot a_2 - 372 \cdot a_1 + 360 \cdot a_0 &= p_6 = 0, \\ 1 \cdot a_7 - 5 \cdot a_6 - 15 \cdot a_5 + 85 \cdot a_4 + 10 \cdot a_3 - 372 \cdot a_2 + 360 \cdot a_1 &= p_7 = 0 \end{aligned}$$

i ogólnie

$$1 \cdot a_{n+6} - 5 \cdot a_{n+5} - 15 \cdot a_{n+4} + 85 \cdot a_{n+3} + 10 \cdot a_{n+2} - 372 \cdot a_{n+1} + 360 \cdot a_n = p_{n+6} = 0$$

dla $n \geq 0$. A więc $\alpha \in V_1$. Pokazaliśmy zatem, że

$$V_2 \subseteq V_1 \quad \text{oraz} \quad \dim V_1 = \dim V_2,$$

czyli $V_1 = V_2$.

Definiujemy trzecią podprzestrzeń $\mathbb{P}$:

$$V_3 = \{ \alpha \in \mathbb{P} : \exists \pi, \rho, \sigma \left(\alpha = \pi \cdot (1 - 2\xi)^{-3} + \rho \cdot (1 + 3\xi)^{-2} + \sigma \cdot (1 - 5\xi)^{-1} \right) \},$$

przy czym $\pi \in \mathbb{C}_3[\xi]$, $\rho \in \mathbb{C}_2[\xi]$ oraz $\sigma \in \mathbb{C}_1[\xi]$. Nietrudno pokazać, że

$$V_3 \cong \mathbb{C}_3[\xi] \times \mathbb{C}_2[\xi] \times \mathbb{C}_1[\xi] \cong \mathbb{C}^6,$$

a więc V_3 jest też podprzestrzenią przestrzeni $\mathbb{P}$ oraz $\dim V_3 = 6$. Pokażemy, że $V_3 \subseteq V_2$. Przypuśćmy zatem, że

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \in V_3.$$

Zatem

$$\alpha = \pi \cdot (1 - 2\xi)^{-3} + \rho \cdot (1 + 3\xi)^{-2} + \sigma \cdot (1 - 5\xi)^{-1}$$

dla pewnych

$$\pi = (p_0 + p_1\xi + p_2\xi^2) \in \mathbb{C}_3[\xi], \quad \rho = (r_0 + r_1\xi) \in \mathbb{C}_2[\xi], \quad \sigma = s_0 \in \mathbb{C}_1[\xi].$$

Chcemy pokazać, że $\alpha\delta \in \mathbb{C}_6[\xi]$. Mamy

$$\begin{aligned} \alpha \cdot \delta &= (\pi \cdot (1 - 2\xi)^{-3} + \rho \cdot (1 + 3\xi)^{-2} + \sigma \cdot (1 - 5\xi)^{-1}) \cdot (1 - 2\xi)^3(1 + 3\xi)^2(1 - 5\xi) = \\ &= \pi(1 + 3\xi)^2(1 - 5\xi) + \rho(1 - 2\xi)^3(1 - 5\xi) + \sigma(1 - 2\xi)^3(1 + 3\xi)^2 = \\ &= \pi(1 + \xi - 21\xi^2 - 45\xi^3) + \rho(1 - 11\xi + 42\xi^2 - 68\xi^3 + 40\xi^4) + \\ &\quad + \sigma(1 - 15\xi^2 + 10\xi^3 + 60\xi^4 - 72\xi^5) = \\ &= (p_0 + p_1\xi + p_2\xi^2) \cdot (1 + \xi - 21\xi^2 - 45\xi^3) + \\ &\quad + (r_0 + r_1\xi) \cdot (1 - 11\xi + 42\xi^2 - 68\xi^3 + 40\xi^4) + \\ &\quad + s_0 \cdot (1 - 15\xi^2 + 10\xi^3 + 60\xi^4 - 72\xi^5) = \\ &= (p_0 + r_0 + s_0) + (p_0 + p_1 - 11r_0 + r_1)\xi + \\ &\quad + (-21p_0 + p_1 + p_2 + 42r_0 - 11r_1 - 15s_0)\xi^2 + \\ &\quad + (-45p_0 - 21p_1 + p_2 - 68r_0 + 42r_1 + 10s_0)\xi^3 + \\ &\quad + (-45p_1 - 21p_2 + 40r_0 - 68r_1 + 60s_0)\xi^4 + (-45p_2 + 40r_1 - 72s_0)\xi^5 \in \mathbb{C}_6[\xi]. \end{aligned}$$

Zatem $\alpha \in V_2$. Pokazaliśmy więc, że $\alpha \in V_2$ i tym samym pokazaliśmy, że $V_3 \subseteq V_2$. Ponieważ $\dim V_2 = \dim V_3 = 6$, więc $V_2 = V_3$.

Definiujemy czwartą podprzestrzeń liniową przestrzeni $\mathbb{P}$:

$$V_4 = \{ \alpha = (a_n) \in \mathbb{P} : \exists u_0, u_1, u_2, v_0, v_1, w_0 \in \mathbb{C}$$

$$\forall n \in \mathbb{N} (a_n = (u_0 + u_1 n + u_2 n^2) \cdot 2^n + (v_0 + v_1 n) \cdot (-3)^n + w_0 \cdot 5^n) \}.$$

Dowód, że V_4 rzeczywiście jest podprzestrzenią liniową $\mathbb{P}$ zostawiamy jako ćwiczenie. Ponieważ każdy szereg $\alpha \in V_4$ jest wyznaczony jednoznacznie przez liczby zespolone $u_0, u_1, u_2, v_0, v_1, w_0$, więc $V_4 \cong \mathbb{C}^6$, czyli $\dim V_4 = 6$. Pokażemy, że $V_3 \subseteq V_4$. Niech zatem $\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \in V_3$. Istnieją $\pi \in \mathbb{C}_3[\xi]$, $\rho \in \mathbb{C}_2[\xi]$ i $\sigma \in \mathbb{C}_1[\xi]$ takie, że

$$\alpha = \pi \cdot (1 - 2\xi)^{-3} + \rho \cdot (1 + 3\xi)^{-2} + \sigma \cdot (1 - 5\xi)^{-1}.$$

Korzystamy teraz z równości (5.1) i (5.2):

$$\begin{aligned} (1 - 2\xi)^{-3} &= \sum_{n=0}^{\infty} \binom{n+2}{2} \cdot 2^n \xi^n = \frac{1}{2} \cdot \sum_{n=0}^{\infty} (n+1)(n+2) \cdot 2^n \xi^n, \\ (1 + 3\xi)^{-2} &= \sum_{n=0}^{\infty} \binom{n+1}{1} \cdot (-3)^n \xi^n = \sum_{n=0}^{\infty} (n+1) \cdot (-3)^n \xi^n, \\ (1 - 5\xi)^{-1} &= \sum_{n=0}^{\infty} 5^n \xi^n. \end{aligned}$$

Niech następnie $\pi = p_0 + p_1 \xi + p_2 \xi^2$, $\rho = r_0 + r_1 \xi$ oraz $\sigma = s_0$. Wówczas

$$\begin{aligned} \pi \cdot (1 - 2\xi)^{-3} &= \frac{1}{2} \cdot (p_0 + p_1 \xi + p_2 \xi^2) \cdot \sum_{n=0}^{\infty} (n+1)(n+2) \cdot 2^n \xi^n = \\ &= \frac{1}{2} \cdot \sum_{n=0}^{\infty} p_0 (n+1)(n+2) \cdot 2^n \xi^n + \frac{1}{2} \cdot \sum_{n=0}^{\infty} p_1 (n+1)(n+2) \cdot 2^n \xi^{n+1} + \\ &\quad + \frac{1}{2} \cdot \sum_{n=0}^{\infty} p_2 (n+1)(n+2) \cdot 2^n \xi^{n+2} = \\ &= \frac{1}{2} \cdot \sum_{n=0}^{\infty} p_0 (n+1)(n+2) \cdot 2^n \xi^n + \frac{1}{2} \cdot \sum_{n=1}^{\infty} p_1 n(n+1) \cdot 2^{n-1} \xi^n + \\ &\quad + \frac{1}{2} \cdot \sum_{n=2}^{\infty} p_2 n(n-1) \cdot 2^{n-2} \xi^n = \\ &= \frac{1}{2} \cdot \sum_{n=0}^{\infty} p_0 (n+1)(n+2) \cdot 2^n \xi^n + \frac{1}{4} \cdot \sum_{n=0}^{\infty} p_1 n(n+1) \cdot 2^n \xi^n + \\ &\quad + \frac{1}{8} \cdot \sum_{n=0}^{\infty} p_2 n(n-1) \cdot 2^n \xi^n = \\ &= \frac{1}{8} \cdot \sum_{n=0}^{\infty} (4p_0 (n+1)(n+2) + 2p_1 n(n+1) + p_2 n(n-1)) \cdot 2^n \xi^n. \end{aligned}$$

Ponieważ

$$\begin{aligned}
 \frac{1}{8} \cdot (4p_0(n+1)(n+2) + 2p_1n(n+1) + p_2n(n-1)) &= \\
 &= \frac{1}{8} \cdot (4p_0(2+3n+n^2) + 2p_1(n+n^2) + p_2(-n+n^2)) = \\
 &= \frac{1}{8} \cdot (8p_0 + (12p_0 + 2p_1 - p_2)n + (4p_0 + 2p_1 + p_2)n^2) = \\
 &= u_0 + u_1n + u_2n^2,
 \end{aligned}$$

gdzie

$$u_0 = p_0, \quad u_1 = \frac{12p_0 + 2p_1 - p_2}{8}, \quad u_2 = \frac{4p_0 + 2p_1 + p_2}{8},$$

więc

$$\pi \cdot (1 - 2\xi)^{-3} = \sum_{n=0}^{\infty} (u_0 + u_1n + u_2n^2) \cdot 2^n \xi^n.$$

Podobnie

$$\begin{aligned}
 \rho \cdot (1 + 3\xi)^{-2} &= (r_0 + r_1\xi) \cdot \sum_{n=0}^{\infty} (n+1) \cdot (-3)^n \xi^n = \\
 &= \sum_{n=0}^{\infty} r_0(n+1) \cdot (-3)^n \xi^n + \sum_{n=0}^{\infty} r_1(n+1) \cdot (-3)^n \xi^{n+1} = \\
 &= \sum_{n=0}^{\infty} r_0(n+1) \cdot (-3)^n \xi^n + \sum_{n=1}^{\infty} r_1n \cdot (-3)^{n-1} \xi^n = \\
 &= \sum_{n=0}^{\infty} r_0(n+1) \cdot (-3)^n \xi^n - \frac{1}{3} \sum_{n=0}^{\infty} r_1n \cdot (-3)^n \xi^n = \\
 &= \frac{1}{3} \cdot \sum_{n=0}^{\infty} (3r_0(n+1) - r_1n) \cdot (-3)^n \xi^n = \\
 &= \frac{1}{3} \cdot \sum_{n=0}^{\infty} (3r_0 + (3r_0 - r_1)n) \cdot (-3)^n \xi^n = \\
 &= \sum_{n=0}^{\infty} (v_0 + v_1n) \cdot (-3)^n \xi^n,
 \end{aligned}$$

gdzie

$$v_0 = r_0, \quad v_1 = \frac{3r_0 - r_1}{3}.$$

Wreszcie

$$\sigma \cdot (1 - 5\xi)^{-1} = s_0 \cdot \sum_{n=0}^{\infty} 5^n \xi^n = \sum_{n=0}^{\infty} w_0 \cdot 5^n \xi^n,$$

gdzie $w_0 = s_0$.

Łącznie otrzymujemy

$$\begin{aligned}\alpha &= \sum_{n=0}^{\infty} a_n \xi^n = \\ &= \pi \cdot (1 - 2\xi)^{-3} + \rho \cdot (1 + 3\xi)^{-2} + \sigma \cdot (1 - 5\xi)^{-1} = \\ &= \sum_{n=0}^{\infty} ((u_0 + u_1 n + u_2 n^2) \cdot 2^n + (v_0 + v_1 n) \cdot (-3)^n + w_0 \cdot 5^n) \xi^n,\end{aligned}$$

skąd wynika, że dla każdego $n \in \mathbb{N}$:

$$a_n = (u_0 + u_1 n + u_2 n^2) \cdot 2^n + (v_0 + v_1 n) \cdot (-3)^n + w_0 \cdot 5^n.$$

Zatem $\alpha \in V_4$. Pokazaliśmy więc, że $V_3 \subseteq V_4$. Ponieważ $\dim V_3 = \dim V_4 = 6$, więc $V_3 = V_4$.

Wszystkie cztery zdefiniowane podprzestrzenie liniowe przestrzeni $\mathbb{P}$ są równe. W szczególności $V_1 = V_4$, co dowodzi, że ciągi (a_n) spełniające równanie rekurencyjne (5.3), a więc należące do V_1 należą również do V_4 . To zaś znaczy, że ciągi te są określone wzorem ogólnym (5.4):

$$a_n = (u_0 + u_1 n + u_2 n^2) \cdot 2^n + (v_0 + v_1 n) \cdot (-3)^n + w_0 \cdot 5^n$$

dla pewnych liczb zespolonych $u_0, u_1, u_2, v_0, v_1, w_0$. To kończy dowód.

11. Równania rekurencyjne liniowe jednorodne o stałych współczynnikach – twierdzenie ogólne

W tym paragrafie udowodnimy twierdzenie o postaci rozwiązań równań rekurencyjnych liniowych jednorodnych o stałych współczynnikach.

Twierdzenie 5.2. Mamy dane równanie rekurencyjne liniowe jednorodne rzędu d

$$a_{n+d} + c_1 a_{n+d-1} + c_2 a_{n+d-2} + \dots + c_{d-1} a_{n+1} + c_d a_n = 0 \quad (5.5)$$

o stałych współczynnikach $c_1, c_2, \dots, c_d \in \mathbb{C}$ (przyjmujemy, że $c_d \neq 0$; w przeciwnym razie równanie miałoby rząd niższy niż d). Przypuśćmy, że równanie charakterystyczne

$$z^d + c_1 z^{d-1} + c_2 z^{d-2} + \dots + c_{d-1} z + c_d = 0$$

ma m pierwiastków zespolonych $r_1, \dots, r_m$ odpowiednio krotności $d_1, \dots, d_m$; oczywiście

$$d_1 + \dots + d_m = d.$$

Wówczas istnieją wielomiany

$$q_1 \in \mathbb{C}_{d_1}[X], \dots, q_m \in \mathbb{C}_{d_m}[X]$$

takie, że

$$a_n = q_1(n) \cdot r_1^n + \dots + q_m(n) \cdot r_m^n$$

dla $n = 0, 1, 2, \dots$

Dowód. Dowód zaczniemy od przekształcenia równania charakterystycznego. Oczywiście równanie charakterystyczne możemy zapisać w postaci

$$(z - r_1)^{d_1} \cdot (z - r_2)^{d_2} \cdot \dots \cdot (z - r_m)^{d_m} = 0.$$

Ponieważ $c_d \neq 0$, więc pierwiastki równania charakterystycznego są różne od zera. podstawmy zatem $\frac{1}{z}$ w miejsce z i pomnóżmy obie strony równania przez z^d , otrzymując kolejno

$$\begin{aligned} \left(\frac{1}{z} - r_1\right)^{d_1} \cdot \left(\frac{1}{z} - r_2\right)^{d_2} \cdot \dots \cdot \left(\frac{1}{z} - r_m\right)^{d_m} &= 0, \\ (1 - r_1 z)^{d_1} \cdot (1 - r_2 z)^{d_2} \cdot \dots \cdot (1 - r_m z)^{d_m} &= 0. \end{aligned}$$

Otrzymane równanie jest oczywiście równoważne równaniu

$$\frac{1}{z^d} + c_1 \cdot \frac{1}{z^{d-1}} + \dots + c_{d-1} \cdot \frac{1}{z} + c_d = 0,$$

czyli

$$1 + c_1 z + c_2 z^2 + \dots + c_{d-1} z^{d-1} + c_d z^d = 0.$$

Inaczej mówiąc, zachodzi równość wielomianów

$$1 + c_1 z + c_2 z^2 + \dots + c_{d-1} z^{d-1} + c_d z^d = (1 - r_1 z)^{d_1} \cdot (1 - r_2 z)^{d_2} \cdot \dots \cdot (1 - r_m z)^{d_m}.$$

Teraz, postępując tak jak w przykładzie, definiujemy cztery podprzestrzenie liniowe przestrzeni $\mathbb{P}$. Oto pierwsza z nich:

$$V_1 = \{\alpha = (a_n) \in \mathbb{P} : a_{n+d} + c_1 a_{n+d-1} + c_2 a_{n+d-2} + \dots + c_{d-1} a_{n+1} + c_d a_n = 0\}.$$

Sprawdzenie, że V_1 jest rzeczywiście podprzestrzenią $\mathbb{P}$ zostawiamy jako ćwiczenie. Ponieważ pierwsze d wyrazów ciągu α możemy wybrać dowolnie, a pozostałe są wyznaczone jednoznacznie przez równanie (5.5), więc $V_1 \cong \mathbb{C}^d$, czyli $\dim V_1 = d$.

Następnie definiujemy szereg formalny δ wzorem

$$\delta = (1, c_1, c_2, \dots, c_d, 0, 0, 0, \dots, 0, \dots).$$

Inaczej mówiąc, ciąg współczynników $c_1, c_2, \dots, c_d$ rozszerzamy, przyjmując

$$C_0 = 1, \quad c_n = 0 \quad \text{dla } n = d+1, d+2, d+3, \dots$$

Z rozważań przeprowadzonych na początku dowodu wynika, że

$$\delta = 1 + c_1 \xi + c_2 \xi^2 + \dots + c_{d-1} \xi^{d-1} + c_d \xi^d = (1 - r_1 \xi)^{d_1} \cdot (1 - r_2 \xi)^{d_2} \cdot \dots \cdot (1 - r_m \xi)^{d_m}.$$

Następnie definiujemy

$$\gamma = \delta^{-1} = (1 - r_1\xi)^{-d_1} \cdot (1 - r_2\xi)^{-d_2} \cdot \dots \cdot (1 - r_m\xi)^{-d_m}.$$

Teraz możemy zdefiniować drugą podprzestrzeń:

$$V_2 = \{\alpha \in \mathbb{P} : \exists \pi \in \mathbb{C}_d[\xi] (\alpha = \pi \cdot \gamma)\} = \{\alpha \in \mathbb{P} : \alpha \cdot \delta \in \mathbb{C}_d[\xi]\}.$$

Znów łatwo sprawdzamy, że V_2 jest podprzestrzenią $\mathbb{P}$ oraz $V_2 \cong \mathbb{C}_d[\xi] \cong \mathbb{C}^d$, czyli $\dim V_2 = d$. Pokazujemy następnie, że $V_2 \subseteq V_1$.

Niech zatem $\alpha \in V_2$. Wówczas $\pi = \alpha \cdot \delta \in \mathbb{C}_d[\xi]$. Niech

$$\pi = (p_0, p_1, \dots, p_d, 0, 0, 0, \dots, 0, \dots).$$

Wówczas

$$(a_0, a_1, \dots, a_n, \dots) \cdot (c_0, c_1, \dots, c_d, 0, 0, 0, \dots, 0, \dots) = (p_0, p_1, \dots, p_d, 0, 0, 0, \dots, 0),$$

czyli

$$\sum_{k=0}^d c_k a_{n-k} = 0$$

dla $n \geq d$. Podstawiając $n + d$ w miejsce n , otrzymujemy

$$\sum_{k=0}^d c_k a_{n+d-k} = 0$$

dla $n = 0, 1, 2, \dots$. Inaczej mówiąc

$$c_0 a_{n+d} + c_1 a_{n+d-1} + c_2 a_{n+d-2} + \dots + c_{d-1} a_{n+1} + c_d a_n = 0,$$

czyli

$$a_{n+d} + c_1 a_{n+d-1} + c_2 a_{n+d-2} + \dots + c_{d-1} a_{n+1} + c_d a_n = 0$$

dla $n = 0, 1, 2, \dots$. Zatem $\alpha \in V_1$. Stąd wynika, że $V_2 = V_1$.

Teraz definiujemy trzecią podprzestrzeń:

$$V_3 = \{\alpha \in \mathbb{P} : \exists \pi_1, \dots, \pi_m (\alpha = \pi_1 \cdot (1 - r_1\xi)^{-d_1} + \dots + \pi_m \cdot (1 - r_m\xi)^{-d_m})\},$$

gdzie $\pi_1 \in \mathbb{C}_{d_1}[\xi], \dots, \pi_m \in \mathbb{C}_{d_m}[\xi]$. Wówczas nietrudno zauważyć, że

$$V_3 \cong \mathbb{C}_{d_1}[\xi] \times \dots \times \mathbb{C}_{d_m}[\xi] \cong \mathbb{C}^{d_1} \times \dots \times \mathbb{C}^{d_m} \cong \mathbb{C}^d.$$

Zatem $\dim V_3 = d$. Tak jak w przykładzie w poprzednim paragrafie, pokazujemy, że $V_3 \subseteq V_2$.

Niech zatem $\alpha \in V_3$. Mamy pokazać, że $\alpha \cdot \delta \in \mathbb{C}_d[\xi]$, czyli, że $\alpha \cdot \delta$ jest wielomianem stopnia niższego niż d . Zauważmy w tym celu, że

$$\alpha \cdot \delta = \sum_{k=1}^m \pi_k \cdot (1 - r_k \xi)^{-d_k} \cdot \delta,$$

czyli

$$\begin{aligned} \alpha \cdot \delta &= \pi_1 \cdot (1 - r_2 \xi)^{d_2} \cdot \dots \cdot (1 - r_m \xi)^{d_m} + \\ &\quad + \pi_2 \cdot (1 - r_1 \xi)^{d_1} \cdot (1 - r_3 \xi)^{d_3} \cdot \dots \cdot (1 - r_m \xi)^{d_m} + \\ &\quad + \dots + \\ &\quad + \pi_1 \cdot (1 - r_1 \xi)^{d_1} \cdot \dots \cdot (1 - r_{k-1} \xi)^{d_{k-1}} \cdot (1 - r_{k+1} \xi)^{d_{k+1}} \cdot \dots \cdot (1 - r_m \xi)^{d_m} + \\ &\quad + \dots + \\ &\quad + \pi_1 \cdot (1 - r_1 \xi)^{d_1} \cdot \dots \cdot (1 - r_{m-1} \xi)^{d_{m-1}}. \end{aligned}$$

Pokażemy, że każdy składnik sumy po prawej stronie jest wielomianem stopnia niższego niż d . Bez straty ogólności można ograniczyć się do pierwszego składnika (każdy składnik może być wybrany jako pierwszy po odpowiednim przenumеровaniu pierwiastków równania charakterystycznego). Mamy zatem wielomian

$$\pi_1 \cdot (1 - r_2 \xi)^{d_2} \cdot \dots \cdot (1 - r_m \xi)^{d_m}.$$

Jego stopień jest równy

$$\deg \pi_1 + d_2 + \dots + d_m = \deg \pi_1 + d - d_1 < d_1 + d - d_1 = d,$$

bo stopień wielomianu π_1 jest mniejszy od d_1 . Stąd wynika, że $\deg(\alpha \cdot \delta) < d$, czyli $\alpha \cdot \delta \in \mathbb{C}_d[\xi]$. A więc $\alpha \in V_2$. Tak jak poprzednio, dostajemy stąd równość $V_2 = V_3$.

Wreszcie definiujemy czwartą podprzestrzeń:

$$V_4 = \{\alpha = (a_n) \in \mathbb{P} : \exists q_1 \in \mathbb{C}_{d_1}[X] \dots \exists q_m \in \mathbb{C}_{d_m}[X] \forall n (a_n = q_1(n) \cdot r_1^n + \dots + q_m(n) \cdot r_m^n)\}$$

i tak jak poprzednio zauważamy, że

$$V_4 \cong \mathbb{C}_{d_1}[X] \times \dots \times \mathbb{C}_{d_m}[X] \cong \mathbb{C}^{d_1} \times \dots \times \mathbb{C}^{d_m} \cong \mathbb{C}^d.$$

Zatem $\dim V_3 = d$ i znów tak jak w poprzednim paragrafie, pokazujemy, że $V_3 \subseteq V_4$.

Niech więc $\alpha \in V_3$. Wówczas

$$\alpha = \beta_1 + \dots + \beta_m,$$

gdzie

$$\beta_1 = \pi_1 \cdot (1 - r_1 \xi)^{-d_1}, \quad \text{gdzie } \pi_1 \in \mathbb{C}_{d_1}[\xi],$$

...

$$\beta_k = \pi_k \cdot (1 - r_k \xi)^{-d_k}, \quad \text{gdzie } \pi_k \in \mathbb{C}_{d_k}[\xi],$$

...

$$\beta_m = \pi_m \cdot (1 - r_m \xi)^{-d_m}, \quad \text{gdzie } \pi_m \in \mathbb{C}_{d_m}[\xi].$$

Niech $1 \leq k \leq m$ i niech

$$\pi_k = p_0 + p_1\xi + p_2\xi^2 + \dots + p_{d_k-1}\xi^{d_k-1},$$

czyli

$$\pi_k = p_0 + p_1\xi + p_2\xi^2 + \dots + p_{d_k-1}\xi^{d_k-1} + p_{d_k}\xi^{d_k} + \dots + p_n\xi^n + \dots,$$

gdzie $p_n = 0$ dla $n \geq d_k$. Korzystamy następnie ze wzoru (5.2):

$$(1 - r_k\xi)^{-d_k} = \sum_{n=0}^{\infty} \binom{n + d_k - 1}{d_k - 1} \cdot r_k^n \cdot \xi^n.$$

Mamy wówczas

$$\begin{aligned} \beta_k &= \pi_k \cdot (1 - r_k\xi)^{-d_k} = \\ &= (p_0 + p_1\xi + \dots + p_{d_k-1}\xi^{d_k-1}) \cdot \sum_{n=0}^{\infty} \binom{n + d_k - 1}{d_k - 1} \cdot r_k^n \cdot \xi^n = \\ &= \sum_{n=0}^{\infty} \left(\sum_{j=0}^n p_j \binom{n - j + d_k - 1}{d_k - 1} \cdot r_k^{n-j} \right) \xi^n. \end{aligned}$$

Wprowadzimy teraz nowe oznaczenie. Przypomnijmy, że symbolem $(x)_n$ oznaczaliśmy wielomian

$$(x)_n = x(x-1)(x-2) \cdot \dots \cdot (x-n+1)$$

dla $n = 1, 2, 3, \dots$. Oznaczmy również $(x)_0 = 1$. Zdefiniujemy wielomian $\binom{x}{n}$ wzorem:

$$\binom{x}{n} = \frac{(x)_n}{n!}$$

dla $n = 0, 1, 2, \dots$. Ponieważ wielomian $(x)_n$ ma stopień n , więc $\binom{x}{n}$ jest też wielomianem stopnia n . Stąd wynika, że

$$\binom{X - j + d_k - 1}{d_k - 1} = \frac{1}{(d_k - 1)!} \cdot (X - j + d_k - 1)(X - j + d_k - 2) \cdot \dots \cdot (X - j + d_k - (d_k - 1))$$

jest wielomianem stopnia $d_k - 1$ zmiennej X . Definiujemy teraz wielomian $q_k(X)$ wzorem:

$$q_k(X) = \sum_{j=0}^n p_j \binom{X - j + d_k - 1}{d_k - 1}.$$

Oczywiście wielomian $q_k(X)$ ma stopień co najwyżej równy $d_k - 1$. Niech ponadto

$$\beta_k = (b_0, b_1, b_2, \dots, b_n, \dots).$$

Wówczas

$$\beta_k = \sum_{n=0}^{\infty} q_k(n) \cdot r_k^n \xi^n,$$

czyli

$$b_n = q_k(n) \cdot r_k^n$$

dla $n = 0, 1, 2, \dots$. Z równości $\alpha = \beta_1 + \dots + \beta_m$ wynika teraz, że

$$a_n = q_1(n) \cdot r_1^n + \dots + q_m(n) \cdot r_k^n$$

dla $n \geq 0$. To dowodzi, że $\alpha \in V_4$.

Zatem $V_1 = V_2 = V_3 = V_4$. Stąd wynika, że każdy ciąg $\alpha = (a_n) \in \mathbb{P}$ spełniający równanie rekurencyjne (5.5) należy do przestrzeni V_4 . Istnieją zatem wielomiany

$$q_1 \in \mathbb{C}_{d_1}[X], \dots, q_m \in \mathbb{C}_{d_m}[X]$$

o tej własności, że ciąg $\alpha = (a_n)$ jest określony wzorem ogólnym

$$a_n = q_1(n) \cdot r_1^n + \dots + q_m(n) \cdot r_k^n$$

dla $n = 0, 1, 2, \dots$. To kończy dowód twierdzenia 5.2.

12. Pierwiastki kwadratowe

Przypuśćmy, że dany jest szereg formalny

$$\alpha = (1, a_1, a_2, \dots, a_n, \dots) \in \mathbb{P}_1.$$

Wyznamy teraz szereg formalny

$$\beta = (b_0, b_1, b_2, \dots, b_n, \dots)$$

taki, że $\beta = \alpha^2$. Mamy kolejno

$$b_0 = 1 \cdot 1 = 1,$$

$$b_1 = 1 \cdot a_1 + a_1 \cdot 1 = 2a_1,$$

$$b_2 = 1 \cdot a_2 + a_1 \cdot a_1 + a_1 \cdot 1 = 2a_2 + a_1^2,$$

$$b_3 = 1 \cdot a_3 + a_1 \cdot a_2 + a_2 \cdot a_1 + a_3 \cdot 1 = 2a_3 + 2a_1a_2,$$

$$b_4 = 1 \cdot a_4 + a_1 \cdot a_3 + a_2 \cdot a_2 + a_3 \cdot a_1 + a_4 \cdot 1 = 2a_4 + 2a_1a_3 + a_2^2$$

i ogólnie

$$b_n = 2a_n + a_1a_{n-1} + a_2a_{n-2} + \dots + a_{n-1}a_1 = 2a_n + \sum_{k=1}^{n-1} a_k a_{n-k}.$$

Powyższe wzory pozwalają rozwiązać zadanie odwrotne. Niech będzie dany szereg formalny $\beta \in \mathbb{P}_1$. Istnieje wówczas dokładnie jeden szereg formalny $\alpha \in \mathbb{P}_1$ taki, że $\alpha^2 = \beta$. Wykażemy najpierw jednoznaczność.

Przypuśćmy bowiem, że mamy dane dwa szeregi formalne $\alpha, \gamma \in \mathbb{P}_1$ takie, że

$$\alpha^2 = \gamma^2 = \beta.$$

Wówczas $\alpha^2 - \gamma^2 = 0$, czyli $(\alpha - \gamma)(\alpha + \gamma) = 0$. Zatem $\alpha = \gamma$ lub $\alpha = -\gamma$. Ale $\alpha, \gamma \in \mathbb{P}_1$, czyli $Z(\alpha) = Z(\gamma) = 1$. Gdyby $\alpha = -\gamma$, to mielibyśmy $Z(\alpha) = -Z(\gamma) = -1$, co jest sprzeczne z założeniem. Zatem $\alpha = \gamma$.

Szereg formalny α taki, że $\alpha^2 = \beta$ definiujemy przez indukcję:

$$\begin{aligned} a_0 &= 1, \\ a_1 &= \frac{b_1}{2}, \\ a_2 &= \frac{b_2 - a_1^2}{2}, \\ &\dots \quad \dots \\ a_n &= \frac{b_n - (a_1 a_{n-1} + a_2 a_{n-2} + \dots + a_{n-1} a_1)}{2} = \frac{b_n}{2} - \frac{1}{2} \cdot \sum_{k=0}^{n-1} a_k a_{n-k}. \end{aligned}$$

Z poprzednio wyprowadzonych wzorów wynika, że rzeczywiście $\alpha^2 = \beta$.

Jeśli $\beta \in \mathbb{P}_1$, to szereg $\alpha \in \mathbb{P}_1$ taki, że $\alpha^2 = \beta$ nazywamy **pierwiastkiem kwadratowym** szeregu β i oznaczamy symbolem $\sqrt{\beta}$ lub $\beta^{\frac{1}{2}}$.

Pokażemy teraz jeden przykład pierwiastka kwadratowego. Ten przykład będzie wykorzystany w dalszej części tego wykładu. Niech

$$\beta = (1 - 4\xi)^{-1} = \sum_{n=0}^{\infty} 4^n \xi^n = (1, 4, 4^2, \dots, 4^n, \dots).$$

Oczywiście $\beta \in \mathbb{P}_1$. Obliczymy kolejne wyrazy szeregu

$$\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \in \mathbb{P}_1$$

takiego, że $\alpha^2 = \beta$. Mamy kolejno:

$$\begin{aligned} a_0 &= 1, \\ a_1 &= \frac{b_1}{2} = 2, \\ a_2 &= \frac{b_2 - a_1^2}{2} = \frac{4^2 - 2^2}{2} = 6, \\ a_3 &= \frac{b_3 - 2a_1a_2}{2} = \frac{4^3 - 2 \cdot 2 \cdot 6}{2} = 20, \\ a_4 &= \frac{b_4 - 2a_1a_3 - a_2^2}{2} = \frac{4^4 - 2 \cdot 2 \cdot 20 - 6^2}{2} = 70. \end{aligned}$$

Otrzymane liczby wyglądają znajomo, jeśli przypomnimy sobie początkowe wiersze trójkąta Pascala:

$$\begin{array}{cccccccccccccccc}
 & & & & & & & & 1 & & & & & & & & \\
 & & & & & & & & & 1 & & & & & & & \\
 & & & & & & & & & & 1 & & & & & & \\
 & & & & & & & & 1 & & 2 & & 1 & & & & \\
 & & & & & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
 & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
 \end{array}$$

Narzuca się hipoteza:

$$a_n = \binom{2n}{n} \quad \text{dla } n \geq 0,$$

czyli

$$(1 - 4\xi)^{-1/2} = \sum_{n=0}^{\infty} \binom{2n}{n} \xi^n.$$

W następnych paragrafach udowodnimy tę hipotezę.

„Tożsamość 4^n ”

W tym paragrafie pokażemy trzy dowody następującej tożsamości kombinatorycznej:

$$\sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} = 4^n. \quad (5.6)$$

Dowód I. Definiujemy funkcje $S_n(x)$ ($k = 0, 1, 2, \dots$) wzorem:

$$S_n(x) = \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} x^k$$

dla $x \in \mathbb{R}$. Różniczkując obie strony otrzymujemy:

$$S'_n(x) = \sum_{k=0}^n k \binom{2k}{k} \binom{2n-2k}{n-k} x^{k-1}$$

dla $x \in \mathbb{R}$. Zmieniając kolejność sumowania (czyli podstawiając $k := n - k$), otrzymujemy

$$S_n(x) = \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} x^{n-k},$$

skąd dostajemy

$$x^n \cdot S_n(x^{-1}) = x^n \cdot \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} x^{k-n} = S_n(x).$$

Następnie różniczkujemy obie strony równości

$$S_n(x) = x^n \cdot S_n(x^{-1}).$$

Otrzymujemy

$$\begin{aligned} S'_n(x) &= (x^n)' \cdot S_n(x^{-1}) + x^n \cdot (S_n(x^{-1}))' = nx^{n-1} S_n(x^{-1}) + x^n \cdot S'_n(x^{-1}) \cdot (-x^{-2}) = \\ &= nx^{n-1} \cdot S_n(x^{-1}) - x^{n-2} \cdot S'_n(x^{-1}). \end{aligned}$$

Podstawiając teraz $x = 1$, otrzymujemy

$$S'_n(1) = x \cdot S_n(1) - S'_n(1),$$

czyli

$$S'_n(1) = \frac{n}{2} \cdot S_n(1).$$

Z drugiej strony

$$S_{n+1}(x) = \sum_{k=0}^{n+1} \binom{2k}{k} \binom{2n+2-2k}{n+1-k} x^k,$$

skąd otrzymujemy

$$\begin{aligned} S'_{n+1}(x) &= \sum_{k=0}^{n+1} k \binom{2k}{k} \binom{2n+2-2k}{n+1-k} x^{k-1} = \sum_{k=1}^{n+1} k \binom{2k}{k} \binom{2n+2-2k}{n+1-k} x^{k-1} = \\ &= \sum_{k=0}^n (k+1) \binom{2k+2}{k+1} \binom{2n-2k}{n-k} x^k = \\ &= \sum_{k=0}^n (k+1) \cdot \frac{2k+2}{k+1} \cdot \binom{2k+1}{k} \binom{2n-2k}{n-k} x^k = \\ &= \sum_{k=0}^n (2k+2) \cdot \binom{2k+1}{k+1} \binom{2n-2k}{n-k} x^k = \\ &= \sum_{k=0}^n (2k+2) \cdot \frac{2k+1}{k+1} \cdot \binom{2k}{k} \binom{2n-2k}{n-k} x^k = \\ &= \sum_{k=0}^n 2(2k+1) \cdot \binom{2k}{k} \binom{2n-2k}{n-k} x^k = \\ &= 4 \cdot \sum_{k=0}^n k \cdot \binom{2k}{k} \binom{2n-2k}{n-k} x^k + 2 \cdot \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} x^k = \\ &= 4x \cdot \sum_{k=0}^n k \cdot \binom{2k}{k} \binom{2n-2k}{n-k} x^{k-1} + 2 \cdot \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} x^k = \\ &= 4x \cdot S'_n(x) + 2 \cdot S_n(x). \end{aligned}$$

Teraz podstawiamy $x = 1$:

$$S'_{n+1}(1) = 4 \cdot S'_n(1) + 2 \cdot S_n(1) = 4 \cdot \frac{n}{2} \cdot S_n(1) + 2 \cdot S_n(1) = (2n + 2) \cdot S_n(1).$$

Ponieważ także

$$S'_{n+1}(1) = \frac{n+1}{2} \cdot S_{n+1}(1),$$

więc

$$\frac{n+1}{2} \cdot S_{n+1}(1) = (2n+2) \cdot S_n(1),$$

czyli

$$S_{n+1}(1) = 4 \cdot S_n(1).$$

Ponieważ

$$S_0(1) = \sum_{k=0}^0 \binom{2k}{k} \binom{0-2k}{0-k} 1^k = 1,$$

więc przez indukcję $S_n(1) = 4^n$. Zatem

$$\sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} = S_n(1) = 4^n,$$

co kończy dowód.

Dowód II. Przypomnijmy tożsamość Cauchy'ego:

$$\sum_{j=0}^k \binom{m}{j} \binom{n}{k-j} = \binom{m+n}{k}.$$

Przypomnijmy oznaczenia, których niedawno używaliśmy: symbolem $(x)_n$ oznaczaliśmy wielomian

$$(x)_n = x(x-1)(x-2) \cdots (x-n+1)$$

dla $n = 1, 2, 3, \dots$. Przyjmujemy również $(x)_0 = 1$. Wprowadziliśmy także oznaczenie:

$$\binom{x}{n} = \frac{(x)_n}{n!}$$

dla $n = 0, 1, 2, \dots$. Niech teraz

$$W(x) = \sum_{j=0}^k \binom{x}{j} \binom{n}{k-j}$$

oraz

$$V(x) = \binom{x+n}{k}.$$

Wielomiany $W(x)$ i $V(x)$ przyjmują te same wartości dla nieskończenie wielu argumentów: $W(m) = V(n)$ dla $n \in \mathbb{N}$. Zatem są identyczne; w szczególności $W(x) = V(x)$ dla dowolnej liczby rzeczywistej x . Weźmy teraz dowolną liczbę $r \in \mathbb{R}$ i rozważmy wielomiany zmiennej y :

$$U(y) = \sum_{j=0}^k \binom{r}{j} \binom{y}{k-j}$$

oraz

$$T(y) = \binom{r+y}{k}.$$

Wielomiany $U(y)$ i $T(y)$ przyjmują te same wartości dla nieskończenie wielu argumentów: $U(n) = T(n)$ dla $n \in \mathbb{N}$. Zatem są identyczne, czyli dla dowolnej liczby rzeczywistej s zachodzi równość $U(s) = T(s)$. To znaczy, że dla dowolnych $r, s \in \mathbb{R}$ mamy:

$$\sum_{j=0}^k \binom{r}{j} \binom{s}{k-j} = \binom{r+s}{k}.$$

Uwaga. Można udowodnić (co pozostawiamy jako ćwiczenie), że jeśli dwa wielomiany $W(x, y)$ i $V(x, y)$ dwóch zmiennych x i y przyjmują te same wartości dla wszystkich $r, s \in \mathbb{R}$ (tzn. $W(r, s) = V(r, s)$), to są identyczne: $W(x, y) = V(x, y)$.

Podstawmy teraz $r = s = -\frac{1}{2}$. Otrzymujemy

$$\sum_{j=0}^k \binom{-\frac{1}{2}}{j} \binom{-\frac{1}{2}}{k-j} = \binom{-1}{k}.$$

Obliczymy teraz współczynniki dwumianowe występujące po obu stronach powyższej równości.

Pokażemy najpierw, że dla dowolnego $n = 0, 1, 2, \dots$ mamy

$$\binom{-1}{n} = (-1)^n.$$

Dla $n = 0$ ta równość jest oczywista. Niech $n \geq 1$. Mamy teraz

$$\begin{aligned} \binom{-1}{n} &= \frac{(-1)_n}{n!} = \frac{(-1) \cdot (-1-1) \cdot (-1-2) \cdot \dots \cdot (-1-n+1)}{n!} = \\ &= \frac{(-1) \cdot (-2) \cdot (-3) \cdot \dots \cdot (-n)}{n!} = \frac{(-1)^n \cdot n!}{n!} = (-1)^n. \end{aligned}$$

Pokażemy teraz, że dla dowolnego $n = 0, 1, 2, \dots$ mamy

$$\binom{-\frac{1}{2}}{n} = \frac{(-1)^n}{4^n} \cdot \binom{2n}{n}.$$

Znów dla $n = 0$ równość jest oczywista. Niech zatem $n \geq 1$. Mamy wówczas

$$\begin{aligned}
 \binom{-\frac{1}{2}}{n} &= \frac{\left(-\frac{1}{2}\right)_n}{n!} = \frac{\left(-\frac{1}{2}\right) \cdot \left(-\frac{1}{2} - 1\right) \cdot \left(-\frac{1}{2} - 2\right) \cdot \dots \cdot \left(-\frac{1}{2} - n + 1\right)}{n!} = \\
 &= \frac{\left(-\frac{1}{2}\right) \cdot \left(-\frac{3}{2}\right) \cdot \left(-\frac{5}{2}\right) \cdot \dots \cdot \left(-\frac{2n-1}{2}\right)}{n!} = \frac{(-1) \cdot (-3) \cdot (-5) \cdot \dots \cdot (-(2n-1))}{2^n \cdot n!} = \\
 &= \frac{(-1)^n \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{2^n \cdot n!} = \\
 &= \frac{(-1)^n \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{2^n \cdot n!} \cdot \frac{2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n)}{2 \cdot 4 \cdot 6 \cdot \dots \cdot (2n)} = \frac{(-1)^n \cdot (2n)!}{2^n \cdot n! \cdot 2^n \cdot n!} = \\
 &= \frac{(-1)^n \cdot (2n)!}{4^n \cdot n! \cdot n!} = \frac{(-1)^n}{4^n} \cdot \frac{(2n)!}{n! \cdot n!} = \frac{(-1)^n}{4^n} \cdot \binom{2n}{n}.
 \end{aligned}$$

Podstawmy teraz obliczone wartości do równości

$$\sum_{j=0}^k \binom{-\frac{1}{2}}{j} \binom{-\frac{1}{2}}{k-j} = \binom{-1}{k}.$$

Otrzymamy

$$\sum_{j=0}^k \frac{(-1)^j}{4^j} \cdot \binom{2j}{j} \cdot \frac{(-1)^{k-j}}{4^{k-j}} \cdot \binom{2k-2j}{k-j} = (-1)^k,$$

czyli

$$\sum_{j=0}^k \frac{(-1)^k}{4^k} \cdot \binom{2j}{j} \cdot \binom{2k-2j}{k-j} = (-1)^k.$$

Zatem

$$\frac{(-1)^k}{4^k} \cdot \sum_{j=0}^k \binom{2j}{j} \binom{2k-2j}{k-j} = (-1)^k,$$

czyli

$$\sum_{j=0}^k \binom{2j}{j} \binom{2k-2j}{k-j} = 4^k,$$

co kończy dowód.

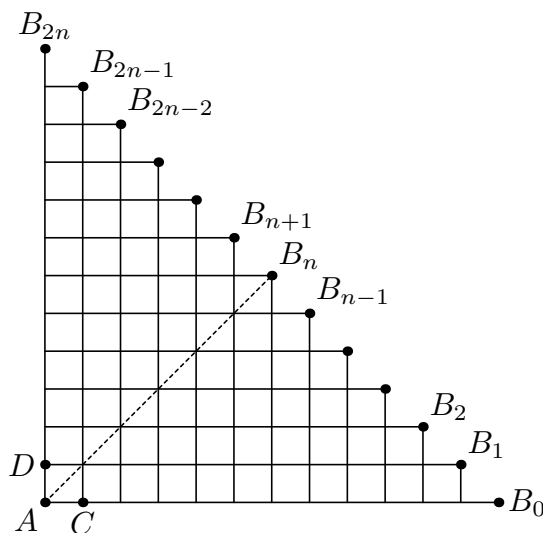
Dowód III. Przeprowadzimy dowód kombinatoryczny.

Udowodnimy najpierw następujący lemat.

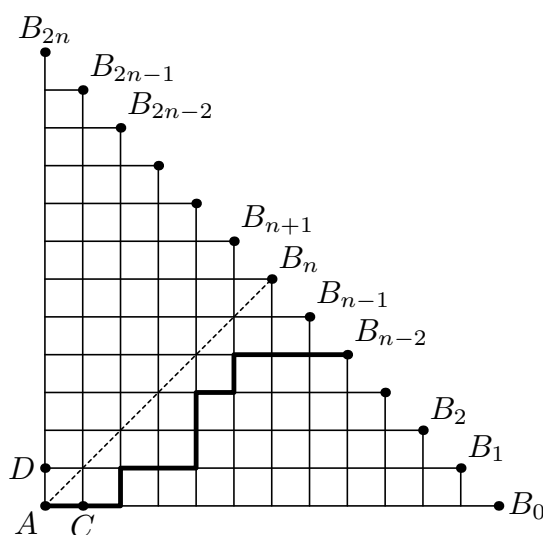
Lemat 5.3. Istnieje $\binom{2n}{n}$ ciągów f długości $2n$ o wyrazach ze zbioru $\{0, 1\}$, mających następującą własność: dla każdej liczby $k \in [2n]$

$$|\{i \in [k] : f(i) = 0\}| \neq |\{i \in [k] : f(i) = 1\}|.$$

Dowód. Popatrzmy najpierw na ilustrację graficzną naszego lematu. Ciągi zerojedynkowe (tzn. o wyrazach ze zbioru $\{0, 1\}$) kodujemy za pomocą dróg na papierze w kratkę. Wyrazowi 0 odpowiada odcinek poziomy, wyrazowi 1 odpowiada odcinek pionowy; wyruszamy z ustalonego punktu A i poruszamy się wyłącznie w prawo i do góry.

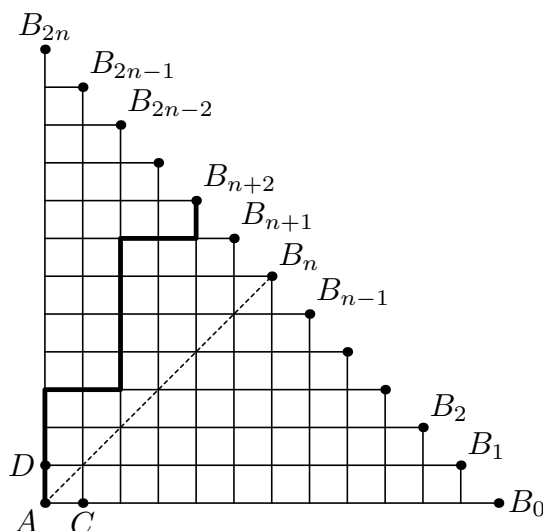


Zauważmy, że droga długości $2n$ zakończy się w jednym z punktów $B_0, B_1, \dots, B_{2n}$; są to punkty leżące na odcinku łączącym punkty B_0 i B_{2n} oddalone od punktu A o $2n$ kratek. Warunek sformułowany w lemacie oznacza, że poprowadzona droga nigdzie (poza punktem wyjścia A) nie dotknie przekątnej: linii łączącej punkt A z punktem B_n . Takie drogi będziemy nazywać drogami **omijającymi przekątną**. Przykład drogi omijającej przekątną widzimy na następnym rysunku:



Drogi omijające przekątną dzielą się na dwa zbiory: drogi zaczynające się od kroku w prawo (czyli do punktu C) i drogi zaczynające się od kroku w górę (do punktu D). Oczywiście drogi omijające przekątną i przechodzące przez punkt C muszą zakończyć się w jednym z punktów $B_0, \dots, B_{n-1}$. Drogi omijające przekątną i przechodzące przez

punkt D zakończą się w jednym z punktów $B_{n+1}, \dots, B_{2n}$. Na następnym rysunku widzimy jedną z takich dróg przechodzących przez punkt D .

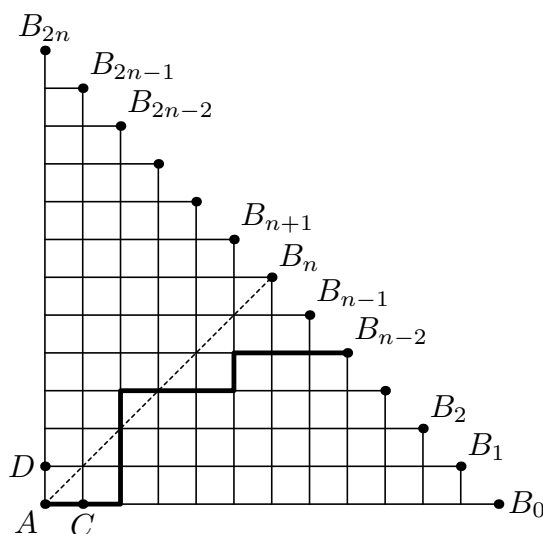


Ze względu na symetrię liczba dróg omijających przekątną i przechodzących przez punkt C jest równa liczbie dróg omijających przekątną i przechodzących przez punkt D . Policzmy te pierwsze drogi. Pomysł polega na tym, by od liczby wszystkich dróg odjąć liczbę dróg, które nie omijają przekątnej.

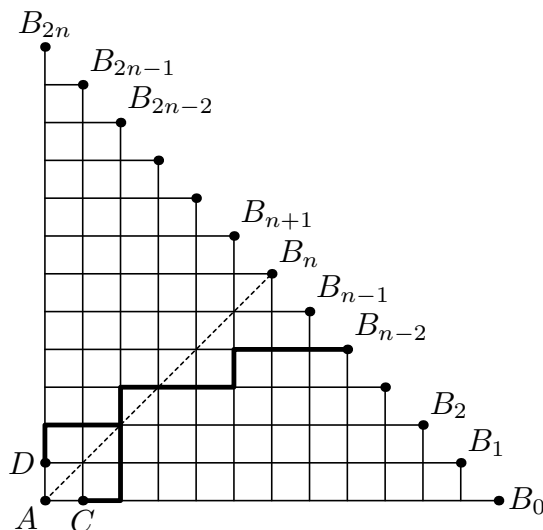
Wprowadźmy wygodne oznaczenie. Jeśli X i Y są dwoma punktami kratowymi, to symbolem $d(X, Y)$ będziemy oznaczać liczbę dróg z X do Y zgodnych z zasadami poruszania się po kratkach (tzn. tylko w prawo i do góry). Wiemy już, że drogi omijające przekątną i przechodzące przez punkt C kończą się w jednym z punktów $B_0, \dots, B_{n-1}$. Liczba wszystkich dróg z A przez C do jednego z tych n punktów jest zatem równa

$$\sum_{k=0}^{n-1} d(C, B_k).$$

Odejmijmy od tej liczby liczbę dróg „złych”: prowadzących z A przez C do jednego z tych n punktów, ale nie omijających przekątnej. Oto przykład takiej drogi:



Droga „zła” w co najmniej jednym punkcie dotyka przekątnej. Fragment tej drogi od punktu C do pierwszego punktu na przekątnej odbijamy symetrycznie względem przekątnej. Otrzymujemy drogę z punktu D do jednego z punktów $B_1, \dots, B_{n-1}$ (zauważmy, że jedyna droga z C do B_0 nie dotyka przekątnej; dlatego pomijamy punkt B_0 jako jeden z punktów końcowych dróg „złych”):



Odwrotnie, każda droga z punktu D do jednego z punktów $B_1, \dots, B_{n-1}$ musi przeciąć przekątną, a więc powstaje z dokładnie jednej drogi „złej” przez odbicie symetryczne. Stąd wynika, że liczba dróg „złych” jest równa

$$\sum_{k=1}^{n-1} d(D, B_k).$$

Zauważmy następnie, że dla każdego $k = 1, 2, \dots, n-1$ mamy równość

$$d(D, B_k) = d(C, B_{k-1}).$$

Mianowicie każdą drogę z D do B_k przesuwamy o jedną kratkę w prawo i jedną w dół, otrzymując w ten sposób drogę z C do B_{k-1} ; to przekształcenie dróg jest oczywiście wzajemnie jednoznaczne. Stąd wynika, że liczba dróg „złych” z C do punktów $B_1, \dots, B_{n-1}$ jest równa

$$\sum_{k=1}^{n-1} d(D, B_k) = \sum_{k=1}^{n-1} d(C, B_{k-1}) = \sum_{k=0}^{n-2} d(C, B_k).$$

Liczba dróg z A przez C omijających przekątną jest zatem równa

$$\sum_{k=0}^{n-1} d(C, B_k) - \sum_{k=0}^{n-2} d(C, B_k) = d(C, B_{n-1}).$$

Wystarczy teraz zauważyć, że jeśli $f \in A_k$, to ciąg f można podzielić jednoznacznie na dwa ciągi: ciąg $f|_{[2k]}$, w którym jest po k zer i jedynek (jest $\binom{2k}{k}$ takich ciągów) i ciąg $f|_{\{2k+1, \dots, 2n\}}$, kodowany za pomocą drogi omijającej przekątną (jest $\binom{2n-2k}{n-k}$ takich dróg). Zatem

$$|A_k| = \binom{2n-2k}{n-k},$$

skąd wynika, że

$$\sum_{k=0}^n |A_k| = \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} = 4^n,$$

co kończy dowód.

13. Przykład pierwiastka kwadratowego

Rozważmy szereg formalny α zdefiniowany wzorem

$$\alpha = (a_0, a_1, a_2, a_3, \dots, a_n, \dots) = \left(1, \binom{2}{1}, \binom{4}{2}, \binom{6}{3}, \dots, \binom{2n}{n}, \dots\right),$$

czyli

$$a_n = \binom{2n}{n}$$

dla $n = 0, 1, 2, \dots$. Oczywiście $\alpha \in \mathbb{P}_1$. Obliczmy teraz $\beta = \alpha^2$. Niech zatem

$$\beta = (b_0, b_1, b_2, \dots, b_n, \dots).$$

Wówczas ze wzoru Cauchy'ego i z „tożsamości 4^n ” wynika, że

$$b_n = \sum_{k=0}^n a_k a_{n-k} = \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} = 4^n$$

dla $n = 0, 1, 2, \dots$. Zatem

$$\beta = (1 - 4\xi)^{-1},$$

czyli

$$\alpha^2 = (1 - 4\xi)^{-1}.$$

Ponieważ $\alpha \in \mathbb{P}_1$, więc zgodnie z przyjętą konwencją możemy napisać, że

$$\alpha = \sqrt{(1 - 4\xi)^{-1}} = (1 - 4\xi)^{-1/2}.$$

Niech teraz szereg γ będzie zdefiniowany wzorem $\gamma = 1 - 4\xi$. Oczywiście $\gamma \cdot \beta = 1$ oraz $\gamma \in \mathbb{P}_1$. Niech zatem $\delta \in \mathbb{P}_1$ będzie szeregiem takim, że $\delta^2 = \gamma$ (czyli $\delta = \sqrt{1 - 4\xi}$). Mamy wówczas

$$\alpha^2 \cdot \gamma^2 = \beta \cdot \gamma \cdot \gamma = \gamma = \delta^2,$$

skąd wynika, że $\alpha \cdot \gamma = \delta$. Stąd otrzymujemy

$$\delta = (1 - 4\xi) \cdot \alpha = \alpha - 4 \cdot \xi \cdot \alpha.$$

Niech

$$\delta = (d_0, d_1, d_2, \dots, d_n, \dots).$$

Wówczas

$$d_0 = a_0 \quad \text{oraz} \quad d_n = a_n - 4a_{n-1} \quad \text{dla } n \geq 1.$$

Zatem $d_0 = 1$ oraz

$$\begin{aligned} d_n &= a_n - 4a_{n-1} = \binom{2n}{n} - 4 \cdot \binom{2n-2}{n-1} = \frac{2n}{n} \cdot \binom{2n-1}{n-1} - 4 \cdot \binom{2n-2}{n-1} = \\ &= 2 \cdot \binom{2n-1}{n-1} - 4 \cdot \binom{2n-2}{n-1} = 2 \cdot \left(\binom{2n-1}{n-1} - 2 \cdot \binom{2n-2}{n-1} \right) = \\ &= 2 \cdot \left(\binom{2n-2}{n-1} + \binom{2n-2}{n-2} - 2 \cdot \binom{2n-2}{n-1} \right) = \\ &= 2 \cdot \left(\binom{2n-2}{n-2} - \binom{2n-2}{n-1} \right) = 2 \cdot \left(\frac{n-1}{n} \cdot \binom{2n-2}{n-1} - \binom{2n-2}{n-1} \right) = \\ &= -\frac{2}{n} \cdot \binom{2n-2}{n-1}. \end{aligned}$$

Stąd wynika, że

$$\sqrt{1-4\xi} = \delta = 1 - 2 \cdot \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^n.$$

14. Liczby Catalana

Przypomnijmy, że ciąg liczb Catalana C_n spełniał następujące równanie rekurencyjne:

$$C_0 = 1, \quad C_n = C_0 C_{n-1} + C_1 C_{n-2} + \dots + C_{n-1} C_0 = \sum_{k=0}^{n-1} C_k C_{n-1-k} \quad \text{dla } n \geq 1.$$

Niech γ będzie szeregiem formalnym zdefiniowanym w następujący sposób:

$$\gamma = \sum_{n=0}^{\infty} C_n \xi^n,$$

czyli

$$\gamma = (C_0, C_1, C_2, \dots, C_n, \dots).$$

Wówczas ze wzoru Cauchy'ego wynika, że

$$\gamma^2 = C_0^2 + (C_0 C_1 + C_1 C_0) \xi + (C_0 C_2 + C_1 C_1 + C_2 C_0) \xi^2 + \dots$$

Dokładniej, przyjmijmy

$$\alpha = \gamma^2 = (a_0, a_1, a_2, \dots, a_n, \dots).$$

Wówczas

$$a_n = \sum_{k=0}^n C_k C_{n-k} = C_{n+1}$$

dla $n = 0, 1, 2, \dots$. Stąd wynika, że

$$1 + \xi \cdot \alpha = \gamma,$$

czyli

$$\xi \cdot \gamma^2 = \gamma - 1.$$

Pomnóżmy obie strony ostatniej równości przez ξ :

$$(\xi \cdot \gamma)^2 = \xi \cdot \gamma - \xi.$$

Przyjmijmy następnie $\beta = \xi \cdot \gamma$. Wtedy oczywiście $\beta \in \mathbb{P}_0$ oraz

$$\beta^2 - \beta + \xi = 0.$$

Rozwiązujemy otrzymane równanie w pierścieniu $\mathbb{P}$. Mamy najpierw

$$\Delta = (-1)^2 - 4 \cdot \xi = 1 - 4\xi.$$

Oczywiście $\Delta \in \mathbb{P}_1$. Niech zatem $\delta = \sqrt{\Delta}$ i niech $\delta \in \mathbb{P}_1$. Nasze równanie kwadratowe ma dwa pierwiastki:

$$\beta_1 = (1 - \delta) \cdot 2^{-1} \quad \text{oraz} \quad \beta_2 = (1 + \delta) \cdot 2^{-1}.$$

Mamy wówczas

$$Z(\beta_1) = Z(1 - \delta) \cdot 2^{-1} = (1 - Z(\delta)) \cdot 2^{-1} = (1 - 1) \cdot 2^{-1} = 0$$

oraz

$$Z(\beta_2) = Z(1 + \delta) \cdot 2^{-1} = (1 + Z(\delta)) \cdot 2^{-1} = (1 + 1) \cdot 2^{-1} = 1.$$

Ponieważ $\beta \in \mathbb{P}_0$, więc $\beta = \beta_1$. Zatem

$$\beta = (1 - \delta) \cdot 2^{-1} = (1 - \sqrt{1 - 4\xi}) \cdot 2^{-1}.$$

Z poprzedniego paragrafu wiemy, że

$$\sqrt{1 - 4\xi} = 1 - 2 \cdot \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^n,$$

czyli

$$1 - \sqrt{1 - 4\xi} = 2 \cdot \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^n.$$

Zatem

$$\beta = (1 - \sqrt{1 - 4\xi}) \cdot 2^{-1} = \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^n = \xi \cdot \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^{n-1}.$$

Ponieważ $\beta = \xi \cdot \gamma$, więc

$$\xi \cdot \gamma = \xi \cdot \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^{n-1}.$$

Z prawa skracania wynika zatem, że

$$\gamma = \sum_{n=1}^{\infty} \frac{1}{n} \binom{2n-2}{n-1} \xi^{n-1} = \sum_{n=0}^{\infty} \frac{1}{n+1} \binom{2n}{n} \xi^n,$$

skąd ostatecznie dostajemy

$$C_n = \frac{1}{n+1} \cdot \binom{2n}{n}.$$

Zliczanie drzew; twierdzenie Cayleya.

Zacniemy od paru faktów pomocniczych.

Twierdzenie. Jeśli f i g są wielomianami (ogólniej: funkcjami różniczkowalnymi) takimi, że

$$\begin{aligned}\forall x \in \mathbb{R} \quad (f'(x) &= g'(x)), \\ \exists x \in \mathbb{R} \quad (f(x) &= g(x)),\end{aligned}$$

to

$$\forall x \in \mathbb{R} \quad (f(x) = g(x)).$$

Przypomnienie. Liczba funkcji

$$f : \{1, \dots, j\} \xrightarrow{\text{na}} \{1, \dots, n\}$$

jest równa

$$s_{j,n} = \sum_{k=0}^n (-1)^k \binom{n}{k} (n-k)^j = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^j.$$

W szczególności, jeśli $j < n$, to

$$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^j = 0.$$

Tożsamości Abela.

- 1) $\sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k} = (x+y+n)^n,$
- 2) $\sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} = \left(\frac{1}{x} + \frac{1}{y}\right) \cdot (x+y+n)^{n-1},$
- 3) $\sum_{k=1}^{n-1} \binom{n}{k} k^{k-1} (n-k)^{n-k-1} = 2(n-1)n^{n-2}.$

Dowody.

$$(1) \quad \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k} = (x+y+n)^n.$$

Dowodzimy tej równości przez indukcję względem n . Dla $n = 0$ (a także dla $n = 1$) jest ona oczywista. W kroku indukcyjnym zakładamy równość dla $n-1$ oraz dowolnych $x, y \in \mathbb{R}$ i dowodzimy jej dla n .

Dla ustalonego $y \in \mathbb{R}$ definiujemy dwie funkcje:

$$\begin{aligned}f(x) &= \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k}, \\ g(x) &= (x+y+n)^n.\end{aligned}$$

Wówczas

$$\begin{aligned}f(x) &= \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k} = \\ &= \sum_{k=0}^{n-1} \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k} + y(y+n)^n,\end{aligned}$$

skąd dostajemy

$$\begin{aligned}
f'(x) &= \sum_{k=0}^{n-1} \binom{n}{k} y(y+k)^{k-1} (n-k)(x+n-k)^{n-k-1} = \\
&= \sum_{k=0}^{n-1} (n-k) \binom{n}{n-k} y(y+k)^{k-1} (x+n-k)^{n-k-1} = \\
&= \sum_{k=0}^{n-1} n \binom{n-1}{n-k-1} y(y+k)^{k-1} (x+n-k)^{n-k-1} = \\
&= n \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} y(y+k)^{k-1} ((x+1) + (n-1) - k)^{(n-1)-k} = \\
&= n \cdot ((x+1) + y + (n-1))^{n-1} = \\
&= n \cdot (x+y+n)^{n-1} = \\
&= g'(x).
\end{aligned}$$

Następnie podstawiamy $x = -y - n$. Wówczas

$$\begin{aligned}
f(-y-n) &= \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (-y-n+n-k)^{n-k} = \\
&= \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (-y-k)^{n-k} = \\
&= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} y(y+k)^{k-1} (y+k)^{n-k} = \\
&= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} y(y+k)^{n-1} = \\
&= \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} y \sum_{j=0}^{n-1} \binom{n-1}{j} y^{n-1-j} k^j = \\
&= \sum_{k=0}^n \sum_{j=0}^{n-1} (-1)^{n-k} \binom{n}{k} \binom{n-1}{j} y^{n-j} k^j = \\
&= \sum_{j=0}^{n-1} \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} \binom{n-1}{j} y^{n-j} k^j = \\
&= \sum_{j=0}^{n-1} \binom{n-1}{j} y^{n-j} \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^j = \\
&= 0,
\end{aligned}$$

bo dla $j < n$ mamy

$$\sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^j = 0.$$

Jednocześnie

$$g(-y-n) = (-y-n+y+n)^n = 0.$$

Stąd wynika, że $f(x) = g(x)$ dla $x \in \mathbb{R}$, co kończy dowód równości 1.

$$(2) \quad \sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} = \left(\frac{1}{x} + \frac{1}{y}\right) \cdot (x+y+n)^{n-1}.$$

Z równości 1 dostajemy

$$\begin{aligned} (x+y+n)^n &= \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k} = \\ &= \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k-1} (x+n-k) = \\ &= \sum_{k=0}^n \binom{n}{k} xy(y+k)^{k-1} (x+n-k)^{n-k-1} + \sum_{k=0}^n \binom{n}{k} y(y+k)^{k-1} (x+n-k)^{n-k-1} (n-k) = \\ &= xy \sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} + \sum_{k=0}^{n-1} n \binom{n-1}{k} y(y+k)^{k-1} (x+n-k)^{n-k-1} = \\ &= xy \sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} + \\ &\quad + n \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} y(y+k)^{k-1} ((x+1) + (n-1) - k)^{(n-1)-k} = \\ &= xy \sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} + n((x+1) + y + (n-1))^{n-1} = \\ &= xy \sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} + n(x+y+n)^{n-1}. \end{aligned}$$

Stąd

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} &= \frac{1}{xy} \cdot ((x+y+n)^n - n(x+y+n)^{n-1}) = \\ &= \frac{1}{xy} \cdot (x+y+n)^{n-1} (x+y+n-n) = \\ &= \frac{x+y}{xy} \cdot (x+y+n)^{n-1} = \\ &= \left(\frac{1}{x} + \frac{1}{y}\right) \cdot (x+y+n)^{n-1}, \end{aligned}$$

co kończy dowód równości 2.

$$(3) \quad \sum_{k=1}^{n-1} \binom{n}{k} k^{k-1} (n-k)^{n-k-1} = 2(n-1)n^{n-2}.$$

Zauważmy najpierw, że

$$\sum_{k=0}^n \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} = \frac{1}{y} (x+n)^{n-1} + \sum_{k=1}^{n-1} \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} + \frac{1}{x} (y+n)^{n-1}.$$

Zatem z równości 2 dostajemy

$$\sum_{k=1}^{n-1} \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} = \left(\frac{1}{x} + \frac{1}{y}\right) \cdot (x+y+n)^{n-1} - \frac{1}{y} (x+n)^{n-1} - \frac{1}{x} (y+n)^{n-1},$$

czyli

$$\begin{aligned} \sum_{k=1}^{n-1} \binom{n}{k} (y+k)^{k-1} (x+n-k)^{n-k-1} &= \\ &= \frac{1}{x} \cdot ((x+y+n)^{n-1} - (y+n)^{n-1}) + \frac{1}{y} \cdot ((x+y+n)^{n-1} - (x+n)^{n-1}). \end{aligned}$$

Teraz przechodzimy do granicy przy $x \rightarrow 0$ i $y \rightarrow 0$:

$$\sum_{k=1}^{n-1} \binom{n}{k} k^{k-1} (n-k)^{n-k-1} = \lim_{x \rightarrow 0} \frac{(x+n)^{n-1} - n^{n-1}}{x} + \lim_{y \rightarrow 0} \frac{(y+n)^{n-1} - n^{n-1}}{y} = 2(n-1)n^{n-2},$$

co kończy dowód równości 3.

Różne dowody twierdzenia Cayleya.

Dowód 1. Niech T_n będzie liczbą drzew, których wierzchołki są ponumerowane liczbami od 1 do n . Wówczas

$$T_n = \sum_{k=1}^{n-1} k \binom{n-2}{k-1} T_k T_{n-k}.$$

Na dwa sposoby zliczamy pary (e, T) , gdzie e jest gałęzią drzewa T .

(1) Drzewo T możemy wybrać na T_n sposobów; jego krawędź na $n-1$ sposobów. Mamy zatem $(n-1)T_n$ par.

(2) Dla dowolnej liczby $k = 1, 2, \dots, n-1$ wybieramy k wierzchołków; dokładniej dobieramy $k-1$ wierzchołków do wierzchołka o numerze 1. Następnie te wierzchołki łączymy w jedno drzewo i pozostałe wierzchołki łączymy w drugie drzewo. Wreszcie prowadzimy dowolną krawędź z jednego drzewa do drugiego – to jest właśnie krawędź e łącząca oba drzewa w drzewo T . Dla danego k otrzymujemy w ten sposób

$$\binom{n-1}{k-1} \cdot T_k \cdot T_{n-k} \cdot k(n-k)$$

par (e, T) . Mamy zatem

$$(n-1)T_n = \sum_{k=1}^{n-1} \binom{n-1}{k-1} k(n-k) T_k T_{n-k}.$$

Stąd dostajemy

$$\begin{aligned} T_n &= \frac{1}{n-1} \cdot \sum_{k=1}^{n-1} \binom{n-1}{k-1} k(n-k) T_k T_{n-k} = \\ &= \frac{1}{n-1} \cdot \sum_{k=1}^{n-1} (n-k) \binom{n-1}{n-k} k T_k T_{n-k} = \\ &= \frac{1}{n-1} \cdot \sum_{k=1}^{n-1} (n-1) \binom{n-2}{n-k-1} k T_k T_{n-k} = \\ &= \sum_{k=1}^{n-1} k \binom{n-2}{k-1} T_k T_{n-k}. \end{aligned}$$

Podstawiając następnie $n - k$ w miejsce k (czyli sumując w drugą stronę), otrzymujemy

$$T_n = \sum_{k=1}^{n-1} (n-k) \binom{n-2}{n-k-1} T_k T_{n-k} = \sum_{k=1}^{n-1} (n-k) \binom{n-2}{k-1} T_k T_{n-k}.$$

Zatem

$$2T_n = \sum_{k=1}^{n-1} k \binom{n-2}{k-1} T_k T_{n-k} + \sum_{k=1}^{n-1} (n-k) \binom{n-2}{k-1} T_k T_{n-k} = n \cdot \sum_{k=1}^{n-1} \binom{n-2}{k-1} T_k T_{n-k},$$

czyli

$$T_n = \frac{n}{2} \cdot \sum_{k=1}^{n-1} \binom{n-2}{k-1} T_k T_{n-k}.$$

Zauważmy następnie, że

$$\binom{n}{k} = \binom{n}{n-k} = \frac{n}{n-k} \cdot \binom{n-1}{n-k-1} = \frac{n}{n-k} \cdot \binom{n-1}{k} = \frac{n(n-1)}{k(n-k)} \cdot \binom{n-2}{k-1}.$$

Zatem

$$T_n = \frac{n}{2} \cdot \sum_{k=1}^{n-1} \binom{n-2}{k-1} T_k T_{n-k} = \frac{n}{2} \cdot \sum_{k=1}^{n-1} \frac{k(n-k)}{n(n-1)} \binom{n}{k} T_k T_{n-k} = \frac{1}{2(n-1)} \cdot \sum_{k=1}^{n-1} k(n-k) \binom{n}{k} T_k T_{n-k}.$$

Teraz – przez indukcję – zakładamy, że $T_k = k^{k-2}$ dla $k < n$. Wówczas

$$\begin{aligned} T_n &= \frac{1}{2(n-1)} \cdot \sum_{k=1}^{n-1} k(n-k) \binom{n}{k} k^{k-2} (n-k)^{n-k-2} = \\ &= \frac{1}{2(n-1)} \cdot \sum_{k=1}^{n-1} \binom{n}{k} k^{k-1} (n-k)^{n-k-1} = (\text{z tożsamości Abela}) \\ &= \frac{1}{2(n-1)} \cdot 2(n-1)n^{n-2} = \\ &= n^{n-2}, \end{aligned}$$

co kończy dowód twierdzenia Cayleya.

Uwaga. Z twierdzenia Cayleya i tożsamości

$$T_n = \frac{1}{2(n-1)} \cdot \sum_{k=1}^{n-1} k(n-k) \binom{n}{k} T_k T_{n-k}$$

otrzymujemy natychmiast tożsamość Abela (3).

Dowód 2. Najpierw wyprowadzimy ważną tożsamość dotyczącą wykładniczej funkcji tworzącej dla liczb Cayleya. Definiujemy najpierw

$$T(x) = \sum_{n=1}^{\infty} \frac{T_n}{(n-1)!} x^n = \sum_{n=1}^{\infty} \frac{nT_n}{n!} x^n = \sum_{n=0}^{\infty} \frac{nT_n}{n!} x^n.$$

Wówczas

$$\frac{T(x)}{x} = \sum_{n=1}^{\infty} \frac{T_n}{(n-1)!} x^{n-1} = T_1 + \sum_{n=2}^{\infty} \frac{T_n}{(n-1)!} x^{n-1} = \sum_{n=0}^{\infty} \frac{T_{n+1}}{n!} x^n.$$

Następnie

$$T'(x) = \sum_{n=1}^{\infty} \frac{T_n}{(n-1)!} \cdot n x^{n-1} = \sum_{n=0}^{\infty} \frac{(n+1)T_{n+1}}{n!} x^n$$

oraz

$$\left(\frac{T(x)}{x}\right)' = \sum_{n=2}^{\infty} \frac{T_n}{(n-1)!} \cdot (n-1)x^{n-2} = \sum_{n=2}^{\infty} \frac{T_n}{(n-2)!} x^{n-2} = \sum_{n=0}^{\infty} \frac{T_{n+2}}{n!} x^n.$$

Zatem

$$\begin{aligned} T'(x) \cdot \frac{T(x)}{x} &= \sum_{n=0}^{\infty} \sum_{k=0}^n \frac{(k+1)T_{k+1}}{k!} x^k \cdot \frac{T_{n-k+1}}{(n-k)!} x^{n-k} = \\ &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^n \frac{(k+1)T_{k+1}T_{n-k+1}}{k!(n-k)!} \right) x^n = \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \cdot \left(\sum_{k=0}^n \frac{(k+1)T_{k+1}T_{n-k+1}n!}{k!(n-k)!} \right) x^n = \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \cdot \sum_{k=0}^n (k+1) \binom{n}{k} T_{k+1}T_{n-k+1} x^n = \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \cdot \sum_{k=1}^{n+1} k \binom{n}{k-1} T_k T_{n+2-k} x^n. \end{aligned}$$

Teraz korzystamy z udowodnionej tożsamości rekurencyjnej

$$T_n = \sum_{k=1}^{n-1} k \binom{n-2}{k-1} T_k T_{n-k}.$$

Podstawiając $n+2$ w miejsce n , otrzymujemy

$$T_{n+2} = \sum_{k=1}^{n+1} k \binom{n}{k-1} T_k T_{n+2-k}.$$

Zatem

$$T'(x) \cdot \frac{T(x)}{x} = \sum_{n=0}^{\infty} \frac{1}{n!} T_{n+2} x^n = \sum_{n=0}^{\infty} \frac{T_{n+2}}{n!} x^n = \left(\frac{T(x)}{x}\right)'.$$

Stąd wynika, że

$$\frac{\left(\frac{T(x)}{x}\right)'}{\left(\frac{T(x)}{x}\right)} = T'(x),$$

czyli

$$\left(\ln \frac{T(x)}{x}\right)' = T'(x).$$

Zatem

$$\ln \frac{T(x)}{x} = T(x) + C$$

dla pewnej stałej C . Stąd dostajemy

$$\frac{T(x)}{x} = e^{T(x)+C} = e^{T(x)} \cdot e^C = d \cdot e^{T(x)}.$$

Podstawiając $x = 0$, otrzymujemy $d = 1$. Zatem ostatecznie

$$\frac{T(x)}{x} = e^{T(x)},$$

czyli

$$x = T(x) \cdot e^{-T(x)}.$$

Przypomnienie z teorii funkcji analitycznych.

Niech funkcja $f(z)$ będzie funkcją analityczną w otoczeniu 0 i niech γ będzie krzywą zamkniętą obiegającą 0 dokładnie jeden raz. Wówczas

$$f^{(m)}(0) = \frac{m!}{2\pi i} \int_{\gamma} \frac{f(z)}{z^{m+1}} dz = \frac{(m-1)!}{2\pi i} \int_{\gamma} \frac{f'(z)}{z^m} dz.$$

Ponadto, jeśli $f'(0) \neq 0$, to $f(\gamma)$ też jest taką krzywą.

Mamy teraz

$$\begin{aligned} T_n &= \frac{1}{n} \cdot T^{(n)}(0) = \frac{1}{n} \cdot \frac{(n-1)!}{2\pi i} \int_{\gamma} \frac{T'(z)}{z^n} dz = \frac{(n-1)!}{2\pi i n} \int_{\gamma} \frac{T'(z)}{(T(z) \cdot e^{-T(z)})^n} dz = \\ &= \frac{(n-1)!}{2\pi i n} \int_{T(\gamma)} \frac{dw}{(w \cdot e^{-w})^n} = \frac{(n-1)!}{2\pi i n} \int_{\Gamma} \frac{e^{wn}}{w^n} dw, \end{aligned}$$

gdzie $\Gamma = T(\gamma)$.

Rozważmy funkcję

$$g(z) = e^{zn} = \sum_{k=0}^{\infty} \frac{(zn)^k}{k!} = \sum_{k=0}^{\infty} \frac{n^k}{k!} z^k.$$

Wówczas

$$g^{(n)}(0) = \frac{n!}{2\pi i} \int_{\Gamma} \frac{g(z)}{z^{n+1}} dz.$$

W szczególności

$$g^{(n-1)}(0) = \frac{(n-1)!}{2\pi i} \int_{\Gamma} \frac{g(z)}{z^n} dz = \frac{(n-1)!}{2\pi i} \int_{\Gamma} \frac{e^{wn}}{w^n} dw.$$

Zatem

$$T_n = \frac{1}{n} \cdot g^{(n-1)}(0) = \frac{1}{n} \cdot n^{n-1} = n^{n-2},$$

co kończy dowód twierdzenia Cayleya.

Autorem tego dowodu jest G. Polya (1937).

Dowód 3. Niech $d_1, \dots, d_n$ będą takimi liczbami całkowitymi dodatnimi, że

$$d_1 + \dots + d_n = 2n - 2.$$

Wtedy liczba drzew o wierzchołkach ponumerowanych liczbami od 1 do n i takich, że $\rho(i) = d_i$ dla $i = 1, \dots, n$, jest równa

$$\frac{(n-2)!}{(d_1-1)! \cdot \dots \cdot (d_n-1)!}.$$

Dowodzimy tego przez indukcję względem n . Dla $n = 1$ i $n = 2$ jest to oczywiste. Niech więc $n > 2$. Istnieje i takie, że $d_i = 1$. Niech np. $d_n = 1$. Usuwamy z drzewa wierzchołek o numerze n i krawędź łączącą go z wierzchołkiem o numerze np. j . Otrzymane drzewo ma wierzchołki stopni

$$d_1, d_2, \dots, d_{j-1}, d_j - 1, d_{j+1}, \dots, d_{n-1}.$$

Takich drzew jest (z założenia indukcyjnego)

$$\frac{(n-3)!}{(d_1-1)! \cdot \dots \cdot (d_{j-1}-1)! \cdot (d_j-2)! \cdot (d_{j+1}-1)! \cdot \dots \cdot (d_{n-1}-1)!},$$

czyli

$$\frac{(d_j-1)(n-3)!}{(d_1-1)! \cdot \dots \cdot (d_{n-1}-1)!}.$$

Zatem liczba wszystkich drzew o podanych stopniach wierzchołków jest równa

$$\begin{aligned} \sum_{j=1}^{n-1} \frac{(d_j-1)(n-3)!}{(d_1-1)! \cdot \dots \cdot (d_{n-1}-1)!} &= \frac{(n-3)!}{(d_1-1)! \cdot \dots \cdot (d_{n-1}-1)!} \cdot \sum_{j=1}^{n-1} (d_j-1) = \\ &= \frac{(n-3)!}{(d_1-1)! \cdot \dots \cdot (d_{n-1}-1)!} \cdot ((2n-3) - (n-1)) = \\ &= \frac{(n-2)!}{(d_1-1)! \cdot \dots \cdot (d_{n-1}-1)!} = \\ &= \frac{(n-2)!}{(d_1-1)! \cdot \dots \cdot (d_n-1)!}. \end{aligned}$$

Teraz skorzystamy z uogólnionego wzoru Newtona. Najpierw definiujemy tzw. **współczynniki wielomianowe** wzorem

$$\binom{n}{k_1, \dots, k_m} = \frac{n!}{k_1! \cdot \dots \cdot k_m!}$$

dla liczb nieujemnych $n, k_1, \dots, k_m$ takich, że $k_1 + \dots + k_m = n$. W szczególności, jeśli $k + l = n$, to

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

Wzór dwumianowy Newtona możemy zapisać w postaci

$$(a+b)^n = \sum_{\substack{k, l \geq 0 \\ k+l=n}} \binom{n}{k, l} a^k b^l.$$

Jego uogólnienie ma postać

$$(a_1 + \dots + a_m)^n = \sum_{\substack{k_1, \dots, k_m \geq 0 \\ k_1 + \dots + k_m = n}} \binom{n}{k_1, \dots, k_m} a_1^{k_1} \cdot \dots \cdot a_m^{k_m}.$$

Teraz liczba wszystkich drzew o wierzchołkach ponumerowanych liczbami od 1 do n jest równa

$$\begin{aligned} \sum_{\substack{d_1, \dots, d_n \geq 1 \\ d_1 + \dots + d_n = 2n-2}} \frac{(n-2)!}{(d_1-1)! \cdot \dots \cdot (d_n-1)!} &= \sum_{\substack{k_1, \dots, k_n \geq 0 \\ k_1 + \dots + k_n = n-2}} \frac{(n-2)!}{k_1! \cdot \dots \cdot k_n!} = \sum_{\substack{k_1, \dots, k_n \geq 0 \\ k_1 + \dots + k_n = n-2}} \binom{n-2}{k_1, \dots, k_n} = \\ &= \underbrace{(1 + \dots + 1)}_n^{n-2} = n^{n-2}. \end{aligned}$$

Dowód 4. Każdemu drzewu, którego wierzchołki są ponumerowane liczbami od 1 do n , przyporządkowujemy tzw. **kod Prüfera**, czyli ciąg $(a_1, \dots, a_{n-2})$ liczb ze zbioru $\{1, \dots, n\}$. Algorytm przyporządkowania jest następujący:

Niech n będzie liczbą wierzchołków drzewa;

niech P będzie pustym ciągiem liczb;

dopóki $n > 2$, powtarzaj

$v :=$ najmniejszy numer liścia (czyli wierzchołka stopnia 1);

$w :=$ numer wierzchołka sąsiadującego z v ;

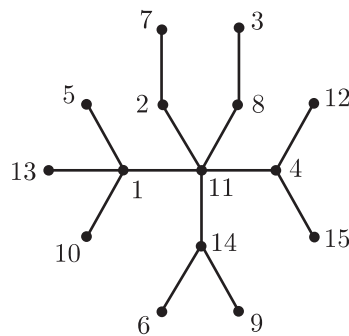
usuń z drzewa wierzchołek v i krawędź vw ;

dopisz w na końcu ciągu P ;

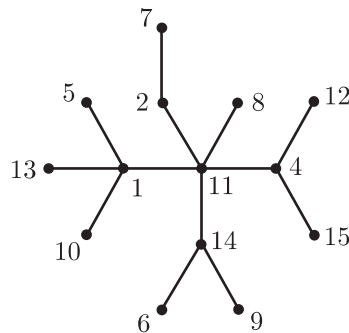
$n := n - 1$;

zwróć kod Prüfera P .

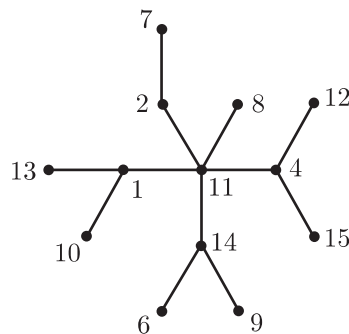
Obejrzyjmy teraz ciąg rysunków ilustrujący powstawanie kodu Prüfera dla następującego drzewa o 15 wierzchołkach.



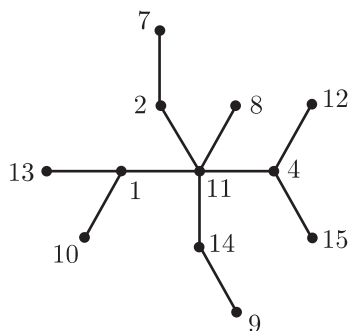
Na początku kodem P jest ciąg pusty. Najmniejszym numerem liścia jest 3; ten liść sąsiaduje z wierzchołkiem numer 8. Usuwamy z drzewa wierzchołek 3 i krawędź $3 - 8$. Na końcu kodu P dopisujemy 8, a więc teraz $P = (8)$. Oto nowe drzewo:



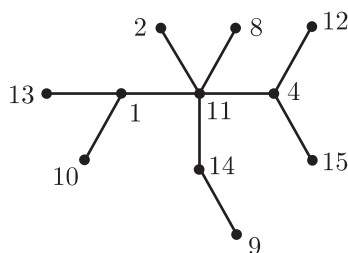
Teraz usuwamy krawędź $1 - 5$ i wydłużamy kod, dopisując 1 na końcu: $P = (8, 1)$. Nowe drzewo ma postać:



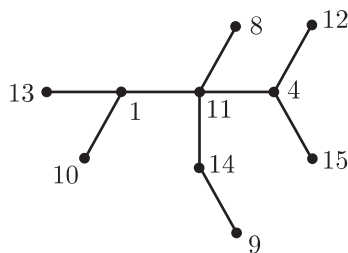
Następnie usuwamy krawędź $6 - 14$ i na końcu kodu dopisujemy 14: $P = (8, 1, 14)$. Otrzymujemy drzewo:



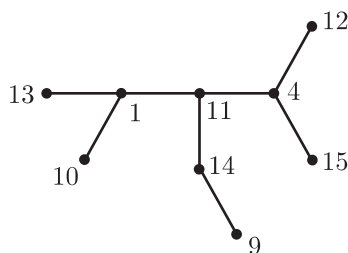
Usuwamy krawędź $2 - 7$ i dopisujemy 2: $P = (8, 1, 14, 2)$. Otrzymujemy drzewo:



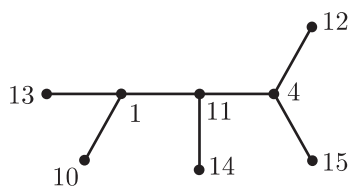
Usuwamy krawędź $2 - 11$ i dopisujemy 11: $P = (8, 1, 14, 2, 11)$. Otrzymujemy drzewo:



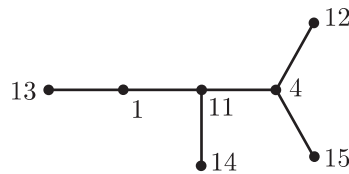
Usuwamy krawędź $8 - 11$ i dopisujemy 11: $P = (8, 1, 14, 2, 11, 11)$. Otrzymujemy drzewo:



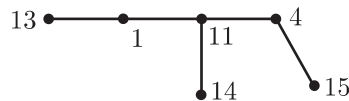
Usuwamy krawędź $9 - 14$ i dopisujemy 14: $P = (8, 1, 14, 2, 11, 11, 14)$. Otrzymujemy drzewo:



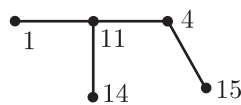
Usuujemy krawędź 1 – 10 i dopisujemy 1: $P = (8, 1, 14, 2, 11, 11, 14, 1)$. Otrzymujemy drzewo:



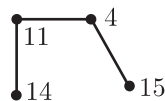
Usuujemy krawędź 4 – 12 i dopisujemy 4: $P = (8, 1, 14, 2, 11, 11, 14, 1, 4)$. Otrzymujemy drzewo:



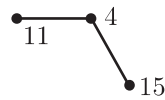
Usuujemy krawędź 1 – 13 i dopisujemy 1: $P = (8, 1, 14, 2, 11, 11, 14, 1, 4, 1)$. Otrzymujemy drzewo:



Usuujemy krawędź 1 – 11 i dopisujemy 11: $P = (8, 1, 14, 2, 11, 11, 14, 1, 4, 1, 11)$. Otrzymujemy drzewo:



Usuujemy krawędź 11 – 14 i dopisujemy 11: $P = (8, 1, 14, 2, 11, 11, 14, 1, 4, 1, 11, 11)$. Otrzymujemy drzewo:



Usuujemy krawędź 4 – 11 i dopisujemy 4: $P = (8, 1, 14, 2, 11, 11, 14, 1, 4, 1, 11, 11, 4)$. Otrzymujemy drzewo:



Ostatnie drzewo ma tylko dwa wierzchołki, więc kończymy algorytm. Otrzymany ciąg

$$P = (8, 1, 14, 2, 11, 11, 14, 1, 4, 1, 11, 11, 4)$$

jest kodem Prüfera naszego drzewa.

Zauważmy jeszcze, że jeśli drzewo ma tylko dwa wierzchołki, to algorytm od razu zwróci nam ciąg pusty jako jego kod Prüfera. Rzeczywiście, jest tylko jedno drzewo o dwóch wierzchołkach (wierzchołki o numerach 1 i 2 połączone krawędzią) i jego kodem jest ciąg pusty.

Powyższy algorytm pozwala utworzyć jednoznacznie kod Prüfera z dowolnego drzewa o wierzchołkach ponumerowanych liczbami od 1 do n . Okazuje się, że na odwrót: z każdego kodu Prüfera można jednoznacznie utworzyć drzewo. Co więcej, jeśli dla danego drzewa utworzymy kod Prüfera, a następnie z tego kodu utworzymy drzewo, to otrzymamy nasze wyjściowe drzewo. Nietrudny dowód tego faktu pozostawimy jako ćwiczenie.

A oto algorytm tworzenia drzewa o zadanym kodzie Prüfera P .

Niech P będzie ciągiem długości $n - 2$ liczb ze zbioru $\{1, \dots, n\}$;

$L := (1, \dots, n)$;

dopóki ciąg P jest niepusty, powtarzaj

$l :=$ najmniejsza liczba w ciągu L nie występująca w P ;

$p :=$ pierwszy wyraz ciągu P ;

utwórz krawędź lp ;

usuń l z ciągu L ;

usuń p z ciągu P ;

utwórz krawędź lp , gdzie l i p są ostatnimi dwiema liczbami w ciągu L .

Następujący ciąg rysunków ilustruje budowanie drzewa o 15 wierzchołkach, którego kodem Prüfera jest ciąg

$$(8, 1, 14, 2, 11, 11, 14, 1, 4, 1, 11, 11, 4).$$

Najpierw tworzymy dwa ciągi:

$$P = (8, 1, 14, 2, 11, 11, 14, 1, 4, 1, 11, 11, 4) \quad L = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15).$$

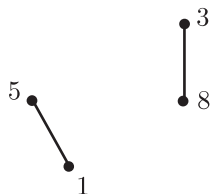
Najmniejszą liczbą w ciągu L , która nie występuje w ciągu P jest 3. Pierwszą liczbą w ciągu P jest 8. Tworzymy krawędź 3 – 8:



i usuwamy liczby 8 i 3 odpowiednio z ciągów P i L . Otrzymujemy ciągi

$$P = (1, 14, 2, 11, 11, 14, 1, 4, 1, 11, 11, 4) \quad L = (1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15).$$

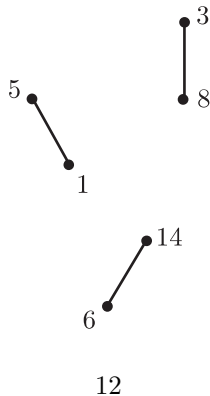
Z ciągu L usuwamy teraz liczbę 5, z ciągu P liczbę 1, tworząc krawędź 1 – 5:



Otrzymujemy ciągi

$$P = (14, 2, 11, 11, 14, 1, 4, 1, 11, 11, 4) \quad L = (1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15).$$

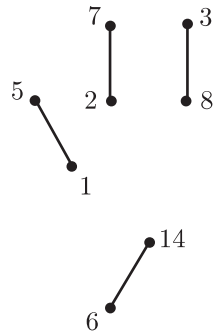
Z ciągu L usuwamy liczbę 6, z ciągu P liczbę 14, tworząc krawędź 6 – 14:



Otrzymujemy ciągi

$$P = (2, 11, 11, 14, 1, 4, 1, 11, 11, 4) \quad L = (1, 2, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15).$$

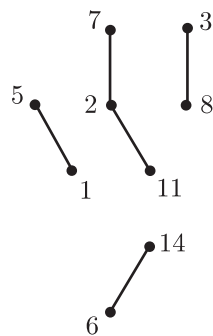
Z ciągu L usuwamy liczbę 7, z ciągu P liczbę 2, tworząc krawędź 2 – 7:



Otrzymujemy ciągi

$$P = (11, 11, 14, 1, 4, 1, 11, 11, 4) \quad L = (1, 2, 4, 8, 9, 10, 11, 12, 13, 14, 15).$$

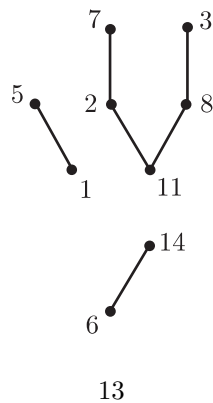
Z ciągu L usuwamy liczbę 2, z ciągu P liczbę 11, tworząc krawędź 2 – 11:



Otrzymujemy ciągi

$$P = (11, 14, 1, 4, 1, 11, 11, 4) \quad L = (1, 4, 8, 9, 10, 11, 12, 13, 14, 15).$$

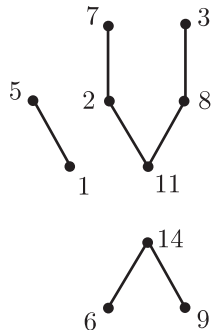
Z ciągu L usuwamy liczbę 8, z ciągu P liczbę 11, tworząc krawędź 8 – 11:



Otrzymujemy ciągi

$$P = (14, 1, 4, 1, 11, 11, 4) \quad L = (1, 4, 9, 10, 11, 12, 13, 14, 15).$$

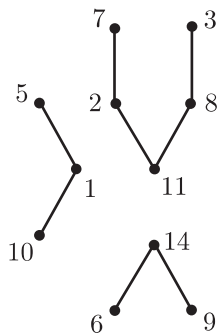
Z ciągu L usuwamy liczbę 9, z ciągu P liczbę 14, tworząc krawędź $9 - 14$:



Otrzymujemy ciągi

$$P = (1, 4, 1, 11, 11, 4) \quad L = (1, 4, 10, 11, 12, 13, 14, 15).$$

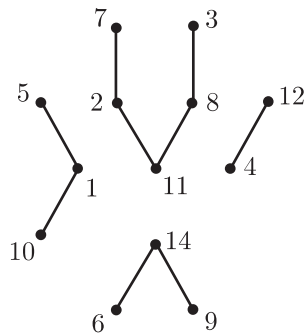
Z ciągu L usuwamy liczbę 10, z ciągu P liczbę 1, tworząc krawędź $1 - 10$:



Otrzymujemy ciągi

$$P = (4, 1, 11, 11, 4) \quad L = (1, 4, 11, 12, 13, 14, 15).$$

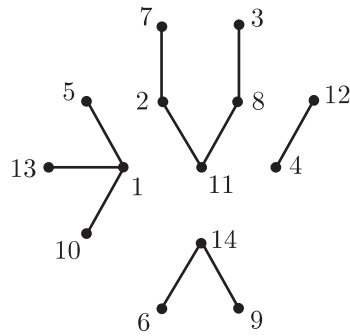
Z ciągu L usuwamy liczbę 12, z ciągu P liczbę 4, tworząc krawędź $4 - 12$:



Otrzymujemy ciągi

$$P = (1, 11, 11, 4) \quad L = (1, 4, 11, 13, 14, 15).$$

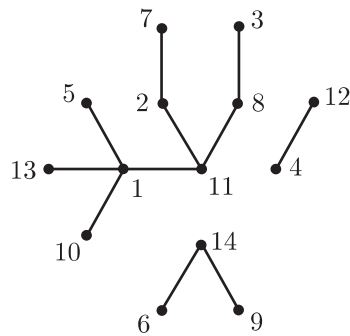
Z ciągu L usuwamy liczbę 13, z ciągu P liczbę 1, tworząc krawędź $1 - 13$:



Otrzymujemy ciągi

$$P = (11, 11, 4) \quad L = (1, 4, 11, 14, 15).$$

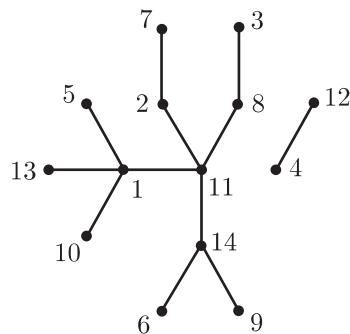
Z ciągu L usuwamy liczbę 1, z ciągu P liczbę 11, tworząc krawędź $1 - 11$:



Otrzymujemy ciągi

$$P = (11, 4) \quad L = (4, 11, 14, 15).$$

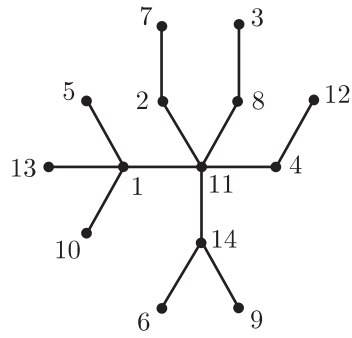
Z ciągu L usuwamy liczbę 14, z ciągu P liczbę 11, tworząc krawędź $11 - 14$:



Otrzymujemy ciągi

$$P = (4) \quad L = (4, 11, 15).$$

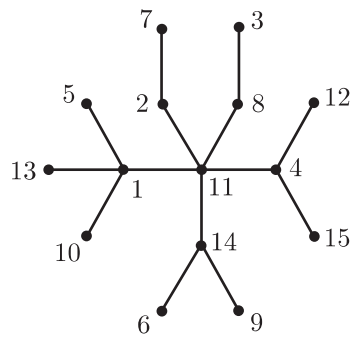
Z ciągu L usuwamy liczbę 11, z ciągu P liczbę 4, tworząc krawędź $4 - 11$:



Otrzymujemy ciągi

$$P = \emptyset \quad L = (4, 15).$$

W ciągu L pozostały dwie liczby: 4 i 15. Dołączamy do ostatniego drzewa krawędź 4 – 15, otrzymując drzewo, od którego rozpoczęliśmy naszą procedurę:



O algebrze w kombinatoryce.

W. Guzicki

(Czwartkowe wykłady popularne z matematyki – 21.04.2005)

W tym wykładzie pokażemy kilka zastosowań algebry do dowodów twierdzeń kombinatorycznych.

Jak zapewne pamiętamy ze szkoły, wielomianem stopnia n nazywamy funkcję postaci

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

gdzie $a_n, a_{n-1}, \dots, a_1, a_0$ są dowolnymi liczbami rzeczywistymi, przy czym $a_n \neq 0$. Te liczby nazywamy **współczynnikami** wielomianu f . Oczywiście współczynniki wielomianu wyznaczają go jednoznacznie. Okazuje się, że jest też i na odwrót: jeśli dwa wielomiany f i g przyjmują te same wartości dla wszystkich argumentów, to mają te same współczynniki (wynika to stąd, że wielomian niezerowy ma tylko skończoną liczbę pierwiastków). Zatem wielomian f jednoznacznie wyznacza swoje współczynniki. Inaczej mówiąc, wielomian f stopnia n możemy utożsamiać z takim ciągiem długości $n + 1$ jego współczynników:

$$(a_n, a_{n-1}, \dots, a_1, a_0),$$

w którym pierwszy wyraz jest różny od zera: $a_n \neq 0$. Okazuje się, że wygodnie jest przyjmować, iż ciąg współczynników jest nieskończony, przy czym wszystkie współczynniki o indeksach większych od n są zerami. Wygodnie też jest zapisywać te współczynniki w odwrotnej kolejności.

Od tej pory wielomian zmiennej rzeczywistej x utożsamiamy z ciągiem nieskończonym

$$f = (a_0, a_1, a_2, \dots, a_n, \dots)$$

liczb rzeczywistych, w którym prawie wszystkie (tzn. wszystkie od pewnego miejsca) wyrazy są równe zeru. Inaczej mówiąc z takim ciągiem, dla którego istnieje liczba naturalna n o tej własności, że

$$a_{n+1} = a_{n+2} = a_{n+3} = \dots = 0.$$

Oczywiście wielomian zerowy utożsamiamy z ciągiem, w którym wszystkie wyrazy są zerami. Wielomian stopnia n utożsamiamy z ciągiem takim, że

$$a_n \neq 0 \quad \text{oraz} \quad \forall m > n \quad (a_m = 0).$$

Po tym utożsamieniu możemy łatwo opisać działania na wielomianach. **Sumą** wielomianów

$$f = (a_0, a_1, a_2, \dots) \quad \text{i} \quad g = (b_0, b_1, b_2, \dots)$$

nazywamy wielomian

$$h = (c_0, c_1, c_2, \dots)$$

zdefiniowany następująco:

$$c_n = a_n + b_n \quad \text{dla } n = 0, 1, 2, \dots$$

Różnicą wielomianów f i g nazwiemy wielomian h zdefiniowany wzorem

$$c_n = a_n - b_n \quad \text{dla } n = 0, 1, 2, \dots$$

Iloczynem wielomianów f i g nazwiemy natomiast wielomian h zdefiniowany wzorem:

$$c_n = a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0 = \sum_{k=0}^n a_k b_{n-k} \quad \text{dla } n = 0, 1, 2, \dots$$

Wzór ten często nazywany wzorem Cauchy’ego. Początkowe współczynniki c_n przedstawiają się następująco:

$$\begin{aligned}c_0 &= a_0 b_0, \\c_1 &= a_0 b_1 + a_1 b_0, \\c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0, \\c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0, \\c_4 &= a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0, \\&\dots \quad \dots\end{aligned}$$

Przykład. Obliczmy iloczyn

$$(2x^2 - x + 3) \cdot (3x^2 + 2x - 1).$$

Po wykonaniu mnożenia sposobem „każdy wyraz przez każdy” i dokonaniu redukcji wyrazów podobnych, otrzymamy:

$$(2x^2 - x + 3) \cdot (3x^2 + 2x - 1) = 6x^4 + 4x^3 - 2x^2 - 3x^3 - 2x^2 + x + 9x^2 + 6x - 3 = 6x^4 + x^3 + 5x^2 + 7x - 3.$$

Wykonajmy teraz mnożenie za pomocą wzoru Cauchy’ego. Nasze wielomiany mają postać:

$$f = (3, -1, 2, 0, 0, 0, \dots) \quad \text{oraz} \quad g = (-1, 2, 3, 0, 0, 0, \dots)$$

Inaczej mówiąc

$$a_0 = 3, a_1 = -1, a_2 = 2, a_n = 0 \quad \text{dla } n > 2$$

oraz

$$b_0 = -1, b_1 = 2, b_2 = 3, b_n = 0 \quad \text{dla } n > 2.$$

Obliczamy kolejno współczynniki wielomianu h , będącego iloczynem wielomianów f i g :

$$\begin{aligned}c_0 &= a_0 b_0 = 3 \cdot (-1) = -3, \\c_1 &= a_0 b_1 + a_1 b_0 = 3 \cdot 2 + (-1) \cdot (-1) = 7, \\c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 = 3 \cdot 3 + (-1) \cdot 2 + 2 \cdot (-1) = 5, \\c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 3 \cdot 0 + (-1) \cdot 3 + 2 \cdot 2 + 0 \cdot (-1) = 1, \\c_4 &= a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 3 \cdot 0 + (-1) \cdot 0 + 2 \cdot 3 + 0 \cdot 2 + 0 \cdot (-1) = 6.\end{aligned}$$

Można łatwo zauważyć, że $c_n = 0$ dla $n > 4$. Zatem wielomian h ma postać

$$h = (-3, 7, 5, 1, 6, 0, 0, 0, \dots),$$

czyli

$$(2x^2 - x + 3) \cdot (3x^2 + 2x - 1) = 6x^4 + x^3 + 5x^2 + 7x - 3.$$

Przypomnimy teraz znane ze szkoły pojęcie współczynnika dwumianowego $\binom{n}{k}$. Niech A będzie dowolnym zbiorem n -elementowym. W dalszym ciągu, jeśli X jest dowolnym zbiorem skończonym, to symbolem $|X|$ będziemy oznaczać liczbę elementów zbioru X . Mamy wówczas:

$$\binom{n}{k} = |\{X \subseteq A : |X| = k\}|$$

dla dowolnych liczb naturalnych n i k . Natychmiast z definicji wynika, że jeśli $k > n$ to

$$\binom{n}{k} = 0,$$

gdyż wtedy zbiór A nie ma podzbiorów k -elementowych. Jeśli natomiast $0 \leq k \leq n$, to ze wzoru znanego ze szkoły wynika, że

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

Współczynniki dwumianowe występują w tzw. wzorze dwumianowym Newtona:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \dots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} a^0 b^n$$

dla dowolnych liczb rzeczywistych a i b i dowolnej liczby naturalnej dodatniej n . Współczynniki dwumianowe tworzą tzw. **trójkąt Pascala**, którego początkowe wiersze przedstawiają się w następujący sposób:

$$\begin{array}{cccccccccccccccc} & & & & & \binom{1}{0} & & & \binom{1}{1} & & & & & & & & \\ & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & & & & \\ & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & & & & & \\ & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & & & & & \\ \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & & & & & \\ \binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} & & & & \end{array}$$

czyli

$$\begin{array}{cccccccccccccccc} & & & & & 1 & & & 1 & & & & & & & & \\ & & & & 1 & & 2 & & 1 & & & & & & & & \\ & & 1 & & 3 & & 3 & & 1 & & & & & & & & \\ & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & \\ & 1 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & \\ & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & \end{array}$$

Po tym wstępie przejdziemy do dowodu następującej równości:

$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n},$$

czyli

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}.$$

Podstawmy we wzorze dwumianowym Newtona $a = 1$ i $b = x$. Otrzymamy wzór

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \dots + \binom{n}{n-1} x^{n-1} + \binom{n}{n} x^n.$$

Podnosimy obie strony do kwadratu:

$$(1+x)^{2n} = \left(\sum_{k=0}^n \binom{n}{k} x^k \right) \cdot \left(\sum_{k=0}^n \binom{n}{k} x^k \right).$$

Po lewej stronie równości mamy oczywiście wielomian stopnia $2n$. Po prawej stronie mamy iloczyn dwóch wielomianów n -tego stopnia, a więc jest to także wielomian stopnia $2n$. Porównajmy współczynniki stojące przy x^n w obu wielomianach. Ponieważ

$$(1+x)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} x^k = \binom{2n}{0} + \binom{2n}{1} x + \binom{2n}{2} x^2 + \dots + \binom{2n}{n} x^n + \dots + \binom{2n}{2n} x^{2n},$$

więc po lewej stronie przy x^n stoi współczynnik $\binom{2n}{n}$. Po prawej stronie mamy iloczyn wielomianów $f \cdot g$, gdzie

$$f = g = \left(\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}, 0, 0, 0, \dots \right).$$

Inaczej mówiąc

$$a_0 = b_0 = \binom{n}{0},$$

$$a_1 = b_1 = \binom{n}{1},$$

$$a_2 = b_2 = \binom{n}{2},$$

$$\dots \quad \dots \quad \dots$$

$$a_n = b_n = \binom{n}{n},$$

$$a_m = b_m = 0 \quad \text{dla } m > n.$$

Możemy też napisać po prostu, że

$$a_m = b_m = \binom{n}{m}$$

dla każdej liczby naturalnej m (gdyż $\binom{n}{m} = 0$ dla $m > n$). Zgodnie ze wzorem Cauchy'ego mamy zatem

$$h = (c_0, c_1, c_2, \dots),$$

gdzie

$$c_m = a_0 b_m + a_1 b_{m-1} + \dots + a_{m-1} b_1 + a_m b_0 = \sum_{k=0}^m a_k b_{m-k}$$

dla $m = 0, 1, 2, \dots$. Po podstawieniu otrzymamy

$$c_n = \binom{n}{0} \binom{n}{n} + \binom{n}{1} \binom{n}{n-1} + \dots + \binom{n}{n-1} \binom{n}{1} + \binom{n}{n} \binom{n}{0} = \sum_{k=0}^n \binom{n}{k} \binom{n}{n-k}.$$

Ponieważ

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

więc ostatecznie otrzymujemy

$$c_n = \sum_{k=0}^n \binom{n}{k} \binom{n}{n-k} = \sum_{k=0}^n \binom{n}{k}^2.$$

Porównując obliczone współczynniki stojące w obu wielomianach przy x^n otrzymamy dowodzoną równość.

W dowodzie następnego wzoru skorzystamy ze wzoru dwumianowego Newtona i z podstawowych własności liczb zespolonych. Przypomnijmy krótko te własności.

Liczbą zespoloną nazywamy liczbę postaci $a + bi$, gdzie i jest tzw. **jednostką urojoną**, tzn. liczbą o tej własności, że $i^2 = -1$. Każda liczba rzeczywista jest liczbą zespoloną:

$$a = a + 0i$$

dla $a \in \mathbb{R}$. Działania na liczbach zespolonych wykonujemy w następujący sposób:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi) - (c + di) = (a - c) + (b - d)i,$$

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i,$$

dla dowolnych liczb zespolonych $a + bi$ oraz $c + di$. Jeśli ponadto $c + di \neq 0$, to

$$\frac{a + bi}{c + di} = \frac{a + bi}{c + di} \cdot \frac{c - di}{c - di} = \frac{(a + bi) \cdot (c - di)}{(c + di) \cdot (c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 - (di)^2} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i.$$

Liczby zespolone wykorzystamy do rozwiązywania równań kwadratowych. Przypuśćmy, że dane jest równanie kwadratowe

$$ax^2 + bx + c = 0,$$

w którym współczynniki są liczbami rzeczywistymi oraz wyróżnik Δ jest ujemny:

$$\Delta = b^2 - 4ac < 0.$$

Wtedy równanie ma dwa pierwiastki zespolone:

$$x_1 = \frac{-b - \sqrt{-\Delta} \cdot i}{2a} \quad \text{oraz} \quad x_2 = \frac{-b + \sqrt{-\Delta} \cdot i}{2a}$$

czyli

$$x_1 = \frac{-b}{2a} + \frac{-\sqrt{-\Delta}}{2a} \cdot i \quad \text{oraz} \quad x_2 = \frac{-b}{2a} + \frac{\sqrt{-\Delta}}{2a} \cdot i.$$

W zbiorze liczb zespolonych prawdziwe są znane ze szkoły wzory skróconego mnożenia, w szczególności przypomniany wcześniej wzór dwumianowy Newtona.

Udowodnimy teraz równość

$$\sum_{k=0}^n \binom{3n}{3k} = \frac{8^n + 2 \cdot (-1)^n}{3}.$$

Przykłady. Dla $n = 1$ dostajemy równość

$$\binom{3}{0} + \binom{3}{3} = 1 + 1 = 2 = \frac{8^1 + 2 \cdot (-1)^1}{3} = \frac{8 - 2}{3} = \frac{6}{3}.$$

Dla $n = 2$ mamy:

$$\binom{6}{0} + \binom{6}{3} + \binom{6}{6} = 1 + 20 + 1 = 22 = \frac{8^2 + 2 \cdot (-1)^2}{3} = \frac{64 + 2}{3} = \frac{66}{3}.$$

Wreszcie dla $n = 3$ otrzymujemy

$$\binom{9}{0} + \binom{9}{3} + \binom{9}{6} + \binom{9}{9} = 1 + 84 + 84 + 1 = 170 = \frac{8^3 + 2 \cdot (-1)^3}{3} = \frac{512 - 2}{3} = \frac{510}{3}.$$

Dowód równości rozpoczniemy od rozwiązania równania

$$x^3 = 1$$

w zbiorze liczb zespolonych. Przekształcamy najpierw to równanie:

$$\begin{aligned} x^3 - 1 &= 0, \\ (x - 1)(x^2 + x + 1) &= 0. \end{aligned}$$

Jednym pierwiastkiem jest oczywiście $x_1 = 1$. Dwa następne pierwiastki otrzymamy rozwiązując równanie kwadratowe

$$x^2 + x + 1 = 0.$$

Ponieważ $\Delta = -3$, więc otrzymujemy pierwiastki zespolone

$$x_2 = \frac{-1 - \sqrt{3} \cdot i}{2} \quad \text{oraz} \quad x_3 = \frac{-1 + \sqrt{3} \cdot i}{2}.$$

Pierwiastki te nazywamy zespolonymi pierwiastkami trzeciego stopnia z jedności. Niech ε będzie którymkolwiek z pierwiastków x_2 lub x_3 . Wtedy oczywiście

$$\varepsilon^3 = 1.$$

Ponadto ε jest pierwiastkiem równania kwadratowego $x^2 + x + 1 = 0$, więc

$$\varepsilon^2 + \varepsilon + 1 = 0.$$

Stąd wynika, że

$$1 + \varepsilon = -\varepsilon^2 \quad \text{oraz} \quad 1 + \varepsilon^2 = -\varepsilon.$$

Obliczmy teraz dwoma sposobami sumę

$$(1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n}.$$

Najpierw skorzystamy ze wzoru dwumianowego Newtona:

$$\begin{aligned} (1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n} &= \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0)^k + \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^1)^k + \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^2)^k = \\ &= \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{0 \cdot k} + \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{1 \cdot k} + \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{2 \cdot k} = \\ &= \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0 + \varepsilon^k + \varepsilon^{2k}) = \\ &= \sum_{k=0}^{3n} \binom{3n}{k} (1 + \varepsilon^k + \varepsilon^{2k}). \end{aligned}$$

Popatrzmy teraz, jak wyglądają sumy

$$1 + \varepsilon^k + \varepsilon^{2k}$$

dla różnych k . Oczywiście dla liczb k podzielnych przez 3 dodajemy do siebie trzy jedynki. Zatem suma jest równa 3. Niech teraz $k = 3l + 1$. Wtedy

$$1 + \varepsilon^k + \varepsilon^{2k} = 1 + \varepsilon^{3l} \cdot \varepsilon + \varepsilon^{6l} \cdot \varepsilon^2 = 1 + \varepsilon + \varepsilon^2 = 0.$$

Podobnie dla $k = 3l + 2$ stwierdzimy, że ta suma równa jest 0. Zatem, kontynuując przerwane obliczenia, dostajemy

$$\sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0 + \varepsilon^k + \varepsilon^{2k}) = \sum_{k=0}^n 3 \binom{3n}{3k} = 3 \cdot \sum_{k=0}^n \binom{3n}{3k}.$$

Następnie obliczymy tę samą sumę bez odwoływania się do wzoru Newtona. Mamy wtedy:

$$\begin{aligned}
 (1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n} &= (1 + 1)^{3n} + (1 + \varepsilon)^{3n} + (1 + \varepsilon^2)^{3n} = \\
 &= 2^{3n} + (-\varepsilon^2)^{3n} + (-\varepsilon)^{3n} = \\
 &= 2^{3n} + (-1)^{3n} \varepsilon^{6n} + (-1)^{3n} \varepsilon^{3n} = \\
 &= 2^{3n} + (-1)^n (\varepsilon^3)^{2n} + (-1)^n (\varepsilon^3)^n = \\
 &= 2^{3n} + (-1)^n + (-1)^n = \\
 &= 2^{3n} + 2 \cdot (-1)^n.
 \end{aligned}$$

W tym dowodzie korzystaliśmy z oczywistej równości:

$$(-1)^{3n} = (-1)^n$$

oraz ze wspomnianych wyżej równości

$$1 + \varepsilon = -\varepsilon^2 \quad \text{oraz} \quad 1 + \varepsilon^2 = -\varepsilon.$$

Porównując wyniki obu obliczeń, otrzymamy:

$$3 \cdot \sum_{k=0}^n \binom{3n}{3k} = 8^n + 2 \cdot (-1)^n,$$

czyli ostatecznie

$$\sum_{k=0}^n \binom{3n}{3k} = \frac{8^n + 2 \cdot (-1)^n}{3}.$$

Dowody niealgebraiczne.

Pokażemy teraz dowody niealgebraiczne obu udowodnionych wyżej równości. Najpierw dowodzimy równości

$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}.$$

Pokażemy tzw. *dowód kombinatoryczny*, polegający na tym, że dwoma sposobami policzymy elementy tego samego zbioru. Niech M i K będą dwoma rozłącznymi zbiorami n elementowymi. Wtedy oczywiście zbiór $M \cup K$ ma $2n$ elementów. Policzymy elementy następującego zbioru A :

$$A = \{X \subseteq M \cup K : |X| = n\}.$$

Z jednej strony, zbiór A ma $\binom{2n}{n}$ elementów,

$$|A| = \binom{2n}{n},$$

co wynika bezpośrednio z definicji współczynnika dwumianowego: zliczamy przecież n -elementowe podzbiory zbioru $2n$ -elementowego. Z drugiej strony, zbiór A jest sumą zbiorów rozłącznych

$$A = A_0 \cup A_1 \cup \dots \cup A_n,$$

gdzie

$$A_k = \{X \in A : |X \cap K| = k\}$$

dla $k = 0, 1, \dots, n$. Stąd wynika, że

$$|A| = |A_0| + |A_1| + \dots + |A_n| = \sum_{k=0}^n |A_k|.$$

Policzymy teraz elementy dowolnego zbioru A_k . Zbiór $X \in A_k$ możemy utworzyć wybierając k elementów ze zbioru K oraz $n - k$ elementów ze zbioru M . Inaczej mówiąc, możemy wybrać k elementów ze zbioru K i odrzucić k elementów ze zbioru M . Stąd wynika, że

$$|A_k| = \binom{n}{k} \cdot \binom{n}{n-k} = \binom{n}{k} \cdot \binom{n}{k} = \binom{n}{k}^2.$$

Zatem

$$|A| = \sum_{k=0}^n \binom{n}{k}^2,$$

co kończy dowód.

Ten dowód kombinatoryczny ma następującą interpretację. Dany jest zbiór $2n$ osób: n kobiet (zbiór K) i n mężczyzn (zbiór M). Pytamy, na ile sposobów można z tego zbioru wybrać delegację składającą się z n osób. Z jednej strony, wybieramy n osób spośród $2n$ osób – oczywiście na $\binom{2n}{n}$ sposobów. Z drugiej strony, najpierw ustalamy liczbę kobiet ($k = 0, 1, \dots, n$), potem wybieramy k kobiet i wreszcie odrzucamy k mężczyzn. Możemy to zrobić na $\binom{n}{k}^2$ sposobów i po dodaniu tych liczb dla wszystkich k otrzymujemy liczbę

$$\sum_{k=0}^n \binom{n}{k}^2$$

jaką łączną liczbę sposobów wyboru.

Teraz udowodnimy równość

$$\sum_{k=0}^n \binom{3n}{3k} = \frac{8^n + 2 \cdot (-1)^n}{3}.$$

Tym razem ułożymy tzw. *zależność rekurencyjną*. Przypuśćmy, że mamy dany zbiór $3n$ -elementowy A . Podzbiór B zbioru A nazwiemy podzbiorem **dobrym**, jeśli liczba jego elementów jest podzielna przez 3. W przeciwnym przypadku podzbiór B nazwiemy podzbiorem **złym**. Niech a_n będzie liczbą wszystkich dobrych podzbiorów zbioru $3n$ -elementowego. Mamy pokazać, że

$$a_n = \frac{8^n + 2 \cdot (-1)^n}{3}$$

dla $n = 1, 2, \dots$

Oczywiście $a_1 = 2$, gdyż zbiór trzejelementowy A ma dwa podzbiory dobre: zbiór pusty $\emptyset$ i cały zbiór A .

Znajdziemy teraz zależność a_{n+1} od a_n . Niech A będzie zbiorem $3n$ -elementowym i niech $a, b, c \notin A$, przy czym $a \neq b$, $a \neq c$ oraz $b \neq c$. Zbiór A ma a_n podzbiorów dobrych i $2^{3n} - a_n$ podzbiorów złych. Chcemy policzyć, ile podzbiorów dobrych ma zbiór $A \cup \{a, b, c\}$.

Dla każdego podzbioru B zbioru A policzymy, ile jest podzbiorów dobrych zbioru $A \cup \{a, b, c\}$ zawierających zbiór B . Jeśli zbiór B jest podzbiorem dobrym, to istnieją 2 dobre podzbiory zbioru $A \cup \{a, b, c\}$ zawierające B : sam zbiór B oraz zbiór $B \cup \{a, b, c\}$. Jeśli zbiór B jest podzbiorem złym, to istnieją 3 podzbiory dobre zbioru $A \cup \{a, b, c\}$ zawierające B . Mianowicie, jeśli liczba elementów zbioru B daje resztę 1 przy dzieleniu przez 3, to tymi podzbiarami dobrymi są:

$$B \cup \{a, b\}, \quad B \cup \{a, c\} \quad \text{oraz} \quad B \cup \{b, c\}.$$

Jeśli zaś liczba elementów zbioru B daje resztę 2 przy dzieleniu przez 3, to tymi podzbiorami dobrymi są:

$$B \cup \{a\}, \quad B \cup \{b\} \quad \text{oraz} \quad B \cup \{c\}.$$

Stąd wynika, że

$$a_{n+1} = 2 \cdot a_n + 3 \cdot (2^{3n} - a_n) = 3 \cdot 8^n - a_n.$$

Ciąg (a_n) spełnia zatem następującą zależność rekurencyjną:

$$\begin{cases} a_1 = 2, \\ a_{n+1} = 3 \cdot 8^n - a_n. \end{cases}$$

Możemy teraz udowodnić przez indukcję, że

$$a_n = \frac{8^n + 2 \cdot (-1)^n}{3}$$

dla $n = 1, 2, \dots$

1. Sprawdzamy warunek początkowy (dla $n = 1$). Mianowicie $a_1 = 2$ oraz

$$\frac{8^1 + 2 \cdot (-1)^1}{3} = \frac{8 - 2}{3} = 2.$$

2. Krok indukcyjny.

Zakładamy, że dla pewnej liczby naturalnej n zachodzi równość

$$a_n = \frac{8^n + 2 \cdot (-1)^n}{3}$$

i dowodzimy, że zachodzi też wtedy równość

$$a_{n+1} = \frac{8^{n+1} + 2 \cdot (-1)^{n+1}}{3}.$$

Otóż

$$\begin{aligned} a_{n+1} &= 3 \cdot 8^n - a_n = 3 \cdot 8^n - \frac{8^n + 2 \cdot (-1)^n}{3} = \frac{9 \cdot 8^n - 8^n - 2 \cdot (-1)^n}{3} = \frac{8 \cdot 8^n + 2 \cdot (-1)^{n+1}}{3} = \\ &= \frac{8^{n+1} + 2 \cdot (-1)^{n+1}}{3}, \end{aligned}$$

co kończy dowód indukcyjny.

Pokażemy jeszcze, w jaki sposób z otrzymanej zależności rekurencyjnej można wyprowadzić wzór ogólny. Definiujemy ciąg (b_n) wzorem

$$b_n = (-1)^n \cdot a_n$$

dla $n = 1, 2, \dots$. Mamy wówczas

$$\begin{aligned} b_{n+1} &= (-1)^{n+1} \cdot a_{n+1} = (-1)^{n+1} \cdot (3 \cdot 8^n - a_n) = 3 \cdot (-1)^{n+1} \cdot 8^n - (-1)^{n+1} \cdot a_n = \\ &= 3 \cdot (-1)^{n+1} \cdot 8^n + (-1)^n \cdot a_n = b_n + 3 \cdot (-1)^{n+1} \cdot 8^n. \end{aligned}$$

Zatem

$$\begin{aligned}
b_n &= b_{n-1} + 3 \cdot (-1)^n \cdot 8^{n-1}, \\
b_{n-1} &= b_{n-2} + 3 \cdot (-1)^{n-1} \cdot 8^{n-2}, \\
b_{n-2} &= b_{n-3} + 3 \cdot (-1)^{n-2} \cdot 8^{n-3}, \\
&\dots \quad \dots \\
b_4 &= b_3 + 3 \cdot (-1)^4 \cdot 8^3, \\
b_3 &= b_2 + 3 \cdot (-1)^3 \cdot 8^2, \\
b_2 &= b_1 + 3 \cdot (-1)^2 \cdot 8^1.
\end{aligned}$$

Po dodaniu stronami tych równości i zredukowaniu wyrazów $b_2, b_3, \dots, b_{n-1}$ występujących po obu stronach równości, dostaniemy

$$\begin{aligned}
b_n &= b_1 + 3 \cdot ((-1)^2 \cdot 8^1 + (-1)^3 \cdot 8^2 + \dots + (-1)^{n-1} \cdot 8^{n-2} + (-1)^n \cdot 8^{n-1}) = \\
&= b_1 - 3 \cdot ((-8)^1 + (-8)^2 + \dots + (-8)^{n-2} + (-8)^{n-1}) = \\
&= b_1 + 24 \cdot (1 + (-8)^1 + \dots + (-8)^{n-3} + (-8)^{n-2}) = \\
&= (-1)^1 \cdot a_1 + 24 \cdot \frac{1 - (-8)^{n-1}}{1 - (-8)} = \\
&= -2 + 24 \cdot \frac{1 - (-8)^{n-1}}{9} = \\
&= -2 + 8 \cdot \frac{1 - (-8)^{n-1}}{3} = \\
&= \frac{-6 + 8 - 8 \cdot (-1)^{n-1} \cdot 8^{n-1}}{3} = \\
&= \frac{2 + (-1)^n \cdot 8^n}{3}.
\end{aligned}$$

Stąd wynika, że

$$\begin{aligned}
(-1)^n \cdot a_n &= \frac{2 + (-1)^n \cdot 8^n}{3}, \\
(-1)^{2n} \cdot a_n &= \frac{2 \cdot (-1)^n + (-1)^{2n} \cdot 8^n}{3}, \\
a_n &= \frac{8^n + 2 \cdot (-1)^n}{3},
\end{aligned}$$

co kończy dowód.

Systemy trójek Steinera.

Na początku popatrzymy na przykład.

Przykład. (V. Bryant, *Aspekty kombinatoryki*, str. 199.) Dziewięć gatunków kawy ma zostać rozdanych do testowania różnym rodzinom. Nie jest wskazane, by każda rodzina porównywała wszystkie dziewięć gatunków (po około czwartej próbie wszystkie one smakują tak samo!). Tak więc każda z dwunastu rodzin otrzyma do porównania trzy gatunki. Podać taką konfigurację eksperymentu, w której każda para gatunków (spośród dziewięciu) jest porównywana w jednej rodzinie.

Rozwiązanie. Niech rodzaje kawy będą ponumerowane liczbami od 1 do 9. Rozdajmy dwunastu rodzinom do porównania następujące zestawy trzech gatunków:

$$\begin{aligned}
&\{1, 2, 3\}, \quad \{4, 5, 6\}, \quad \{7, 8, 9\}, \\
&\{1, 4, 7\}, \quad \{2, 5, 8\}, \quad \{3, 6, 9\}, \\
&\{1, 5, 9\}, \quad \{2, 6, 7\}, \quad \{3, 4, 8\}, \\
&\{1, 6, 8\}, \quad \{2, 4, 9\}, \quad \{3, 5, 7\}.
\end{aligned}$$

Wówczas każda para liczb od 1 do 9 znajduje się w jednym z tych zbiorów.

Systemem trójek Steinera nazywamy parę zbiorów (S, T) o następujących własnościach:

- (1) zbiory S i T są skończone,
- (2) elementami zbioru T są 3-elementowe podzbiory zbioru S :

$$X \in T \Rightarrow X \subseteq S \wedge |X| = 3,$$

- (3) każda para elementów zbioru S występuje w dokładnie jednym zbiorze należącym do T :

$$a, b \in S \wedge a \neq b \Rightarrow \text{istnieje dokładnie jeden zbiór } X \in T \text{ taki, że } a, b \in X.$$

Elementy zbioru S nazywamy często **punktami**, a zbiory należące do T nazywamy **trójkami** punktów. Warunek (3) możemy zatem wysłować w taki sposób, że każde dwa punkty ze zbioru S należą do dokładnie jednej trójki ze zbioru T .

Zbiór trójek w powyższym przykładzie ma jeszcze jedną interesującą własność. Mianowicie w każdym wierszu występują wszystkie punkty (czyli liczby od 1 do 9). Zatem zbiór T trójek punktów można podzielić na 4 rozłączne zbiory o tej własności, że elementy trójek z każdego z tych zbiorów wyczerpują cały zbiór punktów.

Warstwą nazwiemy taki zbiór trójek parami rozłącznych, którego sumą jest cały zbiór S . **Systemem trójek Kirkmana** nazywamy taki system trójek Steinera, w którym zbiór trójek T można podzielić na parami rozłączne warstwy. System trójek Steinera pokazany w powyższym przykładzie jest zatem systemem trójek Kirkmana.

Przykłady.

1. Niech $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Niech następnie zbiór T będzie zbiorem trójek z poprzedniego przykładu:

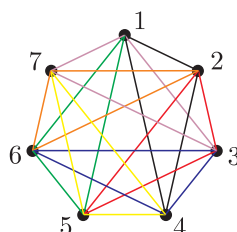
$$T = \left\{ \begin{array}{l} \{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \\ \{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\} \end{array} \right\}.$$

Wtedy para (S, T) jest systemem trójek Steinera. Widzieliśmy już, że jest to także system trójek Kirkmana.

2. Niech $S = \{1, 2, 3, 4, 5, 6, 7\}$ i niech T będzie następującym zbiorem trójek:

$$T = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}\}.$$

Wtedy para (S, T) jest systemem trójek Steinera. Ten system trójek Steinera ma ładną interpretację graficzną:



3. Niech $S = \{1, 2, \dots, 15\}$ i niech T będzie zbiorem następujących trójek liczb:

$$\begin{array}{cccccc} \{1, 2, 3\}, & \{4, 8, 12\}, & \{5, 10, 14\}, & \{6, 11, 13\}, & \{7, 9, 15\}, \\ \{1, 4, 5\}, & \{2, 8, 10\}, & \{3, 13, 15\}, & \{6, 9, 14\}, & \{7, 11, 12\}, \\ \{1, 6, 7\}, & \{2, 9, 11\}, & \{3, 12, 14\}, & \{4, 10, 15\}, & \{5, 8, 13\}, \\ \{1, 8, 9\}, & \{2, 12, 15\}, & \{3, 5, 6\}, & \{4, 11, 14\}, & \{7, 10, 13\}, \\ \{1, 10, 11\}, & \{2, 13, 14\}, & \{3, 4, 7\}, & \{5, 9, 12\}, & \{6, 8, 15\}, \\ \{1, 12, 13\}, & \{2, 4, 6\}, & \{3, 9, 10\}, & \{5, 11, 15\}, & \{7, 8, 14\}, \\ \{1, 14, 15\}, & \{2, 5, 7\}, & \{3, 8, 11\}, & \{4, 9, 13\}, & \{6, 10, 12\}. \end{array}$$

Wtedy para (S, T) jest systemem trójek Steiner. Zauważmy, że ten system jest również systemem trójek Kirkmana (warstwami są wiersze powyższej tablicy). Ten system stanowi rozwiązanie następującego zadania postawionego i rozwiązanego przez Kirkmana:

Czy możliwe jest, aby 15 uczennic wychodziło na spacer przez 7 dni tygodnia w taki sposób, by codziennie spacerowały w 5 rzędach po 3 uczennice w każdym rzędzie oraz, by każda para uczennic spacerowała w tym samym rzędzie dokładnie jednego dnia?

Wiersze powyższej tablicy ilustrują sposób ustawienia uczennic przez kolejne dni tygodnia, od poniedziałku do niedzieli.

Twierdzenie. Jeśli istnieje system trójek Steiner (S, T) , w którym $|S| = n$, to liczba n przy dzieleniu przez 6 daje resztę 1 lub 3.

Dowód. Dwoma sposobami zliczamy pary punktów. Z jednej strony, liczba par jest równa $\binom{n}{2}$. Z drugiej strony, każda para należy do dokładnie jednej trójki ze zbioru T . Ponieważ w każdej trójce są dokładnie 3 pary, więc

$$3 \cdot |T| = \binom{n}{2} = \frac{n(n-1)}{2},$$

czyli

$$|T| = \frac{n(n-1)}{6}.$$

Natępnie bierzemy dowolny element x zbioru S i rozważamy zbiór

$$U = \{t \in T : x \in t\}.$$

Zauważmy, że rodzina par

$$\{t \setminus \{x\} : t \in U\}$$

jest podziałem zbioru $S \setminus \{x\}$ na zbiory dwuelementowe. Stąd wynika, że liczba n jest nieparzysta. Zatem n przy dzieleniu przez 6 może dać jedną z reszt 1, 3 lub 5. Ponieważ liczba $n(n-1)$ jest podzielna przez 6, więc n nie może dawać reszty 5 przy dzieleniu przez 6, co kończy dowód twierdzenia.

Wniosek. Jeśli istnieje system trójek Kirkmana (S, T) , w którym $|S| = n$, to liczba n daje resztę 3 przy dzieleniu przez 6.

Dowód. Ponieważ jedna warstwa daje podział zbioru S na zbiory trzelementowe, więc liczba n dzieli się przez 3. Nie może zatem dawać reszty 1 przy dzieleniu przez 6.

Prawdziwe jest też twierdzenie odwrotne: jeśli liczba naturalna $n \geq 3$ daje resztę 1 lub 3 przy dzieleniu przez 6, to istnieje system trójek Steiner (S, T) , w którym $|S| = n$. Pokażemy teraz sposób konstrukcji systemu trójek Steiner (S, T) , w którym $|S| = 6m+3$. Do tego wprowadzimy kilka pojęć algebraicznych.

Niech Q będzie zbiorem skończonym, w którym jest określone działanie dwuargumentowe $\circ$. Mówimy, że zbiór Q (z działaniem $\circ$) jest **quasigrupą przemenną**, jeśli spełnione są następujące warunki:

(1) $a \circ b = b \circ a$ dla dowolnych $a, b \in Q$,

(2) dla dowolnych $a, c \in Q$ istnieje dokładnie jeden element b zbioru Q taki, że $a \circ b = c$.

Warunek (2) jest równoważny następującemu warunkowi (2'):

(2') dla dowolnego $a \in Q$ funkcja $f : Q \rightarrow Q$ określona wzorem $f(x) = a \circ x$ jest różnowartościowa

Mówimy następnie, że quasigrupa Q jest **idempotentna**, jeśli ponadto jest spełniony warunek

(3) $a \circ a = a$ dla dowolnego $a \in Q$.

Przykłady.

1. Zbiór liczb $Q = \{0, 1, 2\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

jest idempotentną quasigrupą przemienną.

2. Zbiór liczb $Q = \{0, 1, 2, 3, 4\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

jest idempotentną quasigrupą przemienną.

Twierdzenie. Jeśli n jest liczbą nieparzystą, to istnieje idempotentna quasigrupa przemienna Q mająca n elementów.

Dowód. Sposób konstrukcji quasigrupy Q zilustrujemy najpierw na przykładzie. Niech $Q = \{0, 1, \dots, n-1\}$ i zdefiniujmy w zbiorze Q działanie $\circ$ wzorem

$$i \circ j = (i + j) \bmod n$$

dla $i, j \in Q$. Symbolem $a \bmod n$ oznaczamy resztę z dzielenia liczby a przez n . Działanie $\circ$ jest zatem działaniem dodawania modulo n . Zauważmy teraz, że dla każdego $j \in Q$ istnieje element $i \in Q$ taki, że $i \circ i = j$. Wynika to stąd, że dla każdej liczby naturalnej j kongruencja

$$2x \equiv j \pmod{n}$$

ma rozwiązanie. Zatem w tabelce działania $\circ$ w zbiorze Q na przekątnej występują wszystkie elementy zbioru Q . Na przykład dla $n = 5$ mamy:

$\circ$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Zauważmy, że na przekątnej stoją liczby 0, 2, 4, 1, 3. Teraz w tej tabelce przenumerowujemy liczby będące wynikami działania w taki sposób, by na przekątnej występowały kolejno liczby 0, 1, 2, 3, 4. Zatem liczbę 0 zostawiamy wszędzie w tabelce bez zmian, zamiast 2 piszemy 1, zamiast 4 piszemy 2, zamiast 1 piszemy 3 i zamiast 3 piszemy 4. Otrzymamy tabelkę

$\circ$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

Nietrudno zauważyć, że dla dowolnej nieparzystej liczby naturalnej n taka konstrukcja jest możliwa. Opiszemy ją teraz dokładnie. Okazuje się, że działanie $\circ$ w zbiorze $Q = \{0, 1, \dots, n-1\}$ będzie wtedy opisane wzorem

$$i \circ j = \begin{cases} \frac{i+j}{2}, & \text{jeśli } i+j \text{ jest liczbą parzystą,} \\ \frac{i+j+n}{2} \bmod n, & \text{jeśli } i+j \text{ jest liczbą nieparzystą} \end{cases}$$

dla dowolnych $i, j \in Q$. Zauważmy, że jeśli $i+j$ jest liczbą nieparzystą, to liczba $i+j+n$ jest parzysta, więc $\frac{i+j+n}{2}$ jest liczbą całkowitą.

Wykażemy, że zbiór Q z działaniem $\circ$ jest idempotentną quasigrupą przemenną. Przemienność działania $\circ$ jest oczywista. Idempotentność wynika stąd, że dla każdego i liczba $i+i$ jest parzysta, więc

$$i \circ i = \frac{i+i}{2} = i.$$

Wykażemy wreszcie warunek (2'). Niech $i, j, k \in Q$ i załóżmy, że

$$i \circ j = i \circ k.$$

Możliwe są trzy przypadki.

Przypadek 1. Liczby $i+j$ oraz $i+k$ są parzyste. Wtedy

$$\frac{i+j}{2} = \frac{i+k}{2},$$

skąd natychmiast wynika, że $j = k$.

Przypadek 2. Liczby $i + j$ oraz $i + k$ są nieparzyste. Wtedy

$$\frac{i + j + n}{2} \bmod n = \frac{i + k + n}{2} \bmod n.$$

Zatem

$$\begin{aligned}\frac{i + j + n}{2} &\equiv \frac{i + k + n}{2} \pmod{n}, \\ i + j + n &\equiv i + k + n \pmod{n}, \\ j &\equiv k \pmod{n}.\end{aligned}$$

Ponieważ $0 \leq j, k < n$, więc $j = k$.

Przypadek 3. Jedna z liczb $i + j$ oraz $i + k$ jest parzysta (np. $i + j$), a druga nieparzysta. Wtedy

$$\frac{i + j}{2} = \frac{i + k + n}{2} \bmod n.$$

Zatem

$$\begin{aligned}\frac{i + j}{2} &\equiv \frac{i + k + n}{2} \pmod{n}, \\ i + j &\equiv i + k + n \pmod{n}, \\ j &\equiv k \pmod{n}.\end{aligned}$$

Tak jak w przypadku 2 otrzymujemy $j = k$, co kończy dowód twierdzenia.

Niech teraz Q będzie idempotentną quasigrupą przemianą mającą $2m + 1$ elementów. Definiujemy zbiór S w następujący sposób

$$S = Q \times \{0, 1, 2\} = \{(a, i) : a \in Q \wedge i \in \{0, 1, 2\}\}.$$

Oczywiście $|S| = n = 6m + 3$. Zdefiniujemy teraz zbiór T .

Do zbioru T zaliczymy dwa rodzaje trójek par:

(1) Trójki pierwszego rodzaju:

$$\{(a, 0), (a, 1), (a, 2)\}$$

dla $a \in Q$.

(2) Trójki drugiego rodzaju:

$$\{(a, 0), (b, 0), (a \circ b, 1)\}, \quad \{(a, 1), (b, 1), (a \circ b, 2)\}, \quad \{(a, 2), (b, 2), (a \circ b, 0)\}$$

dla $a, b \in Q$ takich, że $a \neq b$.

Udowodnimy teraz, że tak określona para (S, T) jest rzeczywiście systemem trójek Steinera. Najpierw pokażemy, że każde dwie pary ze zbioru S znajdują się w co najmniej jednej trójce ze zbioru T . Niech więc $(a, k), (b, l) \in S$ oraz $(a, k) \neq (b, l)$. Możliwe są trzy przypadki.

Przypadek 1. $a = b$. Wtedy $k \neq l$ oraz

$$(a, k), (a, l) \in \{(a, 0), (a, 1), (a, 2)\} \in T.$$

Przypadek 2. $a \neq b$ oraz $k = l$. Wtedy

$$(a, k), (b, k) \in \{(a, k), (b, k), (a \circ b, (k + 1) \bmod 3)\} \in T.$$

Przypadek 3. $a \neq b$ oraz $k \neq l$. Para liczb $\{k, l\}$ jest jedną z trzech par: $\{0, 1\}, \{1, 2\}, \{2, 0\}$. Możemy zatem przyjąć, że $l = (k + 1) \bmod 3$. Z definicji quasigrupy wynika, że istnieje element $c \in Q$ taki, że $a \circ c = b$. Ponieważ Q jest quasigrupą idempotentną oraz $a \neq b$, więc $c \neq a$. Zatem

$$(a, k), (b, l) \in \{(a, k), (c, k), (a \circ c, (k + 1) \bmod 3)\} = \{(a, k), (c, k), (b, l)\} \in T.$$

Aby teraz pokazać, że każde dwie pary należą do dokładnie jednej trójki ze zbioru T , wystarczy pokazać, że zbiór T ma $\frac{n(n-1)}{6}$ elementów. Otóż w zbiorze T istnieje $2m+1$ trójek pierwszego rodzaju oraz $3 \cdot \binom{2m+1}{2}$ trójek drugiego rodzaju. Zatem

$$|T| = (2m + 1) + 3 \cdot \frac{(2m + 1) \cdot 2m}{2} = (2m + 1) + 3m(2m + 1) = (2m + 1)(3m + 1)$$

oraz

$$\frac{n(n-1)}{6} = \frac{(6m+3)(6m+2)}{6} = (2m+1)(3m+1).$$

To kończy dowód, że para (S, T) jest systemem trójek Steinerja.

Przykłady.

1. Dla quasigrupy $\{0, 1, 2\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Otrzymujemy następujący zbiór S :

$$S = \left\{ \begin{pmatrix} (0,0) & (1,0) & (2,0) \\ (0,1) & (1,1) & (2,1) \\ (0,2) & (1,2) & (2,2) \end{pmatrix} \right\}.$$

Zbiór T składa się z trzech trójek pierwszego rodzaju:

$$\{(0,0), (0,1), (0,2)\}, \quad \{(1,0), (1,1), (2,1)\} \quad \text{oraz} \quad \{(2,0), (2,1), (2,2)\}$$

i dziewięciu trójek drugiego rodzaju:

$$\begin{aligned} \{(0,0), (1,0), (0 \circ 1, 1)\} &= \{(0,0), (1,0), (2,1)\}, \\ \{(0,1), (1,1), (0 \circ 1, 2)\} &= \{(0,1), (1,1), (2,2)\}, \\ \{(0,2), (1,2), (0 \circ 1, 0)\} &= \{(0,2), (1,2), (2,0)\}, \\ \{(0,0), (2,0), (0 \circ 2, 1)\} &= \{(0,0), (2,0), (1,1)\}, \\ \{(0,1), (2,1), (0 \circ 2, 2)\} &= \{(0,1), (2,1), (1,2)\}, \\ \{(0,2), (2,2), (0 \circ 2, 0)\} &= \{(0,2), (2,2), (1,0)\}, \\ \{(1,0), (2,0), (1 \circ 2, 1)\} &= \{(1,0), (2,0), (0,1)\}, \\ \{(1,1), (2,1), (1 \circ 2, 2)\} &= \{(1,1), (2,1), (0,2)\}, \\ \{(1,2), (2,2), (1 \circ 2, 0)\} &= \{(1,2), (2,2), (0,0)\}. \end{aligned}$$

Zauważmy następnie, że jeśli ponumerujemy pary $(i, j) \in S$ w następujący sposób

$$\begin{array}{lll} (0, 0) \mapsto 1 & (1, 0) \mapsto 4 & (2, 0) \mapsto 9 \\ (0, 1) \mapsto 2 & (1, 1) \mapsto 5 & (2, 1) \mapsto 7 \\ (0, 2) \mapsto 3 & (1, 2) \mapsto 6 & (2, 2) \mapsto 8 \end{array}$$

to otrzymany system trójek Steiner'a będzie identyczny z systemem pokazanym w pierwszym przykładzie. Jest to zatem system trójek Kirkmana.

2. Dla quasigrupy $Q = \{0, 1, 2, 3, 4\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

otrzymujemy następujący zbiór S :

$$S = \left\{ \begin{array}{ccccc} (0, 0) & (1, 0) & (2, 0) & (3, 0) & (4, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) & (4, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) & (4, 2) \end{array} \right\}.$$

Trójki pierwszego rodzaju mają następującą postać:

$$S = \left\{ \begin{array}{ccccc} (0, 0) & (1, 0) & (2, 0) & (3, 0) & (4, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) & (4, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) & (4, 2) \end{array} \right\}$$

Kolorami czerwonym, zielonym i niebieskim zaznaczone są trójki

$$\{(0, 0), (0, 1), (0, 2)\}, \quad \{(3, 0), (3, 1), (3, 2)\} \quad \text{oraz} \quad \{(4, 0), (4, 1), (4, 2)\}.$$

Trójki drugiego rodzaju mają postać:

$$S = \left\{ \begin{array}{ccccc} (0, 0) & (1, 0) & (2, 0) & (3, 0) & (4, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) & (4, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) & (4, 2) \end{array} \right\}$$

Kolorem czerwonym zaznaczona jest trójka

$$\{(2, 0), (3, 0), (2 \circ 3, 1)\} = \{(2, 0), (3, 0), (0, 1)\},$$

kolorem zielonym zaznaczona jest trójka

$$\{(3, 1), (4, 1), (3 \circ 4, 2)\} = \{(3, 1), (4, 1), (1, 2)\},$$

wreszcie kolorem niebieskim zaznaczona jest trójka

$$\{(0, 2), (3, 2), (0 \circ 3, 0)\} = \{(0, 2), (3, 2), (4, 0)\}.$$

Można pokazać, że otrzymany system trójek Steiner nie jest systemem trójek Kirkmana, zatem różni się istotnie od przykładu pokazanego wcześniej.

Pokażemy teraz sposób konstrukcji systemu trójek Steiner (S, T) , w którym $|S| = 6m + 1$. Znowż zaczniemy od pojęć algebraicznych. Mówimy, że quasigrupa przemienna $Q = \{0, 1, \dots, 2n - 1\}$ (mająca zatem $2n$ elementów) jest **pólidempotentna**, jeśli spełnia następujący warunek:

$$(4) \ a \circ a = (n + a) \circ (n + a) = a \text{ dla } a = 0, 1, \dots, n.$$

Przykłady.

1. Zbiór liczb $Q = \{0, 1\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	0	1
0	0	1
1	1	0

jest pólidempotentną quasigrupą przemienną.

2. Zbiór liczb $Q = \{0, 1, 2, 3\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

jest idempotentną quasigrupą przemienną.

2. Zbiór liczb $Q = \{0, 1, 2, 3, 4, 5\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	0	1	2	3	4	5
0	0	3	1	4	2	5
1	3	1	4	2	5	0
2	1	4	2	5	0	3
3	4	2	5	0	3	1
4	2	5	0	3	1	4
4	5	0	3	1	4	2

jest idempotentną quasigrupą przemienną.

Twierdzenie. Dla każdej liczby naturalnej $n \geq 1$ istnieje pólidempotentna quasigrupa przemienna $Q = \{0, 1, \dots, 2n - 1\}$ mająca $2n$ elementów.

Szkic dowodu. Znów możemy przenieść tabelkę dodawania modulo $2n$. Działanie $\circ$ w zbiorze Q będzie wtedy określone wzorem:

$$i \circ j = \begin{cases} \frac{(i+j) \bmod 2n}{2}, & \text{jeśli } i+j \text{ jest liczbą parzystą,} \\ \frac{(i+j-1) \bmod 2n}{2}, & \text{jeśli } i+j \text{ jest liczbą nieparzystą} \end{cases}$$

dla $i, j \in \{0, 1, \dots, 2n-1\}$. Sprawdzenie, że zbiór Q z tak określonym działaniem $\circ$ jest pólidempotentna quasigrupą przemienną, pozostawimy jako ćwiczenie.

Niech teraz $Q = \{0, 1, \dots, 2m-1\}$ będzie pólidempotentną quasigrupą przemienną mającą $2m$ elementów i niech $\infty \notin Q \times \{0, 1, 2\}$. Definiujemy zbiór S w następujący sposób

$$S = \{\infty\} \cup (Q \times \{0, 1, 2\}) = \{\infty\} \cup \{(a, i) : a \in Q \wedge i \in \{0, 1, 2\}\}.$$

Oczywiście $|S| = n = 6m + 1$. Zdefiniujemy teraz zbiór T .

Do zbioru T zaliczymy trzy rodzaje trójek par:

(1) Trójki pierwszego rodzaju:

$$\{(a, 0), (a, 1), (a, 2)\}$$

dla $a = 0, \dots, m-1$.

(2) Trójki drugiego rodzaju:

$$\{\infty, (a, 1), (a+m, 0)\}, \quad \{\infty, (a, 2), (a+m, 1)\}, \quad \{\infty, (a, 0), (a+m, 2)\}$$

dla $a = 0, \dots, m-1$.

(2) Trójki trzeciego rodzaju:

$$\{(a, 0), (b, 0), (a \circ b, 1)\}, \quad \{(a, 1), (b, 1), (a \circ b, 2)\}, \quad \{(a, 2), (b, 2), (a \circ b, 0)\}$$

dla $a, b \in Q$ takich, że $a \neq b$.

Wykazanie, że tak określona para (S, T) jest rzeczywiście systemem trójek Steinera, pozostawimy jako ćwiczenie.

Przykłady.

1. Dla quasigrupy $\{0, 1\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	0	1
0	0	1
1	1	0

Otrzymujemy następujący zbiór S :

$$S = \left\{ \begin{matrix} \infty & (0, 0) & (1, 0) \\ & (0, 1) & (1, 1) \\ & (0, 2) & (1, 2) \end{matrix} \right\}.$$

Zbiór T składa się z jednej trójki pierwszego rodzaju:

$$\{(0, 0), (0, 1), (0, 2)\},$$

trzech trójek drugiego rodzaju:

$$\{\infty, (1, 0), (0, 1)\}, \quad \{\infty, (1, 1), (0, 2)\}, \quad \{\infty, (1, 2), (0, 0)\}$$

i trzech trójek trzeciego rodzaju:

$$\begin{aligned} \{(0, 0), (1, 0), (0 \circ 1, 1)\} &= \{(0, 0), (1, 0), (1, 1)\}, \\ \{(0, 1), (1, 1), (0 \circ 1, 2)\} &= \{(0, 1), (1, 1), (1, 2)\}, \\ \{(0, 2), (1, 2), (0 \circ 1, 0)\} &= \{(0, 2), (1, 2), (1, 0)\}. \end{aligned}$$

Zauważmy następnie, że jeśli ponumerujemy elementy zbioru S w następujący sposób

$$\begin{array}{lll} (0, 0) \mapsto 1 & (1, 0) \mapsto 6 \\ \infty \mapsto 7 & (0, 1) \mapsto 2 & (1, 1) \mapsto 5 \\ & (0, 2) \mapsto 4 & (1, 2) \mapsto 3 \end{array}$$

to otrzymany system trójek Steinerja będzie identyczny z systemem pokazanym poprzednio dla siedmioelementowego zbioru S .

1. Dla quasigrupy $\{0, 1, 2, 3\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	0	1	2	3
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

otrzymamy następujący zbiór S :

$$S = \left\{ \infty \begin{array}{llll} (0, 0) & (1, 0) & (2, 0) & (3, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) \end{array} \right\}.$$

Zbiór T składa się z dwóch trójek pierwszego rodzaju (zaznaczonych kolorami czerwonym i zielonym):

$$S = \left\{ \infty \begin{array}{llll} (0, 0) & (1, 0) & (2, 0) & (3, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) \end{array} \right\}$$

sześciu trójek drugiego rodzaju, z których trzy zostały zaznaczone kolorami czerwonym, zielonym i niebieskim:

$$S = \left\{ \infty \begin{array}{llll} (0, 0) & (1, 0) & (2, 0) & (3, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) \end{array} \right\}$$

$$S = \left\{ \infty \begin{array}{llll} (0, 0) & (1, 0) & (2, 0) & (3, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) \end{array} \right\}$$

$$S = \left\{ \infty \begin{array}{llll} (0, 0) & (1, 0) & (2, 0) & (3, 0) \\ (0, 1) & (1, 1) & (2, 1) & (3, 1) \\ (0, 2) & (1, 2) & (2, 2) & (3, 2) \end{array} \right\}$$

i 18 trójek trzeciego rodzaju, z których trzy również zostały zaznaczone kolorami czerwonym, zielonym i niebieskim:

$$S = \left\{ \begin{array}{cccc} \infty & \begin{smallmatrix} (0,0) \\ (0,1) \\ (0,2) \end{smallmatrix} & \begin{smallmatrix} (1,0) \\ (1,1) \\ (1,2) \end{smallmatrix} & \begin{smallmatrix} (2,0) \\ (2,1) \\ (2,2) \end{smallmatrix} & \begin{smallmatrix} (3,0) \\ (3,1) \\ (3,2) \end{smallmatrix} \end{array} \right\}$$

Dowód niealgebraiczny.

Naszukujemy teraz pochodzący od Kirkmana, oryginalny dowód istnienia systemów trójek Steinera. Wprowadzimy najpierw dwa pojęcia pomocnicze.

Niech $X = \{\sigma_0, \dots, \sigma_{2n-2}\} \cup \{\alpha\}$ będzie zbiorem $2n$ -elementowym i niech H będzie zbiorem wszystkich dwuelementowych podzbiorów zbioru X :

$$H = \{A \subseteq X : |A| = 2\}.$$

Ciąg zbiorów $(H_0, \dots, H_{2n-2})$ nazywamy **1-faktoryzacją** zbioru H , jeśli dla każdego $x \in X$ w każdym zbiorze H_j istnieje dokładnie jedna para, której x jest elementem.

Ćwiczenie. Ciąg zbiorów $(H_0, \dots, H_{2n-2})$ zdefiniowanych w następujący sposób

$$H_j = \{\{\sigma_k, \sigma_l\} : k + l \equiv j + 1 \pmod{2n-1}\} \cup \{\{\alpha, \sigma_{(j+1)n \bmod (2n-1)}\}\}$$

dla $j = 0, \dots, 2n-2$ jest 1-faktoryzacją zbioru H .

Przykład. Ciąg zbiorów $(H_0, \dots, H_6)$ zdefiniowanych w następujący sposób

$$\begin{aligned} H_0 &= \{\{\sigma_0, \sigma_1\}, \{\sigma_2, \sigma_6\}, \{\sigma_3, \sigma_5\}, \{\sigma_4, \alpha\}\}, \\ H_1 &= \{\{\sigma_0, \sigma_2\}, \{\sigma_3, \sigma_6\}, \{\sigma_4, \sigma_5\}, \{\sigma_1, \alpha\}\}, \\ H_2 &= \{\{\sigma_0, \sigma_3\}, \{\sigma_1, \sigma_2\}, \{\sigma_4, \sigma_6\}, \{\sigma_5, \alpha\}\}, \\ H_3 &= \{\{\sigma_0, \sigma_4\}, \{\sigma_1, \sigma_3\}, \{\sigma_5, \sigma_6\}, \{\sigma_2, \alpha\}\}, \\ H_4 &= \{\{\sigma_0, \sigma_5\}, \{\sigma_1, \sigma_4\}, \{\sigma_2, \sigma_3\}, \{\sigma_6, \alpha\}\}, \\ H_5 &= \{\{\sigma_0, \sigma_6\}, \{\sigma_1, \sigma_5\}, \{\sigma_2, \sigma_4\}, \{\sigma_3, \alpha\}\}, \\ H_6 &= \{\{\sigma_1, \sigma_6\}, \{\sigma_2, \sigma_5\}, \{\sigma_3, \sigma_4\}, \{\sigma_0, \alpha\}\} \end{aligned}$$

jest 1-faktoryzacją zbioru $X = \{\sigma_0, \dots, \sigma_6\} \cup \{\alpha\}$. Tę 1-faktoryzację nazywamy **faktoryzacją Kirkmana**.

W dalszym ciągu szczególnie ważne będzie to, że:

$$\begin{aligned} \{\sigma_0, \sigma_1\} &\in H_0, \\ \{\sigma_0, \sigma_2\}, \{\sigma_1, \alpha\} &\in H_1, \\ \{\sigma_0, \sigma_{j+1}\}, \{\sigma_1, \sigma_j\} &\in H_j \quad \text{dla } j = 2, \dots, 2n-3, \\ \{\sigma_0, \alpha\}, \{\sigma_1, \sigma_{2n-2}\} &\in H_{2n-2}. \end{aligned}$$

Przypuśćmy następnie, że para (S, T) jest systemem trójek Steinera, w którym $|S| = n$ (przypominamy, że n jest liczbą nieparzystą). Niech następnie $x, y \in S$ i niech z będzie jedynym elementem zbioru S takim, że $\{x, y, z\} \in T$. Mówimy, że system (S, T) jest **x, y -ogrodzony**, a ciąg $(s_0, \dots, s_{n-4})$ elementów zbioru S jest jego **x, y -ogrodzeniem**, jeśli

$$\{x, s_0, s_1\}, \{y, s_1, s_2\}, \{x, s_2, s_3\}, \{y, s_3, s_4\}, \dots, \{y, s_{n-6}, s_{n-5}\}, \{x, s_{n-5}, s_{n-4}\}, \{y, s_{n-4}, s_0\} \in T.$$

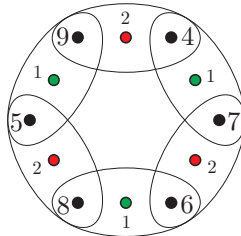
Przykład. System trójek Steinera (S, T) , w którym $S = \{1, \dots, 9\}$ oraz

$$T = \left\{ \begin{array}{l} \{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \\ \{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\} \end{array} \right\}$$

jest systemem 1, 2-ogrodzonym, a jego 1, 2-ogrodzeniem jest ciąg $(4, 7, 6, 8, 5, 9)$:

$$\{1, 4, 7\}, \{2, 7, 6\}, \{1, 6, 8\}, \{2, 8, 5\}, \{1, 5, 9\}, \{2, 9, 4\} \in T.$$

A oto graficzna ilustracja tego ogrodzenia:



Dowód Kirkmana wynika teraz (przez indukcję, której szczegóły pozostawimy jako ćwiczenie) z następujących trzech faktów.

1. Istnieje system trójek Steinera (S, T) , w którym $|S| = 3$.
2. Jeśli istnieje system trójek Steinera (S, T) , w którym $|S| = 2n - 1$, to istnieje ogrodzony system trójek Steinera (S^*, T^*) , w którym $|S^*| = 4n - 1$.
3. Jeśli istnieje ogrodzony system trójek Steinera (S, T) , w którym $|S| = 2n + 1$ (przy czym $n \geq 3$), to istnieje ogrodzony system trójek Steinera (S^*, T^*) , w którym $|S^*| = 4n - 3$.

Fakt 1 jest oczywisty. Pokażemy teraz szkice dowodów faktów 2 i 3.

2. Niech (S, T) będzie systemem trójek Steinera, w którym $S = \{s_0, \dots, s_{2n-2}\}$ oraz niech zbiór $X = \{\sigma_0, \dots, \sigma_{2n-2}\} \cup \{\alpha\}$ będzie zbiorem rozłącznym ze zbiorem S . Niech następnie ciąg $(H_0, \dots, H_{2n-2})$ będzie faktoryzacją Kirkmana zbioru H dwuelementowych podzbiorów zbioru X . Definiujemy rodzinę trójek U w następujący sposób:

$$U = \{\{s_j, a, b\} : (j \in \{0, \dots, 2n-2\}) \wedge (\{a, b\} \in H_j)\}.$$

Niech następnie $S^* = S \cup X$ oraz $T^* = T \cup U$. Wtedy para (S^*, T^*) jest σ_0, σ_1 -ogrodzonym systemem trójek Steinera oraz ciąg

$$(s_1, \sigma_2, s_2, \sigma_3, s_3, \sigma_4, \dots, \sigma_{2n-2}, s_{2n-2}, \alpha)$$

jest jego σ_0, σ_1 -ogrodzeniem.

3. Niech (S, T) będzie systemem trójek Steinera, w którym $S = \{x, y, z, s_0, \dots, s_{2n-3}\}$ oraz $\{x, y, z\} \in T$. Załóżmy, że system (S, T) jest x, y -ogrodzony, przy czym ciąg

$$(s_0, s_1, \dots, s_{2n-4}, s_{2n-3})$$

jest jego x, y -ogrodzeniem. Niech zbiór $X = \{\sigma_0, \dots, \sigma_{2n-2}\} \cup \{\alpha\}$ będzie zbiorem rozłącznym ze zbiorem S . Niech następnie ciąg $(H_0, \dots, H_{2n-2})$ będzie faktoryzacją Kirkmana zbioru H dwuelementowych podzbiorów zbioru X . Definiujemy następujące rodziny trójek:

$$\begin{aligned} T_1 &= \{\{a, b, c\} \in T : \{a, b, c\} \cap \{x, y\} = \emptyset\}, \\ U &= \{\{s_j, a, b\} : (j \in \{0, \dots, 2n-3\}) \wedge (\{a, b\} \in H_{j+1}) \wedge (\{a, b\} \cap \{\sigma_0, \sigma_1\} = \emptyset)\}, \\ V &= \{\{z, a, b\} : (\{a, b\} \in H_0) \wedge (\{a, b\} \neq \{\sigma_0, \sigma_1\})\}, \\ W &= \{\{s_j, s_{j+1}, s_{j+2}\} : 0 \leq j < 2n-3\} \cup \{\{\alpha, s_0, s_{2n-3}\}\}. \end{aligned}$$

Niech następnie $S^* = \{s_0, \dots, s_{2n-3}\} \cup \{z\} \cup \{\sigma_2, \dots, \sigma_{2n-2}\} \cup \{\alpha\}$ oraz $T^* = T_1 \cup U \cup V \cup W$. Wtedy $\{\sigma_2, \sigma_3, s_3\} \in T^*$ oraz para (S^*, T^*) jest σ_2, σ_3 -ogrodzonym systemem trójek Steinera, przy czym ciąg

$$(s_0, s_1, s_2, \alpha, s_4, \sigma_4, s_5, \sigma_5, \dots, s_{2n-3}, \sigma_{2n-3}, z, \sigma_{2n-2})$$

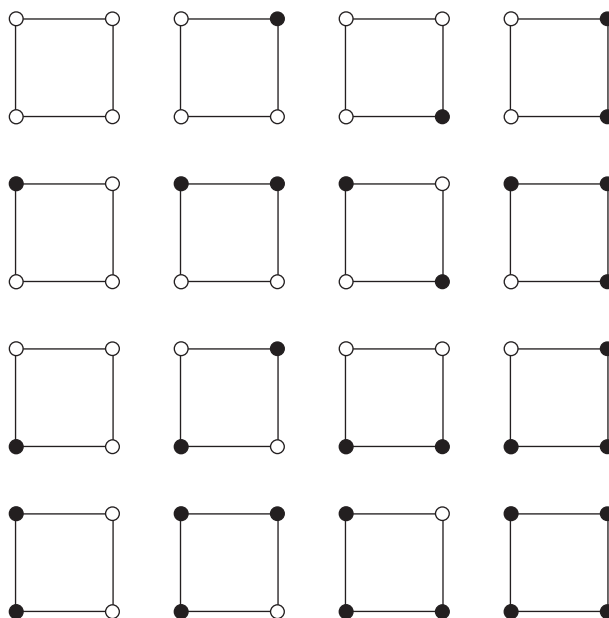
jest jego σ_2, σ_3 -ogrodzeniem.

Szczegóły dowodów pozostawimy również jako ćwiczenie.

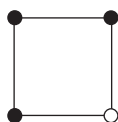
Zliczanie kolorowań; lemat Burnside'a.

Popatrzmy na cztery przykłady.

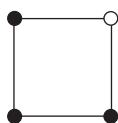
Przykład 1. Wierzchołki kwadratu można pokolorować co najwyżej dwoma kolorami na 16 różnych sposobów:



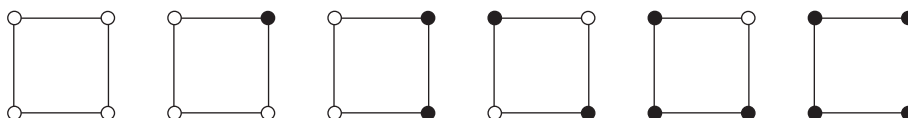
Przykład 2. Niektóre z kolorowań pokazanych w przykładzie 1 możemy uznać za jednakowe w tym sensie, że pewna izometria kwadratu przeprowadza jedno z tych kolorowań na drugie. Na przykład kolorowanie



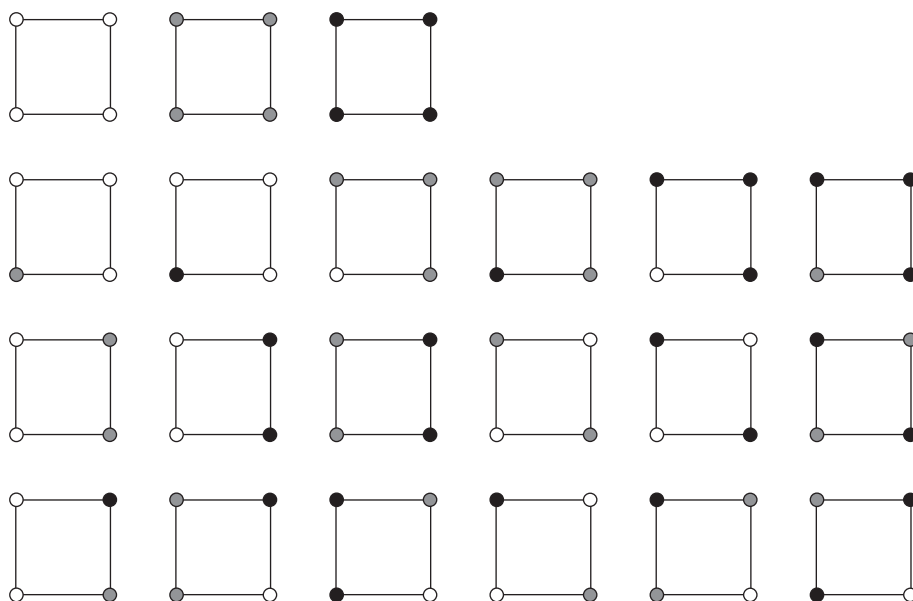
powstaje z kolorowania



przez obrót o 90° w kierunku przeciwnym do ruchu wskazówek zegara. Takie kolorowania będziemy nazywać kolorowaniami geometrycznie nierozróżnialnymi. Okazuje się, że istnieje dokładnie 6 geometrycznie rozróżnialnych kolorowań wierzchołków kwadratu za pomocą co najwyżej dwóch kolorów:

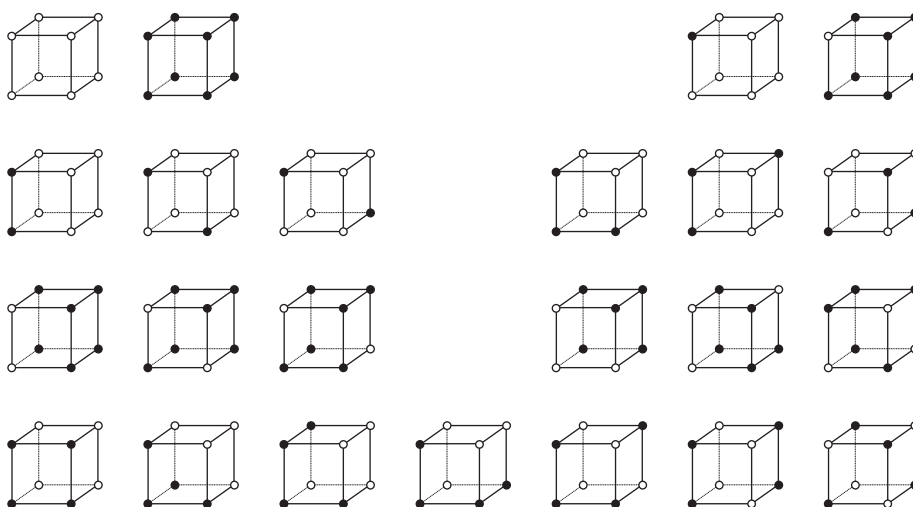


Przykład 3. Używając trzech kolorów można pokolorować wierzchołki kwadratu na 21 geometrycznie rozróżnialnych sposobów:



W ostatnim przykładzie będziemy kolorować wierzchołki sześcianu. Dwa kolorowania uważamy za identyczne (geometrycznie nierozróżnialne), jeśli jedno można otrzymać z drugiego przez odpowiedni obrót sześcianu.

Przykład 4. Wierzchołki sześcianu można pokolorować na dokładnie 23 geometrycznie rozróżnialne sposoby za pomocą co najwyżej dwóch kolorów:



Definicja geometrycznej nierozróżnialności zależy od tego, jakie izometrie będziemy rozważać. Gdybyśmy w ostatnim przykładzie dopuścili wszystkie izometrie sześcianu (czyli również symetrie), to otrzymalibyśmy dokładnie 22 geometrycznie rozróżnialne kolorowania za pomocą co najwyżej dwóch kolorów. Pozostawimy Czytelnikowi jako ćwiczenie znalezienie dwóch kolorowań, które są rozróżnialne, gdy rozpatrujemy wyłącznie obroty sześcianu i są nierozróżnialne, gdy dopuścimy również symetrie.

Widzimy więc, że definicja geometrycznej rozróżnialności kolorowań zależy od tego, jaką grupę izometrii będziemy rozpatrywać. Problemem rozróżnialności kolorowań zajmemy się teraz bardziej ogólnie.

Niech będzie dany zbiór skończony A . Kolorowaniem zbioru A nazwiemy dowolną funkcję

$$c : A \rightarrow \{1, \dots, k\}.$$

Mówimy też wtedy, że elementy zbioru A kolorujemy za pomocą k kolorów (nawet, jeśli nie wszystkie kolory zostały użyte). Niech K będzie zbiorem wszystkich kolorowań zbioru A za pomocą k kolorów. Przypuśćmy następnie, że dana jest pewna grupa G przekształceń zbioru A na siebie (czyli podgrupa grupy wszystkich permutacji zbioru A). Definiujemy teraz grupę G^* przekształceń zbioru K . Dla dowolnego przekształcenia $\pi \in G$ definiujemy przekształcenie

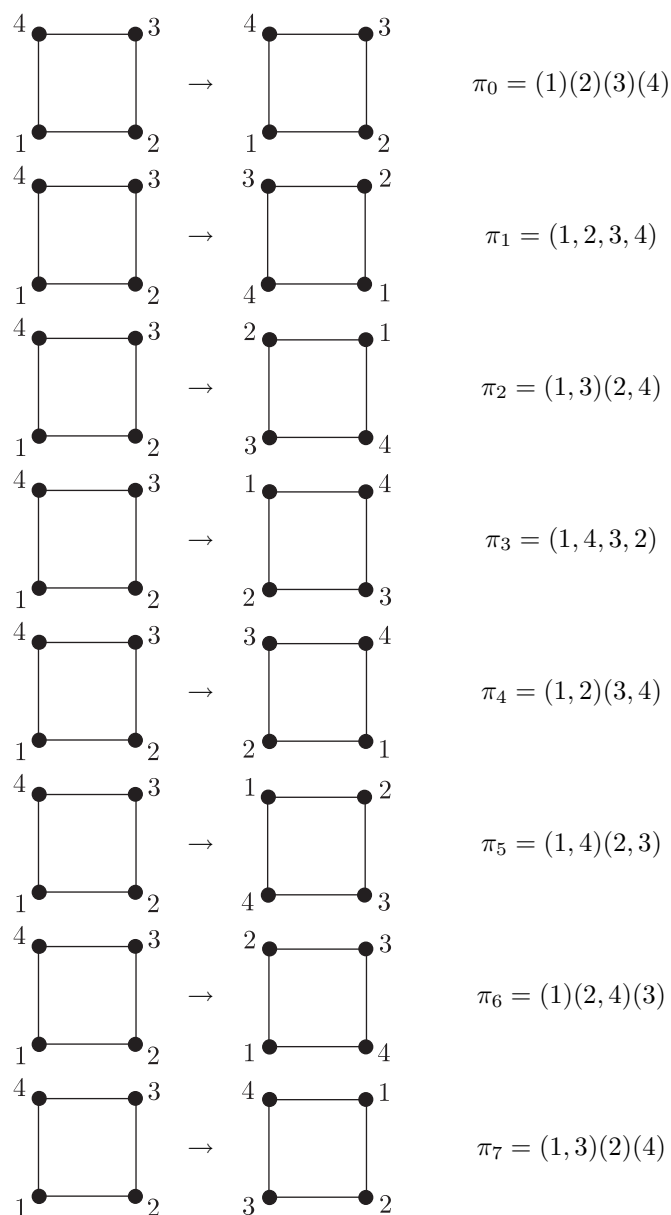
$$\pi^* : K \rightarrow K$$

wzorem $\pi^*(c) = c \circ \pi^{-1}$. Wreszcie przyjmujemy

$$G^* = \{\pi^* : \pi \in G\}.$$

Ćwiczenie. Jeśli $k \geq 2$, $\pi, \sigma \in G$ oraz $\pi \neq \sigma$, to $\pi^* \neq \sigma^*$. W szczególności $|G^*| = |G|$.

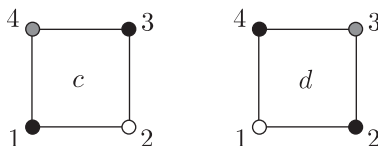
Przykład 5. Niech A będzie zbiorem wierzchołków kwadratu. Grupa G wszystkich izometrii kwadratu składa się z następujących 8 przekształceń:



Popatrzmy na następujące dwa kolorowania

$$c, d : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3\}$$

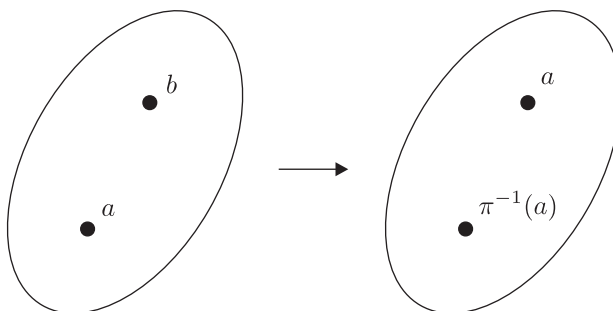
(kolorowi białemu odpowiada liczba 1, kolorowi szaremu liczba 2 i kolorowi czarnemu liczba 3):



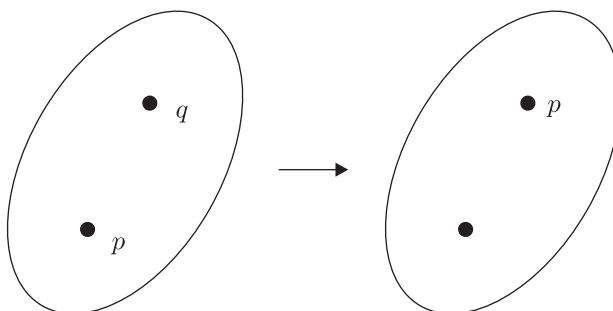
Zauważmy, że kolorowanie d powstało przez „obrócenie” kolorowania c o 90° zgodnie z ruchem wskazówek zegara, czyli w taki sposób, w jaki działa na wierzchołkach kwadratu przekształcenie π_3 . Pokażemy, że rzeczywiście $d = \pi_3^*(c)$. Mianowicie

$$\begin{aligned}\pi_3^*(c)(1) &= c(\pi_3^{-1}(1)) = c(2) = 1 = d(1), \\ \pi_3^*(c)(2) &= c(\pi_3^{-1}(2)) = c(3) = 3 = d(2), \\ \pi_3^*(c)(3) &= c(\pi_3^{-1}(3)) = c(4) = 2 = d(3), \\ \pi_3^*(c)(4) &= c(\pi_3^{-1}(4)) = c(1) = 3 = d(4).\end{aligned}$$

Przykład 6. Ogólniej, przypuśćmy, że przekształcenie $\pi \in G$ przeprowadza element $a \in A$ na element $b \in A$, tzn. $\pi(a) = b$:



Przypuśćmy następnie, że elementy a i b zostały pokolorowane (w kolorowaniu c) kolorami p i q . Przekształcenie π^* zamienia wtedy kolory w następujący sposób:



Mamy wówczas

$$\pi^*(c)(b) = p = c(a) = c(\pi^{-1}(b)) = c \circ \pi^{-1}(b),$$

czyli

$$\pi^*(c) = c \circ \pi^{-1}.$$

Mówimy teraz, że dwa kolorowania c i d zbioru A są nierozróżnialne (ze względu na grupę G), jeśli istnieje przekształcenie $\pi \in G$ takie, że $\pi^*(c) = d$. Interesuje nas wyznaczenie liczby kolorowań rozróżnialnych ze względu na grupę G .

Definicja. Jeśli G jest pewną grupą przekształceń zbioru A oraz $a \in A$, to **orbitą** elementu a (ze względu na grupę G) nazywamy zbiór

$$O(a) = \{\pi(a) : \pi \in G\}.$$

Naszym celem jest więc wyznaczenie liczby orbit grupy G w zbiorze K .

Definicja. Niech G będzie pewną grupą przekształceń zbioru A i niech $a \in A$. Wówczas **stabilizatorem** elementu a nazywamy zbiór

$$S(a) = \{\pi \in G : \pi(a) = a\}.$$

Nietrudno zauważyć, że stabilizator elementu a jest podgrupą grupy G . Udowodnimy następujący lemat:

Lemat. Dla każdego elementu a zbioru A zachodzi równość

$$|S(a)| \cdot |O(a)| = |G|.$$

Dowód. Niech $O(a) = \{b_1, \dots, b_r\}$. Wybieramy takie przekształcenia $\pi_1, \dots, \pi_r \in G$, by

$$\pi_1(a) = b_1, \dots, \pi_r(a) = b_r.$$

Niech $P = \{\pi_1, \dots, \pi_r\}$. Oczywiście $|P| = |O(a)|$. Pokażemy, że każde przekształcenie $\pi \in G$ można przedstawić jednoznacznie w postaci $\pi = \sigma \circ \rho$, gdzie $\sigma \in P$ oraz $\rho \in S(a)$. To oczywiście zakończy dowód.

Niech więc $\pi \in G$. Niech następnie $\pi(a) = b_s$, gdzie $1 \leq s \leq r$. Zatem $\pi(a) = \pi_s(a)$. Przyjmijmy

$$\sigma = \pi_s, \quad \rho = \pi_s^{-1} \circ \pi.$$

Oczywiście

$$\sigma \circ \rho = \pi_s \circ (\pi_s^{-1} \circ \pi) = \pi.$$

Ponadto $\sigma = \pi_s \in P$. Pokażemy, że $\rho \in S(a)$. Mianowicie

$$\rho(a) = (\pi_s^{-1} \circ \pi)(a) = \pi_s^{-1}(\pi(a)) = \pi_s^{-1}(\pi_s(a)) = a.$$

To dowodzi, że przekształcenie π może być przedstawione w żądanej postaci.

Przypuśćmy teraz, że

$$\pi_s \circ \rho = \pi_t \circ \tau,$$

gdzie $1 \leq s, t \leq r$ oraz $\rho, \tau \in S(a)$. Wówczas

$$(\pi_s \circ \rho)(a) = (\pi_t \circ \tau)(a),$$

$$\pi_s(\rho(a)) = \pi_t(\tau(a)),$$

$$\pi_s(a) = \pi_t(a),$$

$$b_s = b_t,$$

$$s = t.$$

Zatem $\pi_s = \pi_t$, skąd oczywiście wynika, że $\rho = \tau$, co kończy dowód lematu.

Definicja. Niech G będzie pewną grupą przekształceń zbioru A i niech $\pi \in G$. Wtedy **charakterem** przekształcenia π nazywamy liczbę tych $a \in A$, dla których $\pi(a) = a$:

$$\chi(\pi) = |\{a \in A : \pi(a) = a\}|.$$

Udowodnimy teraz następujący lemat:

Lemat Burnside’a. Niech G będzie pewną grupą przekształceń zbioru A . Wtedy liczba orbit w zbiorze A (ze względu na grupę G) jest równa

$$t(G) = \frac{1}{|G|} \cdot \sum_{\pi \in G} \chi(\pi).$$

Dowód. Będziemy zliczać na dwa sposoby liczbę elementów zbioru

$$X = \{(\pi, a) \in G \times A : \pi(a) = a\}.$$

Dla każdego $\pi \in G$ istnieje $\chi(\pi)$ takich $a \in A$, dla których $\pi(a) = a$, czyli $(\pi, a) \in X$. Zatem

$$|X| = \sum_{\pi \in G} \chi(\pi).$$

Z drugiej strony, dla każdego $a \in A$ istnieje $|S(a)|$ takich przekształceń π , dla których $\pi(a) = a$, czyli $(\pi, a) \in X$. Zatem

$$|X| = \sum_{a \in A} |S(a)|.$$

Z poprzedniego lematu wynika, że

$$|X| = \sum_{a \in A} \frac{|G|}{|O(a)|} = |G| \cdot \sum_{a \in A} \frac{1}{|O(a)|}.$$

Przypuśćmy teraz, że zbiór A został rozbity na $r = t(G)$ orbit i niech $b_1, \dots, b_r$ będą reprezentantami tych orbit. Wówczas

$$\begin{aligned} \sum_{a \in A} \frac{1}{|O(a)|} &= \sum_{j=1}^r \sum_{a \in O(b_j)} \frac{1}{|O(a)|} = \sum_{j=1}^r \sum_{a \in O(b_j)} \frac{1}{|O(b_j)|} = \sum_{j=1}^r \left(\frac{1}{|O(b_j)|} \cdot \sum_{a \in O(b_j)} 1 \right) = \\ &= \sum_{j=1}^r \left(\frac{1}{|O(b_j)|} \cdot |O(b_j)| \right) = \sum_{j=1}^r 1 = r = t(G). \end{aligned}$$

Zatem

$$|X| = |G| \cdot t(G),$$

czyli

$$|G| \cdot t(G) = \sum_{\pi \in G} \chi(\pi),$$

skąd natychmiast wynika teza lematu Burnside’a.

Przypuśćmy teraz, że dany jest zbiór A i pewna grupa G przekształceń zbioru A . Rozważamy zbiór K kolorowań zbioru A za pomocą k kolorów i grupę G^* przekształceń zbioru K . Wówczas liczba orbit grupy G^* jest równa

$$t(G^*) = \frac{1}{|G^*|} \cdot \sum_{\sigma \in G^*} \chi(\sigma) = \frac{1}{|G|} \cdot \sum_{\pi \in G} \chi(\pi^*).$$

Dla dowolnego przekształcenia $\pi \in G$ chcemy obliczyć $\chi(\pi^*)$. Przypuśćmy zatem, że $c \in K$. Zauważmy, że następujące warunki są równoważne:

$$\begin{aligned}\pi^*(c) &= c, \\ c \circ \pi^{-1} &= c, \\ c &= c \circ \pi, \\ \forall a \in A \quad (c(\pi(a)) &= c(a)).\end{aligned}$$

Ostatni warunek jest równoważny temu, że wszystkie elementy tego samego cyklu (w rozkładzie permutacji π na cykle) są pokolorowane tym samym kolorem. Zatem, jeśli $z(\pi)$ oznacza liczbę cykli permutacji π , to

$$\chi(\pi^*) = k^{z(\pi)}.$$

Stąd otrzymujemy wzór

$$t(G^*) = \frac{1}{|G|} \cdot \sum_{\pi \in G} k^{z(\pi)}.$$

Przykład 7. Przypomnijmy, że grupa izometrii kwadratu (traktowana jako grupa przekształceń zbioru wierzchołków ponumerowanych liczbami 1,2,3,4) składa się z 8 przekształceń:

$$\begin{aligned}\pi_0 &= (1)(2)(3)(4), \\ \pi_1 &= (1, 2, 3, 4), \\ \pi_2 &= (1, 3)(2, 4), \\ \pi_3 &= (1, 4, 3, 2), \\ \pi_4 &= (1, 2)(3, 4), \\ \pi_5 &= (1, 4)(2, 3), \\ \pi_6 &= (1)(2, 4)(3), \\ \pi_7 &= (1, 3)(2)(4).\end{aligned}$$

Zatem liczba geometrycznie rozróżnialnych kolorowań wierzchołków kwadratu za pomocą k kolorów jest równa

$$\frac{1}{8} \cdot (k^4 + k + k^2 + k + k^2 + k^2 + k^3 + k^3) = \frac{1}{8} \cdot (k^4 + 2k^3 + 3k^2 + 2k).$$

Dla $k = 2$ otrzymujemy

$$\frac{1}{8} \cdot (2^4 + 2 \cdot 2^3 + 3 \cdot 2^2 + 2 \cdot 2) = \frac{1}{8} \cdot (16 + 16 + 12 + 4) = \frac{48}{8} = 6$$

kolorowań. Dla $k = 3$ otrzymujemy

$$\frac{1}{8} \cdot (3^4 + 2 \cdot 3^3 + 3 \cdot 3^2 + 2 \cdot 3) = \frac{1}{8} \cdot (81 + 54 + 27 + 6) = \frac{168}{8} = 21$$

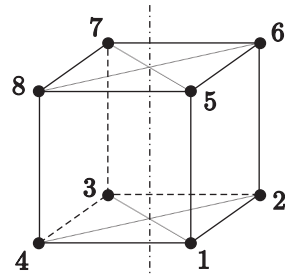
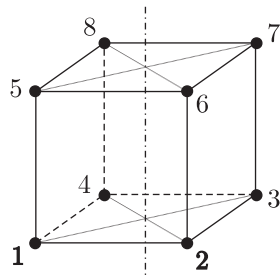
kolorowań.

Przykład 8. Grupa obrotów sześciianu składa się z 24 przekształceń. Znów traktujemy ją jako grupę przekształceń zbioru wierzchołków ponumerowanych liczbami od 1 do 8.

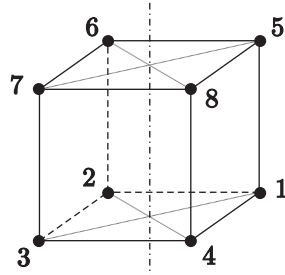
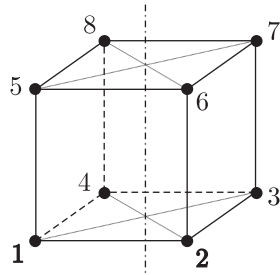
Pierwszym przekształceniem jest identyczność:

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

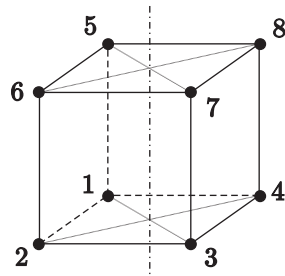
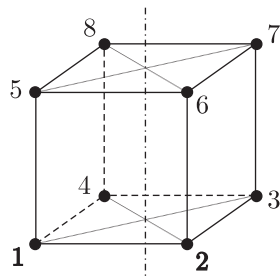
Następnie mamy obroty sześciianu wokół osi przechodzącej przez środki przeciwległych ścian (są 3 takie osie).



Obrót sześcianu o 90° : $\pi = (1, 2, 3, 4)(5, 6, 7, 8)$

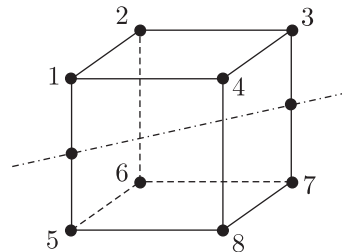
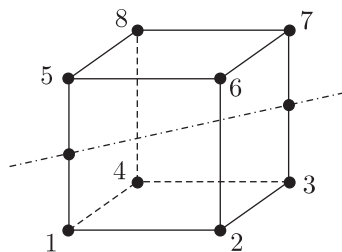


Obrót sześcianu o 180° : $\pi = (1, 3)(2, 4)(5, 7)(6, 8)$



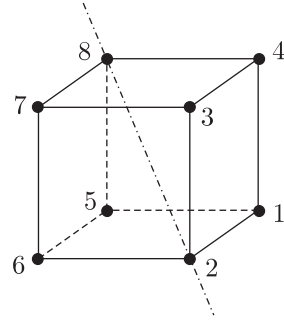
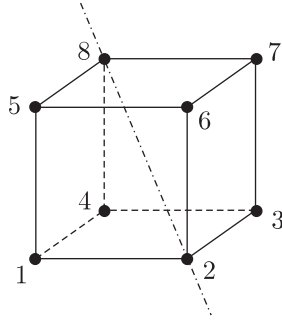
Obrót sześcianu o 270° : $\pi = (1, 4, 3, 2)(5, 8, 7, 6)$

Teraz mamy obrót sześcianu wokół osi przechodzącej przez środki przeciwległych krawędzi (jest 6 takich osi).

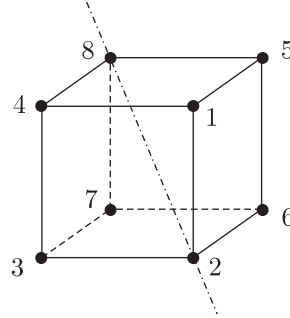
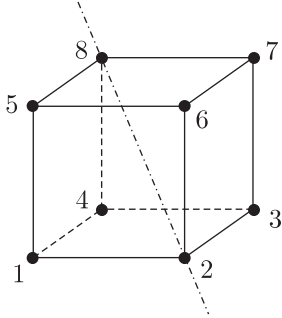


Obrót sześcianu o 180° : $\pi = (1, 5)(2, 8)(3, 7)(4, 6)$

Wreszcie mamy obroty sześcianu wokół osi przechodzącej przez przeciwległe wierzchołki (są 4 takie osie).



Obrót sześcianu o 120° : $\pi = (1, 3, 6)(2)(4, 7, 5)(8)$



Obrót sześcianu o 240° : $\pi = (1, 6, 3)(2)(4, 5, 7)(8)$

Mamy zatem jedną permutację o 8 cyklach, 6 permutacji o 2 cyklach i 17 permutacji o 4 cyklach. Stąd wynika, że liczba geometrycznie rozróżnialnych kolorowań wierzchołków sześcianu za pomocą k kolorów jest równa

$$\frac{1}{24} \cdot (k^8 + 17k^4 + 6k^2).$$

Dla $k = 2$ otrzymujemy

$$\frac{1}{24} \cdot (2^8 + 17 \cdot 2^4 + 6 \cdot 2^2) = \frac{1}{24} \cdot (256 + 272 + 24) = \frac{552}{24} = 23$$

kolorowania. W podobny sposób stwierdzamy, że dla $k = 3$ istnieją 333 kolorowania.

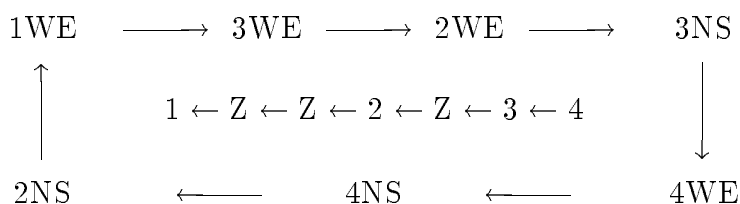
Przykład 9. Grupa wszystkich izometrii sześcianu składa się z 48 przekształceń. Wśród tych permutacji zbioru wierzchołków jest jedna mająca 8 cykli, 6 mających 6 cykli, 21 mających 4 cykle i 20 mających 2 cykle. Zatem liczba kolorowań rozróżnialnych ze względu na grupę wszystkich izometrii jest równa

$$\frac{1}{48} \cdot (k^8 + 6k^6 + 21k^4 + 20k^2).$$

Dla $k = 2$ istnieją 22 kolorowania, dla $k = 3$ istnieje 267 kolorowań.

Turnieje Howella

Przypuśćmy, że osiem par brydżowych chce rozegrać turniej. Chcą przy tym, by każda para zagrała przeciwko każdej innej parze. Jednym ze sposobów rozegrania takiego turnieju jest wykorzystanie tzw. kart pilotujących Howella (od nazwiska matematyka, który pierwszy zaproponował użycie takich kart). Oto przykład karty pilotującej do turnieju Howella dla ośmiu par.



Turniej jest rozgrywany na czterech stołach, o numerach od 1 do 4. Na każdym stole grają dwie pary: jedna na linii NS, druga na linii WE. Siedem par (o numerach od 1 do 7) otrzymuje takie karty, każda z zaznaczoną inną pozycją startową:

1	1 WE
2	2 NS
3	4 NS
4	4 WE
5	3 NS
6	2 WE
7	3 WE

Para numer 8 nie otrzymuje karty pilotującej; zajmuje ona miejsce na linii NS na stole 1 i nie zmienia swojej pozycji przez cały czas trwania turnieju. Pozostałe pary przechodzą w kolejnych rundach na następne miejsce na swojej karcie pilotującej. I tak na przykład w drugiej rundzie pary o numerach od 1 do 7 przejdą na następujące pozycje:

1	1 WE	→	3 WE
2	2 NS	→	1 WE
3	4 NS	→	2 NS
4	4 WE	→	4 NS
5	3 NS	→	4 WE
6	2 WE	→	3 NS
7	3 WE	→	2 WE

W następnych rundach pary poruszają się według tego samego schematu. W tym samym czasie pudełka z kartami również zmieniają swoje położenia. Oprócz czterech stolików,

na których są rozgrywane kolejne rozdania, sędzia ustawia trzy dodatkowe stoliki, zwane zbiornicami. Na tych stolikach znajdują się pudełka z rozdaniem, które w danej rundzie nie są rozgrywane. Dwie zbiornice znajdują się między stolikami o numerach 1 i 2, trzecia między stolikami o numerach 2 i 3. Karty w kolejnych rundach są przenoszone w kierunku malejących numerów stolików, uwzględniając zbiornice (oraz ze stolika 1 na stolik 4). Na początku karty zajmują następujące pozycje:

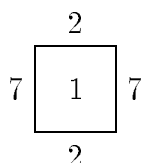
rozdanie 1	stolik 1
rozdanie 2	zbiornica
rozdanie 3	zbiornica
rozdanie 4	stolik 2
rozdanie 5	zbiornica
rozdanie 6	stolik 3
rozdanie 7	stolik 4

W następnej rundzie zajmą pozycje:

rozdanie 1	stolik 4
rozdanie 2	stolik 1
rozdanie 3	zbiornica
rozdanie 4	zbiornica
rozdanie 5	stolik 2
rozdanie 6	zbiornica
rozdanie 7	stolik 3

W następnych rundach rozdania będą przemieszczać się według tego samego schematu. A oto przebieg całego turnieju. W kolejnych wierszach tabeli mamy podane pozycje par i kart w kolejnych rundach. Wewnątrz kwadratu znajduje się numer rozdania rozgrywanego w danej rundzie na danym stole. Liczby nad i pod kwadratem oznaczają numer pary grającej na linii NS, z lewej i prawej strony – numer pary grającej na linii WE.

I tak oznaczenie



wskazuje, że na danym stoliku para 2 gra na linii NS przeciwko parze 7 grającej na linii WE; rozgrywane jest rozdanie numer 1.

Przebieg turnieju.

Stół 1	Stół 4	Stół 3	Z	Stół 2	Z	Z
1 8 1 8 1	4 3 7 3 4	7 5 6 5 7	5	6 2 4 2 6	3	2
2 8 2 8 2	5 4 1 4 5	1 6 7 6 1	6	7 3 5 3 7	4	3
3 8 3 8 3	6 5 2 5 6	2 7 1 7 2	7	1 4 6 4 1	5	4
4 8 4 8 4	7 6 3 6 7	3 1 2 1 3	1	2 5 7 5 2	6	5
5 8 5 8 5	1 7 4 7 1	4 2 3 2 4	2	3 6 1 6 3	7	6
6 8 6 8 6	2 1 5 1 2	5 3 4 3 5	3	4 7 2 7 4	1	7
7 8 7 8 7	3 2 6 2 3	6 4 5 4 6	4	5 1 3 1 5	2	1

Można zauważyć, że karta pilotująca jest skonstruowana w taki sposób, by każda para zagrała przeciwko każdej innej parze dokładnie jeden raz i by każda para zagrała każde rozdanie dokładnie jeden raz. Karta pilotująca ma jeszcze jedną własność, której teraz się przyjrzymy. Popatrzmy najpierw na dzieje rozdania numer 6.

Runda	Stół	para NS	para WE
1	3	5	7
2	Z	—	—
3	2	4	1
4	Z	—	—
5	Z	—	—
6	1	8	6
7	4	2	3

Protokół turniejowy tego rozdania może wyglądać następująco:

Nr	NS	WE	Kontrakt	Rozgr.	Lew	NS	WE	NS	WE
3	5	7	3♠	N	9	140		3	3
2	4	1	4♠	S	10	420		6	0
1	8	6	3♠	S	9	140		3	3
4	2	3	4♠	N	9		50	0	6

W pierwszej kolumnie zapisany jest numer stołu, na którym to rozdanie było rozgrywane. W dwóch następnych kolumnach zapisane są numery par grających to rozdanie. W następnych trzech kolumnach zapisany jest wylicytowany kontrakt, oznaczenie rozgrywającego oraz liczba lew. W kolejnych dwóch kolumnach zapisana jest wartość osiągniętego kontraktu. Te wszystkie kolumny wypełniają grzeczne po rozegraniu rozdania.

Ostatnie dwie kolumny są przeznaczone na wynik i wypełnia je sędzia turnieju. W kolumnie NS wpisywany jest wynik dla pary grającej na linii NS. Za każdy wynik (innej pary) gorszy od uzyskanego przez daną parę ta para otrzymuje 2 punkty; za jednakowy otrzymuje 1 punkt. I tak para numer 4 otrzymuje 6 punktów: po 2 punkty za wyniki gorsze (140, 140, −50). Para numer 5 otrzymuje 3 punkty: 2 punkty za wynik gorszy (−50) i 1 punkt za wynik jednakowy (140). Tyle samo punktów uzyskuje para numer 8. Wreszcie para numer 2 uzyskuje 0 punktów, bo wszystkie pary uzyskały wyniki lepsze od niej.

Podobnie przyznaje się punkty parom grającym na linii WE. Można zauważyć, że suma punktów przyznanych parom grającym na tym samym stole jest zawsze równa 6. Punkty uzyskane w ten sposób we wszystkich rozdaniach dodaje się i otrzymane sumy decydują o miejscu w turnieju. Ten sposób punktacji nie jest najlepszy w przypadku tak małego turnieju, ale jest najprostszy i najlepiej pokazuje istotę turnieju brydżowego. Pary grające dane rozdanie na linii NS są porównywane między sobą; podobnie pary grające na linii WE.

Ostatnia wspomniana wcześniej własność karty pilotującej polega na tym, że każde dwie pary są ze sobą porównywane w tej samej liczbie rozdań. Na przykład, pary 7 i 5 są porównywane ze sobą trzy razy:

1. w rozdaniu 2 obie grają na linii NS (para 7 w rundzie 6, para 5 w rundzie 3);
2. w rozdaniu 3 obie grają na linii WE (para 7 w rundzie 4; para 5 w rundzie 7);
3. w rozdaniu 7 obie grają na linii NS (para 7 w rundzie 7; para 5 w rundzie 4).

Podobnie pary 2 i 6 są porównywane ze sobą trzy razy:

1. w rozdaniu 3 obie grają na linii NS (para 2 w rundzie 5, para 6 w rundzie 4);
2. w rozdaniu 5 obie grają na linii WE (para 2 w rundzie 6; para 6 w rundzie 7);
3. w rozdaniu 6 obie grają na linii NS (para 2 w rundzie 7; para 6 w rundzie 6).

Mówimy, że turniej jest całkowicie zrównoważony, gdy każde dwie pary są porównywane ze sobą tę samą liczbę razy.

Przypuśćmy teraz, że n par brydżowych chce rozegrać podobny turniej. Czy istnieje karta pilotująca Howella dla n par? Chcemy, by zachowane były następujące warunki:

- (1) w turnieju rozgrywa się $n - 1$ rund;
- (2) w każdej rundzie na każdym z $\frac{n}{2}$ stołów jest rozgrywane jedno rozdanie, grają je dwie pary: jedna na linii NS, druga na linii WE;
- (3) każda para gra przeciwko każdej innej parze dokładnie jeden raz;
- (4) każda para gra każde rozdanie dokładnie jeden raz;
- (5) każde dwie pary grają tę samą liczbę rozdań na tej samej linii.

Z warunku (2) wynika, że liczba par jest parzysta: $n = 2m$, gdzie m jest liczbą stołów, na których są rozgrywane rozdania. W każdym rozdaniu m par gra na linii NS i m par gra na linii WE. Zatem $\binom{m}{2}$ par jest porównywanych ze sobą na każdej z tych linii; łącznie zatem w jednym rozdaniu mamy $2 \cdot \binom{m}{2} = m(m - 1)$ porównań. Ponieważ w turnieju mamy $2m - 1$ rozdań, więc łączna liczba porównań par w całym turnieju wynosi $m(m - 1)(2m - 1)$.

Niech teraz k będzie liczbą porównań każdych dwóch par: z warunku (5) wynika, że dla każdych dwóch par ta liczba jest taka sama. Mamy zatem $\binom{2m}{2} = m(2m - 1)$ par, czyli łączna liczba porównań wynosi $km(2m - 1)$. Stąd wynika, że

$$m(m - 1)(2m - 1) = km(2m - 1),$$

czyli

$$k = m - 1.$$

To znaczy, że dowolne dwie pary rozgrywają ze sobą $m - 1$ rozdań na tej samej linii i m rozdań na przeciwnych liniach.

Udowodnimy teraz, że liczba n jest podzielna przez 4.

Każde z $2m - 1$ rozdań dzieli zbiór X wszystkich par na dwa podzbiory rozłączne. Dla rozdania o numerze i mamy

A_i^0 = zbiór par grających rozdanie i na linii NS;

A_i^1 = zbiór par grających rozdanie i na linii WE.

Mamy zatem

$$A_i^0 \cap A_i^1 = \emptyset, \quad A_i^0 \cup A_i^1 = X, \quad |A_i^0| = |A_i^1| = m.$$

Każda para p należy do dokładnie $2m - 1$ zbiorów A_i^ε ($i = 1, 2, \dots, 2m - 1, \varepsilon = 0, 1$):

$$\left| \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \right\} \right| = 2m - 1.$$

Warunek (5) można wysłowić w sposób następujący: dla dowolnych dwóch par p i q mamy

$$\left| \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \wedge q \in A_i^\varepsilon \right\} \right| = m - 1.$$

Niech p, q i r będą trzema dowolnymi parami. Definiujemy teraz cztery zbiory:

$$B = \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \wedge q \in A_i^\varepsilon \wedge r \in A_i^\varepsilon \right\}$$

$$C = \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \wedge q \notin A_i^\varepsilon \wedge r \in A_i^\varepsilon \right\}$$

$$D = \left\{ (i, \varepsilon) : p \notin A_i^\varepsilon \wedge q \in A_i^\varepsilon \wedge r \in A_i^\varepsilon \right\}$$

$$E = \left\{ (i, \varepsilon) : p \notin A_i^\varepsilon \wedge q \notin A_i^\varepsilon \wedge r \in A_i^\varepsilon \right\}$$

Oczywiście zbiory B, C, D i E są parami rozłączne. Niech

$$|B| = b, \quad |C| = c, \quad |D| = d, \quad |E| = e.$$

Zauważmy następnie, że

$$B \cup C = \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \wedge r \in A_i^\varepsilon \right\}$$

oraz

$$B \cup D = \left\{ (i, \varepsilon) : q \in A_i^\varepsilon \wedge r \in A_i^\varepsilon \right\}.$$

Stąd wynika, że

$$b + c = b + d = m - 1,$$

czyli

$$c = d = m - 1 - b.$$

Następnie

$$B \cup C \cup D \cup E = \left\{ (i, \varepsilon) : r \in A_i^\varepsilon \right\}.$$

Zatem

$$b + (m - 1 - b) + (m - 1 - b) + e = 2m - 1,$$

czyli

$$e = b + 1.$$

Stąd wynika, że

$$|B \cup E| = 2b + 1.$$

Definiujemy jeszcze jeden zbiór:

$$E' = \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \wedge q \in A_i^\varepsilon \wedge r \notin A_i^\varepsilon \right\}.$$

Można łatwo zauważyć, że

$$(i, \varepsilon) \in E \Leftrightarrow (i, 1 - \varepsilon) \in E'.$$

Stąd wynika, że $|E| = |E'|$. Ponieważ zbiory E i E' są rozłączne ze zbiorem B , więc

$$|B \cup E| = |B \cup E'|.$$

Ale

$$B \cup E' = \left\{ (i, \varepsilon) : p \in A_i^\varepsilon \wedge q \in A_i^\varepsilon \right\},$$

skąd wynika, że

$$|B \cup E'| = m - 1.$$

Zatem

$$2b + 1 = m - 1,$$

czyli

$$m = 2b + 2,$$

a więc liczba m jest parzysta. To znaczy, że liczba n jest podzielna przez 4.

Udowodnimy teraz, że jeśli liczba n jest podzielna przez 4 oraz liczba $p = n - 1$ jest pierwsza, to można zorganizować turniej spełniający warunki (1) – (5). Okaze się też, że sposób zmiany miejsc przez pary i zmiany rozdań da się opisać za pomocą karty pilotującej.

Żałóżmy więc, że $p > 3$ jest liczbą pierwszą oraz $p \equiv 3 \pmod{4}$. Wykażemy, że istnieje karta pilotująca Howella dla $n = p + 1$ par.

Niech a będzie dowolną liczbą niepodzielną przez p . Przypominamy, że liczbę a nazywamy resztą kwadratową modulo p , jeśli istnieje liczba całkowita x taka, że

$$x^2 \equiv a \pmod{p}.$$

Jeśli taka liczba x nie istnieje, to liczbę a nazywamy nieresztą kwadratową modulo p . W dalszym ciągu będziemy używać symbolu Legendre'a:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{jeśli } a \text{ jest resztą kwadratową modulo } p; \\ -1 & \text{jeśli } a \text{ jest nieresztą kwadratową modulo } p. \end{cases}$$

Zauważmy najpierw, że z twierdzenia Eulera wynika, że $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$, a więc -1 jest nieresztą kwadratową modulo p . Stąd wynika, że dla dowolnej liczby a takiej, że $0 < a < p$ mamy:

$$\left(\frac{-a}{p}\right) = -\left(\frac{a}{p}\right),$$

czyli

$$a \text{ jest resztą kwadratową modulo } p \iff -a \text{ jest nieresztą kwadratową modulo } p.$$

Definiujemy $\alpha = \frac{p+5}{4}$. Oczywiście α jest liczbą całkowitą. Proste obliczenia pokazują, że

$$\alpha \not\equiv 1 \pmod{p} \quad \text{oraz} \quad \alpha \not\equiv -1 \pmod{p}.$$

Zatem $\alpha - 1 \neq 0$ oraz $\alpha + 1 \neq 0$ w ciele $\mathbb{Z}_p$.

Zauważmy następnie, że

$$4(\alpha - 1) = p + 1 \quad \text{oraz} \quad 4(\alpha + 1) = p + 9.$$

Stąd wynika, że

$$\begin{aligned} 4(\alpha - 1) &\equiv 1 \pmod{p}, \\ \left(\frac{4(\alpha - 1)}{p}\right) &= 1, \\ \left(\frac{4}{p}\right) \cdot \left(\frac{\alpha - 1}{p}\right) &= 1, \\ \left(\frac{\alpha - 1}{p}\right) &= 1. \end{aligned}$$

Podobnie

$$\begin{aligned} 4(\alpha + 1) &\equiv 9 \pmod{p}, \\ \left(\frac{4(\alpha + 1)}{p}\right) &= \left(\frac{9}{p}\right) = 1, \\ \left(\frac{4}{p}\right) \cdot \left(\frac{\alpha + 1}{p}\right) &= 1, \\ \left(\frac{\alpha + 1}{p}\right) &= 1. \end{aligned}$$

Zatem $\alpha - 1$ i $\alpha + 1$ są resztami kwadratowymi modulo p . Stąd też $\alpha^2 - 1$ jest resztą kwadratową modulo p .

Definiujemy teraz zbiory:

$$\begin{aligned} X &= \{0, 1, \dots, p-1, p\} \quad \text{zbiór numerów par,} \\ Y &= \{0, 1, \dots, p-1\} \quad \text{zbiór numerów rozdań,} \\ R &= \{0, 1, \dots, p-1\} \quad \text{zbiór numerów rund,} \\ S &= \{0, 1, \dots, p-1\} \quad \text{zbiór numerów stołów,} \\ L &= \{-1, +1\} \quad \text{zbiór oznaczeń linii (+1 oznacza linię NS, -1 oznacza linię WE).} \end{aligned}$$

Mamy zatem $n = p + 1$ par numerowanych liczbami od 0 do p oraz p rozdań numerowanych liczbami od 0 do $p-1$. Wszystkie rozdania są rozgrywane w rundach, w każdej rundzie grają wszystkie pary. Mamy p rund, numerowanych liczbami od 0 do $p-1$. Mamy następnie p stołów, numerowanych liczbami od 0 do $p-1$. W każdej rundzie pary grają przy $\frac{p+1}{2}$ stołach, pozostałe stoły są wolne. Na tych stołach jednak znajdują się karty; są to zbiornice. Okaze się, że numery zbiornic są stałe: nie zależą od rundy.

Definiujemy teraz trzy funkcje:

$$\begin{aligned} T &: Y \times R \rightarrow S, \\ t &: X \times R \rightarrow S, \\ s &: X \times R \rightarrow L. \end{aligned}$$

Jeśli $x \in X$, $y \in Y$ oraz $r \in R$, to:

$$\begin{aligned} T(y, r) &= \text{numer stołu, na którym rozdanie } y \text{ jest grane w rundzie } r, \\ t(x, r) &= \text{numer stołu, na którym para } x \text{ gra w rundzie } r, \\ s(x, r) &= \text{oznaczenie linii, na której para } x \text{ gra w rundzie } r. \end{aligned}$$

A oto definicje tych funkcji:

$$T(y, r) = r - y.$$

$$t(x, r) = \begin{cases} 0 & \text{jeśli } x = p \text{ lub } x = r; \\ \frac{x-r}{\alpha-1} & \text{jeśli } x-r \text{ jest resztą kwadratową modulo } p; \\ \frac{r-x}{\alpha+1} & \text{jeśli } r-x \text{ jest resztą kwadratową modulo } p. \end{cases}$$

$$s(x, r) = \begin{cases} +1 & \text{jeśli } x = p; \\ -1 & \text{jeśli } x = r; \\ +1 & \text{jeśli } x-r \text{ jest resztą kwadratową modulo } p; \\ -1 & \text{jeśli } r-x \text{ jest resztą kwadratową modulo } p. \end{cases}$$

Wszystkie działania w tej definicji są wykonywane w ciele $\mathbb{Z}_p$.

Zauważmy, że albo $t(x, r) = 0$, albo $t(x, r)$ jest resztą kwadratową modulo p . Rozdania rozgrywane są zatem na stole o numerze 0 i na stołach, których numery są resztami kwadratowymi modulo p . Zauważmy, że istnieje dokładnie $\frac{n}{2}$ stołów, przy których rozgrywane są kolejne rozdania; są to stoły o tych samych numerach w każdej rundzie. Numery stołów, na których nie rozgrywa się rozdań (czyli zbiornic), są nieresztami kwadratowymi modulo p .

Przypuśćmy teraz, że dany jest numer stołu t_0 i numer rundy r_0 . W tej rundzie na stole t_0 znajduje się rozdanie $y_0 = r_0 - t_0$. Mianowicie

$$T(y_0, r_0) = r_0 - y_0 = r_0 - (r_0 - t_0) = t_0.$$

Ponieważ liczba rozdań jest równa liczbie stołów, więc w każdej rundzie na każdym stole znajduje się dokładnie jedno rozdanie.

Wykażemy teraz, że w każdej rundzie na każdym stole, którego numer nie jest nieresztą kwadratową modulo p , spotkają się dokładnie dwie pary. Niech więc dany będzie numer stołu t_0 i numer rundy r_0 .

Przypuśćmy najpierw, że $t_0 = 0$. Z definicji funkcji t wynika, że na stole o numerze 0 w rundzie r_0 mogą grać tylko dwie pary o numerach p i r_0 . Z definicji funkcji s wynika, że para o numerze p gra na linii NS, a para o numerze r_0 gra na linii WE.

Niech teraz $t_0 \neq 0$. Zatem t_0 jest resztą kwadratową modulo p . Przypuśćmy, że para o numerze x gra w rundzie r_0 na stole o numerze t_0 . Oczywiście wtedy $x \neq p$ oraz $x \neq r_0$. Możliwe są teraz dwa przypadki:

(1) $x - r_0$ jest resztą kwadratową modulo p . Wtedy

$$t_0 = \frac{x - r_0}{\alpha - 1},$$

czyli

$$x = r_0 + t_0(\alpha - 1).$$

Ponadto $s(x, r_0) = +1$.

(2) $r_0 - x$ jest resztą kwadratową modulo p . Wtedy

$$t_0 = \frac{r_0 - x}{\alpha + 1},$$

czyli

$$x = r_0 - t_0(\alpha + 1).$$

Ponadto $s(x, r_0) = -1$.

Proste obliczenia pokazują, że te dwie pary rzeczywiście grają w rundzie r_0 na stole o numerze t_0 .

Tak więc w rundzie r_0 na stole o numerze t_0 grają dwie pary:

$$x_0 = r_0 + t_0(\alpha - 1) \quad \text{na linii NS}$$

oraz

$$x_1 = r_0 - t_0(\alpha + 1) \quad \text{na linii WE.}$$

Wykażemy teraz, że każda para gra przeciwko każdej innej parze. Ponieważ w każdej rundzie każda para gra przeciwko dokładnie jednej parze i liczba rund jest równa liczbie par, więc wyniknie stąd, że każde dwie pary grają przeciwko sobie dokładnie jeden raz.

Niech zatem będą dane dwie pary o numerach x_0 i x_1 . Definiujemy liczbę r wzorami:

$$r = \begin{cases} x_0 & \text{jeśli } x_1 = p; \\ x_1 & \text{jeśli } x_0 = p; \\ \frac{x_1 + x_0}{2} + \frac{x_1 - x_0}{2\alpha} & \text{jeśli } \frac{x_1 - x_0}{2\alpha} \text{ jest resztą kwadratową modulo } p; \\ \frac{x_1 + x_0}{2} + \frac{x_0 - x_1}{2\alpha} & \text{jeśli } \frac{x_0 - x_1}{2\alpha} \text{ jest resztą kwadratową modulo } p. \end{cases}$$

Pozostawimy jako proste ćwiczenie wykazanie, że w rundzie r pary x_0 i x_1 grają na tym samym stole, jedna na linii NS, druga na linii WE.

Następnie wykazujemy, że każda para gra każde rozdanie. Ponieważ liczba rund jest równa liczbie rozdań, więc z tego wyniknie, że każda para gra każde rozdanie dokładnie jeden raz.

Niech zatem dana będzie para o numerze x_0 i rozdanie o numerze y_0 . Definiujemy liczbę r wzorami:

$$r = \begin{cases} y_0 & \text{jeśli } x_0 = p \text{ lub } x_0 = y_0; \\ y_0 + \frac{y_0 - x_0}{\alpha} & \text{jeśli } \frac{y_0 - x_0}{\alpha} \text{ jest resztą kwadratową modulo } p; \\ y_0 + \frac{x_0 - y_0}{\alpha} & \text{jeśli } \frac{x_0 - y_0}{\alpha} \text{ jest resztą kwadratową modulo } p. \end{cases}$$

Proste ćwiczenie pokazuje, że w rundzie r para o numerze x_0 i rozdanie o numerze y_0 znajdują się na tym samym stole, a więc para x_0 gra rozdanie y_0 .

Wreszcie wykażemy, że każde dwie pary grają tę samą liczbę rozdań na tej samej linii. Wprowadzamy w tym celu nową funkcję

$$S : X \times Y \rightarrow L,$$

zdefiniowaną w następujący sposób:

$$S(x, y) = \text{linia, na której para } x \text{ gra rozdanie } y.$$

Niech będzie dana para o numerze x i rozdanie o numerze y . Wiemy już, że para x gra rozdanie y w rundzie r , gdzie

$$r = \begin{cases} y_0 & \text{jeśli } x_0 = p \text{ lub } x_0 = y_0; \\ y_0 + \frac{y_0 - x_0}{\alpha} & \text{jeśli } \frac{y_0 - x_0}{\alpha} \text{ jest resztą kwadratową modulo } p; \\ y_0 + \frac{x_0 - y_0}{\alpha} & \text{jeśli } \frac{x_0 - y_0}{\alpha} \text{ jest resztą kwadratową modulo } p. \end{cases}$$

Wtedy

$$S(x, y) = s(x, r),$$

skąd łatwo dostajemy wzór

$$S(x, y) = \begin{cases} +1 & \text{jeśli } x = p; \\ -1 & \text{jeśli } x = y; \\ +1 & \text{jeśli } \frac{x - y}{\alpha} \text{ jest resztą kwadratową modulo } p; \\ -1 & \text{jeśli } \frac{x - y}{\alpha} \text{ jest nieresztą kwadratową modulo } p. \end{cases}$$

Inaczej mówiąc:

$$S(x, y) = \begin{cases} +1 & \text{jeśli } x = p; \\ -1 & \text{jeśli } x = y; \\ \left(\frac{(x - y)\alpha^{-1}}{p} \right) & \text{jeśli } x \neq p \text{ oraz } x \neq y. \end{cases}$$

Przyjmijmy teraz, że $\left(\frac{0}{p}\right) = 0$. Mamy wówczas następującą własność symbolu Legendre'a:

$$\sum_{y=0}^{p-1} \left(\frac{y}{p}\right) = 0.$$

Wynika ona stąd, że $\left(\frac{0}{p}\right) = 0$ oraz w zbiorze $\{1, 2, \dots, p-1\}$ jest tyle samo reszt kwadratowych modulo p co niereszt kwadratowych modulo p . Stąd otrzymujemy wniosek:

$$\sum_{y=0}^{p-1} \left(\frac{x-y}{p}\right) = 0.$$

Ta równość wynika natychmiast z poprzedniej, gdyż jeśli y przebiega wszystkie liczby od 0 do $p-1$, to $x-y$ przebiega (w ciele $\mathbb{Z}_p$) ten sam zbiór liczb. Zatem

$$\sum_{y=0}^{p-1} \left(\frac{x-y}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) = 0.$$

Wreszcie udowodnimy ważny lemat.

Lemat. Jeśli $a \neq 0$, to

$$\sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \cdot \left(\frac{y+a}{p}\right) = -1.$$

Dowód. Zauważmy najpierw, że

$$\sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \cdot \left(\frac{y+a}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{y(y+a)}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{y^2(1+ay^{-1})}{p}\right) = \sum_{y=1}^{p-1} \left(\frac{1+ay^{-1}}{p}\right).$$

Zauważmy następnie, że jeśli y przebiega liczby od 1 do $p-1$, to $1+ay^{-1}$ przebiega (w ciele $\mathbb{Z}_p$) wszystkie liczby różne od 1. Zatem

$$\sum_{y=1}^{p-1} \left(\frac{1+ay^{-1}}{p}\right) = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) - \left(\frac{1}{p}\right) = -1,$$

co kończy dowód lematu.

Warunek, że dowolne dwie pary grają tę samą liczbę rozdań na tej samej linii, jest równoważny równości

$$\sum_{y=0}^{p-1} S(x_1, y) \cdot S(x_2, y) = -1$$

dla dowolnych x_1 i x_2 takich, że $x_1 \neq x_2$. Udowodnimy teraz tę równość. Możliwe są dwa przypadki.

Jeśli jedna z liczb x_1 lub x_2 jest równa p , to nasza równość przybiera postać

$$\sum_{y=0}^{p-1} S(x, y) \cdot S(p, y) = -1$$

dla $x \neq p$. Ale $S(p, y) = +1$. Mamy więc dowieść, że

$$\sum_{y=0}^{p-1} S(x, y) = -1.$$

Ale

$$\begin{aligned} \sum_{y=0}^{p-1} S(x, y) &= \sum_{y \neq x} S(x, y) + S(x, x) = \sum_{y=0}^{p-1} \left(\frac{(x-y)\alpha^{-1}}{p} \right) - 1 = \\ &= \left(\frac{\alpha^{-1}}{p} \right) \cdot \sum_{y \neq x} \left(\frac{x-y}{p} \right) - 1 = \left(\frac{\alpha^{-1}}{p} \right) \cdot \sum_{y=0}^{p-1} \left(\frac{x-y}{p} \right) - 1 = \\ &= -1. \end{aligned}$$

Jeśli zaś obie liczby x_1 i x_2 są różne od p , to

$$\begin{aligned} \sum_{y=0}^{p-1} S(x_1, y) \cdot S(x_2, y) &= \\ &= \sum_{y \neq x_1, x_2} S(x_1, y) \cdot S(x_2, y) + S(x_1, x_1) \cdot S(x_2, x_1) + S(x_1, x_2) \cdot S(x_2, x_2) = \\ &= \sum_{y \neq x_1, x_2} S(x_1, y) \cdot S(x_2, y) - S(x_2, x_1) - S(x_1, x_2) = \\ &= \sum_{y \neq x_1, x_2} S(x_1, y) \cdot S(x_2, y), \end{aligned}$$

gdyż $S(x_1, x_2) = -S(x_2, x_1)$. Jeśli $x \neq y$, to

$$S(x, y) = \left(\frac{(x-y)\alpha^{-1}}{p} \right).$$

Zatem

$$\begin{aligned}
\sum_{y=0}^{p-1} S(x_1, y) \cdot S(x_2, y) &= \sum_{y \neq x_1, x_2} \left(\frac{(x_1 - y)\alpha^{-1}}{p} \right) \cdot \left(\frac{(x_2 - y)\alpha^{-1}}{p} \right) \\
&= \left(\frac{\alpha^{-2}}{p} \right) \cdot \sum_{y=0}^{p-1} \left(\frac{x_1 - y}{p} \right) \cdot \left(\frac{x_2 - y}{p} \right) \\
&= \sum_{y=0}^{p-1} \left(\frac{x_1 - y}{p} \right) \cdot \left(\frac{x_2 - y}{p} \right) \\
&= \sum_{y=0}^{p-1} \left(\frac{y}{p} \right) \cdot \left(\frac{y + (x_2 - x_1)}{p} \right) \\
&= -1.
\end{aligned}$$

W ten sposób dowiedliśmy, że każde dwie pary grają tę samą liczbę rozdań na tej samej linii. Pozostaje tylko pokazać konstrukcję karty pilotującej.

Zauważamy najpierw, że każde rozdanie w następnej rundzie przechodzi na stół o numer o 1 większy (ze stolika $p - 1$ na stół o numerze 0). Można łatwo pokazać, że pary poruszają się według następującego schematu:

$$(0, +1) \rightarrow (0, +1),$$

czyli para grająca na stoliku o numerze 0 na linii NS pozostaje w tym samym miejscu;

$$(0, -1) \rightarrow ((\alpha + 1)^{-1}, -1),$$

czyli para grająca na stoliku o numerze 0 na linii WE , przenosi się na stół o numerze $(\alpha + 1)^{-1}$ na linię WE . Wreszcie dla $t \neq 0$ mamy

$$(t, +1) \rightarrow \begin{cases} \left(\frac{1 - t(\alpha - 1)}{\alpha + 1}, -1 \right) & \text{jeśli } 1 - t(\alpha - 1) = 0 \text{ lub } \left(\frac{1 - t(\alpha - 1)}{p} \right) = 1 \\ \left(t - (\alpha - 1)^{-1}, +1 \right) & \text{jeśli } \left(\frac{1 - t(\alpha - 1)}{p} \right) = -1 \end{cases}$$

oraz

$$(t, -1) \rightarrow \begin{cases} \left(t + (\alpha + 1)^{-1}, +1 \right) & \text{jeśli } \left(\frac{1 + t(\alpha + 1)}{p} \right) = 1 \\ \left(\frac{-1 - t(\alpha + 1)}{\alpha - 1}, -1 \right) & \text{jeśli } \left(\frac{1 + t(\alpha + 1)}{p} \right) = -1. \end{cases}$$

Przykład

Niech $p = 7$. Zatem w turnieju uczestniczy $n = p + 1 = 8$ par. Mamy wówczas w ciele $\mathbb{Z}_7$ następujące reszty i niereszty kwadratowe:

$$\begin{array}{ll} \text{reszty kwadratowe:} & 1, 2, 4; \\ \text{niereszty kwadratowe:} & 3, 5, 6. \end{array}$$

Przydatna będzie również tablica elementów odwrotnych modulo 7:

$$\begin{array}{l} 1^{-1} = 1; \\ 2^{-1} = 4; \\ 3^{-1} = 5; \\ 4^{-1} = 2; \\ 5^{-1} = 3; \\ 6^{-1} = 6. \end{array}$$

Przystępujemy teraz do konstrukcji karty pilotującej turnieju Howella dla 8 par. Najpierw definiujemy

$$\alpha = \frac{p+5}{4} = 3.$$

Mamy wówczas

$$\alpha - 1 = 2, \quad (\alpha - 1)^{-1} = 4$$

oraz

$$\alpha + 1 = 4, \quad (\alpha + 1)^{-1} = 2.$$

Gra toczy się na stole o numerze 0 i na stołach, których numery są resztami kwadratowymi modulo 7. Zatem są to stoły o numerach: 0, 1, 2, 4. Stoły o numerach 3, 5 i 6 są zbiornicami. Karty w kolejnych rundach przechodzą na stół o numerze o 1 większym, czyli ze stołu o numerze i na stół o numerze $i + 1$, przy czym dodawanie jest brane modulo 7. Zatem karty poruszają się według schematu:

$$\rightarrow 0 \rightarrow 1 \rightarrow 2 \rightarrow Z \rightarrow 4 \rightarrow Z \rightarrow Z \rightarrow$$

Zajmiemy się teraz sposobem poruszania się par. Para numer 8 przez cały czas turnieju zajmuje miejsce przy stole 0, na linii NS. Reguły poruszania się pozostałych par mają

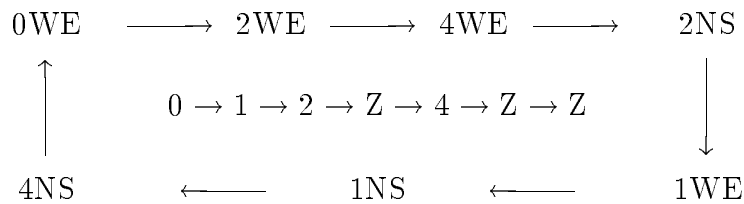
postać:

$$\begin{aligned}
(0, +1) &\rightarrow (0, +1), \\
(0, -1) &\rightarrow (2, -1), \\
(t, +1) &\rightarrow \begin{cases} (3t+2, -1) & \text{jeśli } 5t+1 = 0 \text{ lub } \left(\frac{5t+1}{p}\right) = 1 \\ (t+3, +1) & \text{jeśli } \left(\frac{5t+1}{p}\right) = -1 \end{cases}, \\
(t, -1) &\rightarrow \begin{cases} (t+2, -1) & \text{jeśli } \left(\frac{4t+1}{p}\right) = 1 \\ (5t+3, +1) & \text{jeśli } \left(\frac{4t+1}{p}\right) = -1. \end{cases}
\end{aligned}$$

Zatem

$$\begin{aligned}
(0, +1) &\rightarrow (0, +1), \\
(0, -1) &\rightarrow (2, -1), \\
(1, +1) &\rightarrow (4, +1), & \text{bo 6 jest nieresztą kwadratową,} \\
(1, -1) &\rightarrow (1, +1), & \text{bo 5 jest nieresztą kwadratową,} \\
(2, +1) &\rightarrow (1, -1), & \text{bo 4 jest resztą kwadratową,} \\
(2, -1) &\rightarrow (4, -1), & \text{bo 2 jest resztą kwadratową,} \\
(4, +1) &\rightarrow (0, -1), & \text{bo } 7 \mid 5 \cdot 4 + 1, \\
(4, -1) &\rightarrow (2, +1), & \text{bo 3 jest nieresztą kwadratową.}
\end{aligned}$$

Ostatecznie karta pilotująca dla par ma postać



Poniższa tabela pokazuje przebieg turnieju. Przenumerujemy teraz pary i stoliki, tak by zgodnie z tradycją brydżową, spełnione były następujące warunki:

- (1) karty poruszają się na stół o numer niższy,
- (2) pary przychodzą do stolika 1 na linię WE w kolejności numerów od 1 do 7,
- (3) para numer 8 siedzi przez cały czas turnieju przy stoliku 1 na linii NS.

Po tym przenumerowaniu otrzymujemy dokładnie tę samą kartę pilotującą, którą widzieliśmy na początku.

Przebieg turnieju.

Stół 0	Stół 1	Stół 2	Stół 3	Stół 4	Stół 5	Stół 6
0 7 0 7 0	3 2 6 2 3	6 4 5 4 6	4	5 1 3 1 5	2	1
1 7 1 7 1	4 3 0 3 4	0 5 6 5 0	5	6 2 4 2 6	3	2
2 7 2 7 2	5 4 1 4 5	1 6 0 6 1	6	0 3 5 3 0	4	3
3 7 3 7 3	6 5 2 5 6	2 0 1 0 2	0	1 4 6 4 1	5	4
4 7 4 7 4	0 6 3 6 0	3 1 2 1 3	1	2 5 0 5 2	6	5
5 7 5 7 5	1 0 4 0 1	4 2 3 2 4	2	3 6 1 6 3	0	6
6 7 6 7 6	2 1 5 1 2	5 3 4 3 5	3	4 0 2 0 4	1	0

Wskazówki bibliograficzne.

Przykłady kart pilotujących do turniejów Howella można znaleźć w [3]. Pojęcie turnieju całkowicie zrównoważonego jest wzięte z [4]. Tam też znajduje się dowód twierdzenia mówiącego, że jeśli istnieje turniej całkowicie zrównoważony, to liczba par jest podzielna przez 4. Parker i Mood podają kilka przykładów kart pilotujących, pisząc jednak wyraźnie, że nie znają żadnej metody ogólnej konstruowania takich kart. Przedstawiona w tekście konstrukcja karty pilotującej pochodzi od Berlekampa i Hwanga [1]. Tam też znajduje się dowód twierdzenia ogólniejszego, mówiącego, że jeśli liczba n jest podzielna przez 4 i $n - 1$ jest potęgą liczby pierwszej, to istnieje turniej całkowicie zrównoważony dla n par. Więcej informacji o istnieniu tzw. rotacji Howella i blisko z nimi związanymi kwadratami Rooma można znaleźć w [2].

- [1] E. R. Berlekamp, F. K. Hwang, Constructions for Balanced Howell Rotations for Bridge Tournaments, *J. Combin. Theory A*, 12 (1972), 159 – 166.
- [2] Ch. J. Colbourn, J. H. Dinitz (ed.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton 1996.
- [3] Encyklopedia brydża, PWN Warszawa 1996.
- [4] E. T. Parker, A. N. Mood, Some Balanced Howell Rotations for Duplicate Bridge Sessions, *Amer. Math. Monthly* 62 (1955), 714 – 716.

Kwadraty Rooma i turnieje brydżowe

Niech N będzie ustalonym zbiorem $(n+1)$ -elementowym. Przypomnijmy, że symbolem $P_2(N)$ oznaczamy zbiór

$$P_2(N) = \{A \subseteq N : |A| = 2\}.$$

Kwadratem Rooma o boku n nazywamy dowolną macierz R wymiaru $n \times n$ o wyrazach ze zbioru $P_2(N) \cup \{\emptyset\}$:

$$R : \{0, \dots, n-1\}^2 \rightarrow P_2(N) \cup \{\emptyset\},$$

spełniającą następujące trzy warunki:

- (R1) każda para $\{a, b\} \in P_2(N)$ występuje dokładnie jeden raz w macierzy R ,
- (R2) każdy element zbioru N występuje dokładnie jeden raz w każdym wierszu macierzy R ,
- (R3) każdy element zbioru N występuje dokładnie jeden raz w każdej kolumnie macierzy R ,

Zauważmy, że wiersze i kolumny kwadratu Rooma numerujemy liczbami od 0 do $n-1$.

Kwadraty Rooma mogą być wykorzystane do opisu turniejów brydżowych. Niech $N = \{0, 1, \dots, n\}$. Liczby ze zbioru N są numerami par startujących w turnieju. Jeśli $i, j \in \{0, \dots, n-1\}$ oraz $R(i, j) = \{a, b\} \in P_2(N)$, to pary o numerach a i b grają ze sobą rozdanie o numerze j w i -tej rundzie turnieju. Jeśli natomiast $R(i, j) = \emptyset$, to rozdanie o numerze j nie jest wykorzystywane w i -tej rundzie. Warunek (R1) mówi, że każde dwie pary startujące w turnieju grają ze sobą dokładnie jeden raz. Warunek (R2) mówi, że każda para gra (dokładnie jeden raz) w każdej rundzie, zaś warunek (R3) mówi, że każda para gra każde rozdanie dokładnie jeden raz.

Oto przykładowy kwadrat Rooma o boku 7. Opisuje on przebieg turnieju brydżowego, w którym startuje 8 par o numerach od 0 do 7.

	0	1	2	3	4	5	6
0	$\{0, 7\}$	$\emptyset$	$\emptyset$	$\{4, 6\}$	$\emptyset$	$\{2, 3\}$	$\{1, 5\}$
1	$\{2, 6\}$	$\{1, 7\}$	$\emptyset$	$\emptyset$	$\{0, 5\}$	$\emptyset$	$\{3, 4\}$
2	$\{4, 5\}$	$\{0, 3\}$	$\{2, 7\}$	$\emptyset$	$\emptyset$	$\{1, 6\}$	$\emptyset$
3	$\emptyset$	$\{5, 6\}$	$\{1, 4\}$	$\{3, 7\}$	$\emptyset$	$\emptyset$	$\{0, 2\}$
4	$\{1, 3\}$	$\emptyset$	$\{0, 6\}$	$\{2, 5\}$	$\{4, 7\}$	$\emptyset$	$\emptyset$
5	$\emptyset$	$\{2, 4\}$	$\emptyset$	$\{0, 1\}$	$\{3, 6\}$	$\{5, 7\}$	$\emptyset$
6	$\emptyset$	$\emptyset$	$\{3, 5\}$	$\emptyset$	$\{1, 2\}$	$\{0, 4\}$	$\{6, 7\}$

Opis turnieju zawarty w tym kwadracie nie jest kompletny. Mianowicie należy jeszcze ustalić na jakiej linii (NS czy WE) gra każda z par w danej rundzie. Ponadto ze względów organizacyjnych należy podać numer stołu, na którym dane pary grają ze sobą oraz opisać ruch kart między stolikami. Te kwestie wyjaśnimy w dalszym ciągu.

Z warunków (R1) – (R3) wynika, że liczba n jest nieparzysta. Powstaje naturalne pytanie, czy dla każdej liczby nieparzystej n istnieje kwadrat Rooma o boku n . Okazuje się, że jest to prawdą dla $n > 5$. Twierdzenia tego nie będziemy tu dowodzić. Pokażemy natomiast konstrukcję kwadratów Rooma dla liczb n pierwszych takich, że $n \equiv 3 \pmod{4}$.

Niech $n = 2m + 1$ i niech G będzie grupą przemienną rzędu n . W dalszym ciągu będziemy używać znaku $+$ jako symbolu działania w grupie G .

Starterem w grupie G nazywamy dowolny ciąg par uporządkowanych

$$((x_1, y_1), \dots, (x_m, y_m))$$

elementów grupy G , spełniający następujące dwa warunki:

- (1) $\{x_1, \dots, x_m\} \cup \{y_1, \dots, y_m\} = G \setminus \{0\}$,
- (2) $\{x_1 - y_1, \dots, x_m - y_m\} \cup \{y_1 - x_1, \dots, y_m - x_m\} = G \setminus \{0\}$.

Starter $((x_1, y_1), \dots, (x_m, y_m))$ nazywamy **silnym starterem**, jeśli spełnia następujące warunki:

- (3) $\forall i \in \{1, \dots, m\} (x_i + y_i \neq 0)$,
- (4) $\forall i, j \in \{1, \dots, m\} (i \neq j \Rightarrow x_i + y_i \neq x_j + y_j)$,

tzn. wszystkie sumy $x_i + y_i$ (dla $i = 1, \dots, m$) są różnymi niezerowymi elementami grupy G .

Sumatorem dla startera $((x_1, y_1), \dots, (x_m, y_m))$ nazywamy ciąg $(a_1, \dots, a_m)$ elementów grupy G spełniający następujące warunki:

- (5) $\forall i \in \{1, \dots, m\} (a_i \neq 0)$,
- (6) $\forall i, j \in \{1, \dots, m\} (i \neq j \Rightarrow a_i \neq a_j)$,
- (7) $\{x_1 + a_1, \dots, x_m + a_m\} \cup \{y_1 + a_1, \dots, y_m + a_m\} = G \setminus \{0\}$.

Inaczej mówiąc, sumatorem nazywamy taki ciąg $(a_0, \dots, a_m)$ różnych, niezerowych elementów grupy G , że ciąg

$$((x_1 + a_1, y_1 + a_1), \dots, (x_m + a_m, y_m + a_m))$$

jest również starterem w grupie G .

Przykłady.

1. Ciąg $((1, 5), (4, 6), (2, 3))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$. Ciąg $(1, 4, 2)$ jest sumatorem dla tego startera. Innym sumatorem jest ciąg $(4, 2, 1)$.
2. Ciąg $((1, 2), (4, 8), (5, 10), (9, 7), (3, 6))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$. Ciąg $(8, 10, 7, 6, 2)$ jest sumatorem dla tego startera. Innym sumatorem jest ciąg $(4, 5, 9, 3, 1)$.

Twierdzenie. Jeśli ciąg $((x_1, y_1), \dots, (x_m, y_m))$ jest starterem w grupie G rzędu n (przy czym $n = 2m + 1$) oraz ciąg $(a_1, \dots, a_m)$ jest sumatorem dla tego startera, to istnieje kwadrat Rooma o boku n .

Dowód. Niech $G = \{g_0, g_1, \dots, g_{n-1}\}$, przy czym $g_0 = 0$. Niech następnie $\infty \notin G$ oraz $N = G \cup \{\infty\}$. Definiujemy kwadrat Rooma R w następujący sposób:

$$R(i, j) = \begin{cases} \{\infty, g_i\}, & \text{jeśli } i = j, \\ \{g_i + x_k, g_i + y_k\}, & \text{jeśli } g_i - g_j = a_k, \\ \emptyset, & \text{jeśli element } g_i - g_j \text{ nie jest wyrazem sumatora } (a_1, \dots, a_m) \end{cases}$$

dla $i, j \in \{0, \dots, n-1\}$.

Musimy wykazać, że tak zdefiniowana macierz R spełnia warunki (R1) – (R3). Najpierw policzymy niepuste wyrazy macierzy R . Istnieje n wyrazów postaci $\{\infty, g_i\}$: leżą one na przekątnej. Następnie dla każdego k istnieje n par (g_i, g_j) (a więc i par (i, j)) takich, że $g_i - g_j = a_k$. Mianowicie są to pary

$$(g_0, g_0 - a_k), \dots, (g_{n-1}, g_{n-1} - a_k)$$

(ponieważ $a_k \neq 0$, więc $g_i \neq g_i - a_k$, czyli $i \neq j$). Łącznie mamy więc $mn + n$ wyrazów niepustych. Ponieważ

$$\binom{n+1}{2} = \frac{n(n+1)}{2} = \frac{n(2m+2)}{2} = n(m+1) = nm + n,$$

więc liczba wyrazów niepustych jest równa liczbie par należących do zbioru $P_2(N)$. Dla dowodu warunku (R1) wystarczy zatem pokazać, że każda taka para jest wyrazem macierzy R .

Zauważyliśmy już, że wszystkie pary postaci $\{\infty, i\}$ są wyrazami macierzy R . Niech zatem $g, h \in G$ oraz $g \neq h$. Z warunku (2) wynika, że istnieje w naszym starterze para (x_k, y_k) taka, że

$$x_k - y_k = g - h \quad \text{lub} \quad y_k - x_k = g - h.$$

Jeśli $x_k - y_k = g - h$ oraz $g_i = g - x_k$ i $g_j = g - x_k - a_k$, to $g_i - g_j = a_k$ i z definicji macierzy R wynika, że

$$R(i, j) = \{g_i + x_k, g_i + y_k\} = \{g, g - x_k + y_k\} = \{g, g - (x_k - y_k)\} = \{g, g - (g - h)\} = \{g, h\}.$$

Jeśli natomiast $g - h = y_k - x_k$, to $h - g = x_k - y_k$ i w podobny sposób pokazujemy, że para $\{h, g\}$ jest wyrazem macierzy R .

Sprawdzamy teraz warunek (R2). Niech $i \in \{0, \dots, n-1\}$. Mamy pokazać, że każdy element zbioru N występuje dokładnie jeden raz w wierszu i . Nietrudno zauważyć, że w każdym wierszu macierzy R występuje dokładnie $m+1$ wyrazów niepustych; stąd wynika, że wystarczy pokazać, iż każdy element zbioru N występuje co najmniej jeden raz w wierszu i . Oczywiście $\infty \in \{\infty, i\} = R(i, i)$, więc element ∞ występuje w tym wierszu. Podobnie $g_i \in R(i, i)$. Niech więc teraz $l \neq i$. Pokażemy, że element g_l też występuje w wierszu i .

Ponieważ $g_l - g_i \neq 0$, więc istnieje liczba $k \in \{1, \dots, m\}$ taka, że

$$g_l - g_i = x_k \quad \text{lub} \quad g_l - g_i = y_k,$$

czyli

$$g_l = g_i + x_k \quad \text{lub} \quad g_l = g_i + y_k.$$

Niech j będzie liczbą taką, że $g_j = g_i - a_k$. Wtedy $g_i - g_j = a_k$ oraz

$$R(i, j) = \{g_i + x_k, g_i + y_k\}.$$

Zatem $g_l \in R(i, j)$.

Wreszcie sprawdzamy warunek (R3). Niech $j \in \{0, \dots, n-1\}$. Znowy wystarczy pokazać, że każdy element zbioru N występuje co najmniej jeden raz w kolumnie j . Ponieważ $R(j, j) = \{\infty, g_j\}$, więc elementy ∞ i g_j występują w tej kolumnie. Niech więc $l \neq j$. Pokażemy, że element g_l też występuje w kolumnie j .

Oczywiście $g_l - g_j \in G \setminus \{0\}$, więc z definicji sumatora wynika, że istnieje liczba k taka, że

$$g_l - g_j = x_k + a_k \quad \text{lub} \quad g_l - g_j = y_k + a_k.$$

Niech i będzie taką liczbą, że $g_i = g_j + a_k$. Wtedy $g_i - g_j = a_k$ oraz

$$R(i, j) = \{g_i + x_k, g_i + y_k\}.$$

Jeśli $g_l - g_j = x_k + a_k$, to

$$g_l = g_j + x_k + a_k = g_i + x_k \in R(i, j).$$

Jeśli zaś $g_l - g_j = y_k + a_k$, to

$$g_l = g_j + y_k + a_k = g_i + y_k \in R(i, j).$$

W obu przypadkach element g_l występuje w kolumnie j . To kończy dowód twierdzenia.

Przypomnijmy teraz pojęcie reszty i niereszy kwadratowej. Jeśli p jest dowolną nieparzystą liczbą pierwszą, to liczbę całkowitą a nazywamy **resztą kwadratową** modulo p , wtedy i tylko wtedy, gdy $p \nmid a$ oraz istnieje liczba całkowita x taka, że

$$x^2 \equiv a \pmod{p}.$$

Jeśli natomiast $p \nmid a$ oraz nie istnieje liczba całkowita x taka, że $x^2 \equiv a \pmod{p}$, to liczbę a nazywamy **nieresztą kwadratową** modulo p . Resztami kwadratowymi są więc te elementy niezerowe ciała $\mathbb{Z}_p$, które są kwadratami w tym ciele. Zbiór elementów niezerowych ciała $\mathbb{Z}_p$ oznaczamy symbolem $\mathbb{Z}_p^*$. Definiujemy następnie tzw. **symbol Legendre'a** wzorem

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{jeśli } a \text{ jest resztą kwadratową modulo } p, \\ -1, & \text{jeśli } a \text{ jest nieresztą kwadratową modulo } p, \\ 0, & \text{jeśli } p \mid a. \end{cases}$$

W dalszym ciągu będziemy korzystać z następujących własności reszt i niereszt kwadratowych:

1. w zbiorze $\mathbb{Z}_p^*$ istnieje $\frac{p-1}{2}$ reszt kwadratowych i $\frac{p-1}{2}$ niereszt kwadratowych,
2. jeśli g jest generatorem grupy mnożeniowej $\mathbb{Z}_p^*$, to g^i jest resztą kwadratową wtedy i tylko wtedy, gdy wykładnik i jest liczbą parzystą,
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$,
4. iloczyn reszt kwadratowych jest resztą kwadratową,
5. iloczyn niereszt kwadratowych jest resztą kwadratową,
6. iloczyn reszty kwadratowej i niereszy kwadratowej jest nieresztą kwadratową,
7. jeśli $ab = 1$ w ciele $\mathbb{Z}_p$ to $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, czyli a jest resztą kwadratową wtedy i tylko wtedy, gdy b jest resztą kwadratową,
8. $\left(\frac{a^2}{p}\right) = 1$,
9. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, czyli liczba -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $p \equiv 1 \pmod{4}$,
10. jeśli $p \equiv 3 \pmod{4}$, to $a \in \mathbb{Z}_p^*$ jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $-a$ jest nieresztą kwadratową modulo p .

Pokażemy teraz konstrukcję starterów i sumatorów w pewnych grupach przemennych.

Założmy, że p jest liczbą pierwszą oraz $p > 3$ i $p = 4q + 3$. Wynika stąd, że liczba -1 jest nieresztą kwadratową modulo p . Niech g będzie generatorem grupy mnożeniowej ciała $\mathbb{Z}_p$. Definiujemy następnie

$$\begin{aligned} x_i &= g^{2i}, \\ y_i &= g^{2i+1} \end{aligned}$$

dla $i = 0, \dots, 2q$. Udowodnimy, że ciąg $((x_0, y_0), \dots, (x_{2q}, y_{2q}))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_p$.

Warunek (1) wynika stąd, że

$$\{x_0, \dots, x_{2q}\} \cup \{y_0, \dots, y_{2q}\} = \{g^0, \dots, g^{4q+1}\} = \{g^0, \dots, g^{p-2}\} = \{1, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\}.$$

Dla dowodu warunku (2) zauważmy najpierw, że

$$x_i - y_i = g^{2i} - g^{2i+1} = g^{2i}(1 - g)$$

oraz

$$y_i - x_i = g^{2i}(g - 1).$$

Elementy ciała $\mathbb{Z}_p$ postaci g^{2i} dla $i = 0, \dots, 2q$ są wszystkimi resztami kwadratowymi modulo p w tym ciele. Jeśli $g - 1$ jest resztą kwadratową, to elementy $x_y - y_i$ dla $i = 0, \dots, 2q$ są wszystkimi resztami kwadratowymi w ciele $\mathbb{Z}_p$ i elementy $y_i - x_i$ są wszystkimi nieresztami kwadratowymi w ciele $\mathbb{Z}_p$. Stąd wynika, że łącznie te różnice wyczerpują cały zbiór $\mathbb{Z}_p^*$. Jeśli zaś $g - 1$ jest nieresztą kwadratową modulo p , to elementy $x_i - y_i$ są wszystkimi nieresztami kwadratowymi i elementy $y_i - x_i$ są wszystkimi resztami kwadratowymi w ciele $\mathbb{Z}_p$, a więc te różnice też wyczerpują zbiór $\mathbb{Z}_p^*$.

Warunki (3) i (4) wynikają stąd, że

$$x_i + y_i = g^{2i}(g + 1).$$

Mianowicie $g + 1 \neq 0$, więc $x_i + y_i \neq 0$ dla $i = 0, \dots, 2q$. Ponadto, jeśli $x_i + y_i = x_j + y_j$, to $g^{2i} = g^{2j}$, skąd wynika, że $i = j$.

Przykłady.

1. Liczba 5 jest generatorem grupy mnożeniowej ciała $\mathbb{Z}_7$. Ponadto

$$5^0 = 1,$$

$$5^1 = 5,$$

$$5^2 = 4,$$

$$5^3 = 6,$$

$$5^4 = 2,$$

$$5^5 = 3.$$

Zatem ciąg $((1, 5), (4, 6), (2, 3))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$.

2. Liczba 2 jest generatorem grupy mnożeniowej ciała $\mathbb{Z}_{11}$. Ponadto

$$2^0 = 1,$$

$$2^1 = 2,$$

$$2^2 = 4,$$

$$2^3 = 6,$$

$$2^4 = 5,$$

$$2^5 = 10,$$

$$2^6 = 9,$$

$$2^7 = 7,$$

$$2^8 = 3,$$

$$2^9 = 6.$$

Zatem ciąg $((1, 2), (4, 8), (5, 10), (9, 7), (3, 6))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$.

Przypuśćmy teraz, że dany jest dowolny silny starter $((x_0, y_0), \dots, (x_{2q}, y_{2q}))$ w grupie addytywnej ciała $\mathbb{Z}_p$. Niech ciąg $(a_0, \dots, a_{2q})$ będzie zdefiniowany wzorem $a_k = -x_k - y_k$ dla $k = 0, \dots, 2q$. Pokażemy, że ciąg $(a_0, \dots, a_{2q})$ jest sumatorem dla tego silnego startera.

Z definicji silnego startera wynika, że wyrazy tego ciągu są różne i niezerowe. Mamy ponadto

$$x_k + a_k = -y_k \quad \text{oraz} \quad y_k + a_k = -x_k,$$

skąd wynika, że

$$\{x_0 + a_0, \dots, x_{2q} + a_{2q}\} \cup \{y_0 + a_0, \dots, y_{2q} + a_{2q}\} = \{-x_0, \dots, -x_{2q}\} \cup \{-y_0, \dots, -y_{2q}\} = \mathbb{Z}_p \setminus \{0\},$$

co kończy dowód.

Przykłady.

1. Ciąg $((1, 5), (4, 6), (2, 3))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$. Ponieważ

$$\begin{aligned} -1 - 5 &= -6 \equiv 1 \pmod{7}, \\ -4 - 6 &= -10 \equiv 4 \pmod{7}, \\ -2 - 3 &= -5 \equiv 2 \pmod{7}, \end{aligned}$$

więc ciąg $(1, 4, 2)$ jest sumatorem dla tego startera.

2. Ciąg $((1, 2), (4, 8), (5, 10), (9, 7), (3, 6))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$. Ponieważ

$$\begin{aligned} -1 - 2 &= -3 \equiv 8 \pmod{11}, \\ -4 - 8 &= -12 \equiv 10 \pmod{11}, \\ -5 - 10 &= -15 \equiv 7 \pmod{11}, \\ -9 - 7 &= -16 \equiv 6 \pmod{11}, \\ -3 - 6 &= -9 \equiv 2 \pmod{11}, \end{aligned}$$

więc ciąg $(8, 10, 7, 6, 2)$ jest sumatorem dla tego startera.

W przypadku silnego startera zdefiniowanego wyżej w grupie addytywnej ciała $\mathbb{Z}_p$ (gdzie $p > 3$ oraz $p \equiv 3 \pmod{4}$) możemy wskazać jeszcze jeden przykład sumatora. Niech g będzie generatorem grupy $\mathbb{Z}_p^*$. Wtedy g^{-1} też jest generatorem tej grupy. Zauważmy także, że $g \neq -1$ oraz $g^2 \neq -1$.

Ćwiczenie. Jeśli $(g+1)(g^2+1)$ jest nieresztą kwadratową modulo p , to $(g^{-1}+1)(g^{-2}+1)$ jest resztą kwadratową. W szczególności istnieje generator g grupy $\mathbb{Z}_p^*$ o tej własności, że $(g+1)(g^2+1)$ jest resztą kwadratową modulo p .

Weźmy zatem taki generator g grupy $\mathbb{Z}_p^*$, że $(g+1)(g^2+1)$ jest resztą kwadratową modulo p i zdefiniujmy ciąg $(a_0, \dots, a_{2q})$ wzorem $a_k = g^{2k+2}$ dla $k = 0, \dots, 2q$. Pokażemy, że ten ciąg jest sumatorem dla startera

$$((g^0, g^1), \dots, (g^{2q}, g^{2q+1})).$$

Oczywiście wszystkie wyrazy a_k są niezerowe i różne. Niech teraz $i \neq j$. Pokażemy, że

$$x_i + a_i \neq x_j + a_j.$$

Gdyby bowiem

$$x_i + a_i = x_j + a_j,$$

to mielibyśmy kolejno

$$\begin{aligned} g^{2i} + g^{2i+2} &= g^{2j} + g^{2j+2}, \\ g^{2i}(g^2 + 1) &= g^{2j}(g^2 + 1), \\ g^{2i} &= g^{2j}, \\ 2i &= 2j, \\ i &= j, \end{aligned}$$

co daje sprzeczność. W podobny sposób pokazujemy, że jeśli $i \neq j$, to $y_i + a_i \neq y_j + a_j$. Pokażemy, że także $x_i + a_i \neq y_j + a_j$. Przypuśćmy bowiem, że

$$x_i + a_i = y_j + a_j.$$

Mamy wówczas

$$\begin{aligned}g^{2i} + g^{2i+2} &= g^{2j+1} + g^{2j+2}, \\g^{2i}(g^2 + 1) &= g^{2j+1}(g + 1), \\g^{2i}(g + 1)(g^2 + 1) &= g^{2j+1}(g + 1)^2.\end{aligned}$$

Po lewej stronie równości mamy iloczyn dwóch reszt kwadratowych: g^{2i} oraz $(g + 1)(g^2 + 1)$. Po prawej stronie mamy natomiast iloczyn niereszty kwadratowej g^{2j+1} przez resztę kwadratową $(g + 1)^2$. Zatem po lewej stronie mamy resztę kwadratową, a po prawej stronie nieresztę, co jest niemożliwe. Udowodniliśmy więc, że zdefiniowany wyżej ciąg $(a_0, \dots, a_{2q})$ jest sumatorem.

Przykłady.

1. Liczba 5 jest generatorem grupy $\mathbb{Z}_7^*$. Mamy przy tym

$$(5 + 1)(5^2 + 1) = 6 \cdot 26 \equiv 6 \cdot 5 = 30 \equiv 2 \equiv 3^2 \pmod{7},$$

więc $(5+1)(5^2+1)$ jest resztą kwadratową modulo 7. Widzieliśmy, że z tego generatora otrzymaliśmy ciąg $((1, 5), (4, 6), (2, 3))$, będący silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$. Ponieważ

$$\begin{aligned}5^2 &= 4, \\5^4 &= 2, \\5^6 &= 1\end{aligned}$$

w ciele $\mathbb{Z}_7$, więc ciąg $(4, 2, 1)$ jest sumatorem dla tego startera. Z tego startera i sumatora otrzymujemy następujący kwadrat Rooma:

	0	1	2	3	4	5	6
0	$\{\infty, 0\}$	$\emptyset$	$\emptyset$	$\{1, 5\}$	$\emptyset$	$\{4, 6\}$	$\{2, 3\}$
1	$\{3, 4\}$	$\{\infty, 1\}$	$\emptyset$	$\emptyset$	$\{2, 6\}$	$\emptyset$	$\{0, 5\}$
2	$\{1, 6\}$	$\{4, 5\}$	$\{\infty, 2\}$	$\emptyset$	$\emptyset$	$\{0, 3\}$	$\emptyset$
3	$\emptyset$	$\{0, 2\}$	$\{5, 6\}$	$\{\infty, 3\}$	$\emptyset$	$\emptyset$	$\{1, 4\}$
4	$\{2, 5\}$	$\emptyset$	$\{1, 3\}$	$\{0, 6\}$	$\{\infty, 4\}$	$\emptyset$	$\emptyset$
5	$\emptyset$	$\{3, 6\}$	$\emptyset$	$\{2, 4\}$	$\{0, 1\}$	$\{\infty, 5\}$	$\emptyset$
6	$\emptyset$	$\emptyset$	$\{0, 4\}$	$\emptyset$	$\{3, 5\}$	$\{1, 2\}$	$\{\infty, 6\}$

2. Liczba 2 jest generatorem grupy $\mathbb{Z}_{11}^*$. Mamy przy tym

$$(2 + 1)(2^2 + 1) = 3 \cdot 5 = 15 \equiv 4 = 2^2 \pmod{11},$$

więc $(2+1)(2^2+1)$ jest resztą kwadratową modulo 11. Widzieliśmy, że z tego generatora otrzymaliśmy ciąg $((1, 2), (4, 8), (5, 10), (9, 7), (3, 6))$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$. Ponieważ

$$\begin{aligned}2^2 &= 4, \\2^4 &= 5, \\2^6 &= 9, \\2^8 &= 3, \\2^{10} &= 1\end{aligned}$$

w ciele $\mathbb{Z}_{11}$, więc ciąg $(10, 7, 6, 2, 1)$ jest sumatorem dla tego startera. Z tego startera i sumatora otrzymujemy następujący kwadrat Rooma:

	0	1	2	3	4	5	6	7	8	9	10
0	$\{\infty, 0\}$	$\emptyset$	$\{5, 10\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{4, 8\}$	$\{1, 2\}$	$\{7, 9\}$	$\emptyset$	$\{3, 6\}$
1	$\{4, 7\}$	$\{\infty, 1\}$	$\emptyset$	$\{0, 6\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{5, 9\}$	$\{2, 3\}$	$\{8, 10\}$	$\emptyset$
2	$\emptyset$	$\{5, 8\}$	$\{\infty, 2\}$	$\emptyset$	$\{1, 7\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{6, 10\}$	$\{3, 4\}$	$\{0, 9\}$
3	$\{1, 10\}$	$\emptyset$	$\{6, 9\}$	$\{\infty, 3\}$	$\emptyset$	$\{2, 8\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{0, 7\}$	$\{4, 5\}$
4	$\{5, 6\}$	$\{0, 2\}$	$\emptyset$	$\{7, 10\}$	$\{\infty, 4\}$	$\emptyset$	$\{3, 9\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{1, 8\}$
5	$\{2, 9\}$	$\{6, 7\}$	$\{1, 3\}$	$\emptyset$	$\{0, 8\}$	$\{\infty, 5\}$	$\emptyset$	$\{4, 10\}$	$\emptyset$	$\emptyset$	$\emptyset$
6	$\emptyset$	$\{3, 10\}$	$\{7, 8\}$	$\{2, 4\}$	$\emptyset$	$\{1, 9\}$	$\{\infty, 6\}$	$\emptyset$	$\{0, 5\}$	$\emptyset$	$\emptyset$
7	$\emptyset$	$\emptyset$	$\{0, 4\}$	$\{8, 9\}$	$\{3, 5\}$	$\emptyset$	$\{2, 10\}$	$\{\infty, 7\}$	$\emptyset$	$\{1, 6\}$	$\emptyset$
8	$\emptyset$	$\emptyset$	$\emptyset$	$\{1, 5\}$	$\{9, 10\}$	$\{4, 6\}$	$\emptyset$	$\{0, 3\}$	$\{\infty, 8\}$	$\emptyset$	$\{2, 7\}$
9	$\{3, 8\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{2, 6\}$	$\{0, 10\}$	$\{5, 7\}$	$\emptyset$	$\{1, 4\}$	$\{\infty, 9\}$	$\emptyset$
10	$\emptyset$	$\{4, 9\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\{3, 7\}$	$\{0, 1\}$	$\{6, 8\}$	$\emptyset$	$\{2, 5\}$	$\{\infty, 10\}$

Zajmiemy się teraz problemem przydziału parom linii (NS lub WE), na których mają grać w kolejnych rundach. Niech p będzie liczbą pierwszą taką, że $p > 3$ oraz $p = 4q + 3$. Niech g będzie generatorem grupy mnożeniowej ciała $\mathbb{Z}_p$. Wiemy już, że ciąg

$$((x_0, y_0), \dots, (x_{2q}, y_{2q})),$$

gdzie

$$x_i = g^{2i}, \quad y_i = g^{2i+1}$$

dla $i = 0, \dots, 2q$, jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_p$. Niech następnie ciąg $(a_0, \dots, a_{2q})$ będzie sumatorem dla tego startera. Definiujemy **uporządkowany kwadrat Rooma**

$$R : \{0, \dots, p-1\}^2 \rightarrow (\mathbb{Z}_p \cup \{p\})^2 \cup \{\emptyset\}$$

wzorem

$$R(i, j) = \begin{cases} (p, i), & \text{jeśli } i = j, \\ (i + x_k, i + y_k), & \text{jeśli } i - j = a_k, \\ \emptyset, & \text{jeśli } i - j \text{ nie jest wyrazem sumatora } (a_0, \dots, a_{2q}) \end{cases}$$

dla $i, j = 0, \dots, p-1$.

Liczby ze zbioru $\mathbb{Z}_p \cup \{p\} = \{0, \dots, p\}$ są numerami par startujących w turnieju. Rozdania i rundy turnieju są numerowane liczbami od 0 do $p-1$. Jeśli $R(i, j) = (a, b)$, to pary o numerach a i b grają ze sobą rozdanie o numerze j w i -tej rundzie, przy czym para o numerze a gra na linii NS, a para o numerze b gra na linii WE. Jeśli natomiast $R(i, j) = \emptyset$, to rozdanie o numerze j nie jest wykorzystywane w i -tej rundzie.

Dokładnie tak samo jak poprzednio możemy pokazać, że uporządkowany kwadrat Rooma R ma następujące własności:

- (R1) dla dowolnych $a, b \in \mathbb{Z}_p \cup \{p\}$ takich, że $a \neq b$ dokładnie jedna z par (a, b) i (b, a) jest wyrazem macierzy R , przy tym występuje w macierzy R w dokładnie jednym miejscu,
- (R2) każdy element zbioru N występuje dokładnie jeden raz w każdym wierszu macierzy R ,

(R3) każdy element zbioru N występuje dokładnie jeden raz w każdej kolumnie macierzy R ,

Jeżeli pary o numerach a i b grają rozdanie o numerze j na tej samej linii, to mówimy, że są porównywane w tym rozdaniu. Udowodnimy, że w zdefiniowanym wyżej uporządkowanym kwadracie Rooma każde dwie pary są porównywane w tej samej liczbie rozdań. Turniej o tej własności nazywamy zazwyczaj turniejem zbalansowanym.

Definiujemy zatem następującą funkcję

$$S : \mathbb{Z}_p^2 \rightarrow \{-1, +1\}$$

wskazującą, na jakiej linii para o numerze i gra rozdanie o numerze j :

$$S(i, j) = \begin{cases} +1, & \text{jeśli para o numerze } i \text{ gra rozdanie o numerze } j \text{ na linii NS,} \\ -1, & \text{jeśli para o numerze } i \text{ gra rozdanie o numerze } j \text{ na linii WE} \end{cases}$$

dla $i, j \in \mathbb{Z}_p$. Z powyższej definicji macierzy R wynika, że

$$S(i, j) = \begin{cases} +1, & \text{jeśli } i = p, \\ -1, & \text{jeśli } i \neq p \text{ oraz } i = j, \\ +1, & \text{jeśli } i \neq p, i \neq j \text{ oraz } i - j = x_k + a_k \text{ dla pewnego } k, \\ -1, & \text{jeśli } i \neq p, i \neq j \text{ oraz } i - j = y_k + a_k \text{ dla pewnego } k. \end{cases}$$

Mieliśmy do czynienia z dwoma sumatorami. Przyjrzyjmy się teraz, jak wygląda funkcja S dla tych sumatorów. Niech najpierw sumator $(a_0, \dots, a_{2q})$ będzie zdefiniowany wzorem

$$a_i = -x_i - y_i$$

dla $i = 0, \dots, 2q$. Wówczas, jeśli $i - j = x_k + a_k$, to $i - j = -y_k$. Ponieważ $y_k - g^{2k+1}$, więc y_k jest nieresztą kwadratową modulo p , a więc $-y_k$ jest resztą kwadratową. Jeśli natomiast $i - j = y_k + a_k$, to $i - j = -x_k$ oraz $-x_k$ jest nieresztą kwadratową modulo p . Zatem definicję funkcji S możemy zapisać w postaci

$$S(i, j) = \begin{cases} +1, & \text{jeśli } i = p, \\ -1, & \text{jeśli } i \neq p \text{ oraz } i = j, \\ \left(\frac{i-j}{p}\right), & \text{jeśli } i \neq p \text{ oraz } i \neq j \end{cases}$$

dla $i, j \in \mathbb{Z}_p$.

Drugi sumator $(a_0, \dots, a_{2q})$ był zdefiniowany wzorem

$$a_i = g^{2i+2}$$

dla $i = 0, \dots, 2q$. W tym przypadku wybieraliśmy generator g w taki sposób, by liczba $(g+1)(g^2+1)$ była resztą kwadratową modulo p . Teraz, jeśli $i - j = x_k + a_k$, to mamy

$$i - j = x_k + a_k = g^{2k} + g^{2k+2} = g^{2k}(g^2 + 1),$$

czyli

$$(i - j)(g + 1) = g^{2k}(g + 1)(g^2 + 1).$$

Zatem $(i - j)(g + 1)$ jest resztą kwadratową modulo p . Jeśli natomiast $i - j = y_k + a_k$, to

$$i - j - y_k + a_k = g^{2k+1} + g^{2k+2} = g^{2k+1}(g + 1),$$

czyli

$$(i - j)(g + 1) = g^{2k+1}(g + 1)^2.$$

Zatem $(i - j)(g + 1)$ jest nieresztą kwadratową modulo p . Stąd wynika, że

$$S(i, j) = \begin{cases} +1, & \text{jeśli } i = p, \\ -1, & \text{jeśli } i \neq p \text{ oraz } i = j, \\ \left(\frac{i-j}{p}\right) \cdot \left(\frac{g+1}{p}\right), & \text{jeśli } i \neq p \text{ oraz } i \neq j \end{cases}$$

dla $i, j \in \mathbb{Z}_p$.

Udowodnimy teraz następujące twierdzenie.

Twierdzenie. Dla dowolnych $u, w \in \mathbb{Z}_p$ takich, że $u \neq w$ zachodzi równość

$$\sum_{j=0}^{p-1} S(u, j) \cdot S(w, j) = -1.$$

Najpierw udowodnimy dwa lematy.

Lemat 1. W ciele $\mathbb{Z}_p$ zachodzi równość

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0.$$

Dowód. Równość ta wynika stąd, że w zbiorze $\{1, 2, \dots, p-1\}$ jest tyle samo reszt kwadratowych modulo p co niereszt kwadratowych modulo p .

Lemat 2. Jeśli $a \in \mathbb{Z}_p$ oraz $a \neq 0$, to

$$\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \cdot \left(\frac{j+a}{p}\right) = -1.$$

Dowód. Zauważmy najpierw, że

$$\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \cdot \left(\frac{j+a}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{j(j+a)}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{j^2(1+aj^{-1})}{p}\right) = \sum_{j=1}^{p-1} \left(\frac{1+aj^{-1}}{p}\right).$$

Zauważmy następnie, że jeśli j przebiega liczby od 1 do $p-1$, to $1+aj^{-1}$ przebiega (w ciele $\mathbb{Z}_p$) wszystkie liczby różne od 1. Zatem

$$\sum_{j=1}^{p-1} \left(\frac{1+aj^{-1}}{p}\right) = \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) - \left(\frac{1}{p}\right) = -1,$$

co kończy dowód lematu.

Dowód twierdzenia. Musimy udowodnić twierdzenie dla obu rozważanych sumatorów. Niech najpierw $a_k = -x_k - y_k$. Wówczas mamy dwa przypadki:

Przypadek 1. Jedna z liczb u i w jest równa p , np. $u = p$. Wtedy

$$\sum_{j=0}^{p-1} S(u, j) \cdot S(w, j) = \sum_{j=0}^{p-1} S(w, j) = \sum_{j \neq w} S(w, j) + S(w, w) = \sum_{j \neq w} \left(\frac{j-w}{p}\right) - 1 = \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) - 1 = -1.$$

Przypadek 2. $u \neq p$ oraz $w \neq p$. Wtedy

$$\begin{aligned}
\sum_{j=0}^{p-1} S(u, j) \cdot S(w, j) &= \sum_{j \neq u, w} S(u, j) \cdot S(w, j) + S(u, u) \cdot S(w, u) + S(u, w) \cdot S(w, w) = \\
&= \sum_{j \neq u, w} S(u, j) \cdot S(w, j) + (-1) \cdot \left(\frac{w-u}{p} \right) + (-1) \cdot \left(\frac{u-w}{p} \right) = \\
&= \sum_{j \neq u, w} S(u, j) \cdot S(w, j) + (-1) \cdot \left(\left(\frac{w-u}{p} \right) + \left(\frac{u-w}{p} \right) \right) = \\
&= \sum_{j \neq u, w} \left(\frac{u-j}{p} \right) \cdot \left(\frac{w-j}{p} \right) = \\
&= \sum_{j=0}^{p-1} \left(\frac{u-j}{p} \right) \cdot \left(\frac{w-j}{p} \right) = \\
&= \sum_{j=0}^{p-1} \left(\frac{j}{p} \right) \cdot \left(\frac{j+w-u}{p} \right) = \\
&= -1.
\end{aligned}$$

(Ostatnia równość wynika z lematu 2.)

Niech teraz $a_k = g^{2k+2}$. Rozpatrujemy takie same dwa przypadki.

Przypadek 1. Jedna z liczb u i w jest równa p , np. $u = p$. Wtedy

$$\begin{aligned}
\sum_{j=0}^{p-1} S(u, j) \cdot S(w, j) &= \sum_{j=0}^{p-1} S(w, j) = \sum_{j \neq w} S(w, j) + S(w, w) = \\
&= \sum_{j \neq w} \left(\frac{j-w}{p} \right) \cdot \left(\frac{g+1}{p} \right) - 1 = \left(\frac{g+1}{p} \right) \cdot \sum_{j=1}^{p-1} \left(\frac{j}{p} \right) - 1 = \\
&= -1.
\end{aligned}$$

Przypadek 2. $u \neq p$ oraz $w \neq p$. Wtedy

$$\begin{aligned}
\sum_{j=0}^{p-1} S(u, j) \cdot S(w, j) &= \sum_{j \neq u, w} S(u, j) \cdot S(w, j) + S(u, u) \cdot S(w, u) + S(u, w) \cdot S(w, w) = \\
&= \sum_{j \neq u, w} S(u, j) \cdot S(w, j) + (-1) \cdot \left(\frac{w-u}{p} \right) \cdot \left(\frac{g+1}{p} \right) + (-1) \cdot \left(\frac{u-w}{p} \right) \cdot \left(\frac{g+1}{p} \right) = \\
&= \sum_{j \neq u, w} S(u, j) \cdot S(w, j) + (-1) \cdot \left(\frac{g+1}{p} \right) \left(\left(\frac{w-u}{p} \right) + \left(\frac{u-w}{p} \right) \right) = \\
&= \sum_{j \neq u, w} \left(\frac{u-j}{p} \right) \cdot \left(\frac{w-j}{p} \right) \cdot \left(\frac{g+1}{p} \right)^2 = \\
&= \sum_{j=0}^{p-1} \left(\frac{u-j}{p} \right) \cdot \left(\frac{w-j}{p} \right) = \\
&= \sum_{j=0}^{p-1} \left(\frac{j}{p} \right) \cdot \left(\frac{j+w-u}{p} \right) = \\
&= -1.
\end{aligned}$$

Dowód twierdzenia jest więc zakończony.

Udowodnione twierdzenie mówi, że każde dwie pary grają $2q+1$ rozdań na tej samej linii i $2q+2$ rozdania na przeciwnych liniach, a więc są porównywane w tej samej liczbie rozdań.

Przykłady.

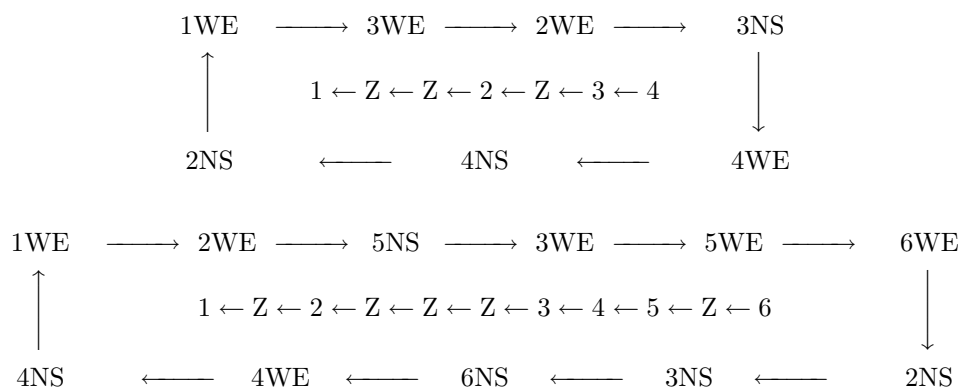
1. Ze startera $((1, 5), (4, 6), (2, 3))$ i sumatora $(4, 2, 1)$ w grupie addytywnej ciała $\mathbb{Z}_7$ otrzymujemy następujący uporządkowany kwadrat Rooma:

	0	1	2	3	4	5	6
0	(7, 0)	$\emptyset$	$\emptyset$	(1, 5)	$\emptyset$	(4, 6)	(2, 3)
1	(3, 4)	(7, 1)	$\emptyset$	$\emptyset$	(2, 6)	$\emptyset$	(5, 0)
2	(6, 1)	(4, 5)	(7, 2)	$\emptyset$	$\emptyset$	(3, 0)	$\emptyset$
3	$\emptyset$	(0, 2)	(5, 6)	(7, 3)	$\emptyset$	$\emptyset$	(4, 1)
4	(5, 2)	$\emptyset$	(1, 3)	(6, 0)	(7, 4)	$\emptyset$	$\emptyset$
5	$\emptyset$	(6, 3)	$\emptyset$	(2, 4)	(0, 1)	(7, 5)	$\emptyset$
6	$\emptyset$	$\emptyset$	(0, 4)	$\emptyset$	(3, 5)	(1, 2)	(7, 6)

2. Ze startera $((1, 2), (4, 8), (5, 10), (9, 7), (3, 6))$ i sumatora $(10, 7, 6, 2, 1)$ w grupie addytywnej ciała $\mathbb{Z}_{11}$ otrzymujemy następujący uporządkowany kwadrat Rooma:

	0	1	2	3	4	5	6	7	8	9	10
0	(11, 0)	$\emptyset$	(5, 10)	$\emptyset$	$\emptyset$	$\emptyset$	(4, 8)	(1, 2)	(9, 7)	$\emptyset$	(3, 6)
1	(4, 7)	(11, 1)	$\emptyset$	(6, 0)	$\emptyset$	$\emptyset$	$\emptyset$	(5, 9)	(2, 3)	(10, 8)	$\emptyset$
2	$\emptyset$	(5, 8)	(11, 2)	$\emptyset$	(7, 1)	$\emptyset$	$\emptyset$	$\emptyset$	(6, 10)	(3, 4)	(0, 9)
3	(1, 10)	$\emptyset$	(6, 9)	(11, 3)	$\emptyset$	(8, 2)	$\emptyset$	$\emptyset$	$\emptyset$	(7, 0)	(4, 5)
4	(5, 6)	(2, 0)	$\emptyset$	(7, 10)	(11, 4)	$\emptyset$	(9, 3)	$\emptyset$	$\emptyset$	$\emptyset$	(8, 1)
5	(9, 2)	(6, 7)	(3, 1)	$\emptyset$	(8, 0)	(11, 5)	$\emptyset$	(10, 4)	$\emptyset$	$\emptyset$	$\emptyset$
6	$\emptyset$	(10, 3)	(7, 8)	(4, 2)	$\emptyset$	(9, 1)	(11, 6)	$\emptyset$	(0, 5)	$\emptyset$	$\emptyset$
7	$\emptyset$	$\emptyset$	(0, 4)	(8, 9)	(5, 3)	$\emptyset$	(10, 2)	(11, 7)	$\emptyset$	(1, 6)	$\emptyset$
8	$\emptyset$	$\emptyset$	$\emptyset$	(1, 5)	(9, 10)	(6, 4)	$\emptyset$	(0, 3)	(11, 8)	$\emptyset$	(2, 7)
9	(3, 8)	$\emptyset$	$\emptyset$	$\emptyset$	(2, 6)	(10, 0)	(7, 5)	$\emptyset$	(1, 4)	(11, 9)	$\emptyset$
10	$\emptyset$	(4, 9)	$\emptyset$	$\emptyset$	$\emptyset$	(3, 7)	(0, 1)	(8, 6)	$\emptyset$	(2, 5)	(11, 10)

Ostatnim problemem organizacyjnym jest numeracja stołów i opis sposobu poruszania się par i rozdań w kolejnych rundach. Stoliki, przy których toczy się gra numerujemy kolejnymi liczbami, pozostawiając między tymi stolikami miejsce na rozdania niewykorzystane w danej rundzie; te miejsca nazywamy zbiornicami. Para o najwyższym numerze gra przez cały czas na stoliku numer 1 na linii NS. Wszystkie pozostałe pary poruszają się według tego samego schematu; jego opis nazywamy kartą pilotującą. A oto otrzymane karty pilotujące turniejów dla 8 i 12 par:



Na zakończenie wspomnimy jeszcze, że jeśli istnieje turniej zbalansowany dla n par, to liczba n jest podzielna przez 4. Nietrudny dowód tego faktu pozostawimy Czytelnikowi jako ćwiczenie.