MATEMATYKA DYSKRETNA

Marysia Nazarczuk

Błędy, uwagi, alternatywne rozwiązania, rozwiązania brakujących zadań
lub innych zadań proszę zgłaszać na maila mn417755@students.mimuw.edu.pl

Ćwiczenia 4

Permutacje i liczby Stirlinga

Zadanie 4.1.
Znajdź wzór na liczbę n-permutacji o danej sygnaturze.

Rozwiązanie:
Niech dana jest sygnatura $1^{\alpha_1}2^{\alpha_2}\dots K^{\alpha_k}$. Dowolną permutację możemy zapisać na $n!$ sposobów. Następnie wstawiamy nawiasy kwadratowe odpowiednich długości (w rosnącej kolejności długości cyklu). W danym cyklu nie ma znaczenia, który element jest pierwszy, czyli dany cykl można zapisać na i sposobów, a że cyklów o długości i jest α_i, toteż dzielimy przez i^{α_i}. Również kolejność cykli nie ma znaczenia, zatem możemy zamieniać miejscami cykle o tej samej długości. Musimy więc podzielić jeszcze przez $(\alpha_i)!$. Zatem wzór na liczbę n-permutacji o danej sygnaturze to $\frac{n!}{\prod(\alpha_i)!i^{\alpha_i}}$.

Zadanie 4.2.
Permutacja f jest inwolucją gdy $f \circ f = id$. Pokaż, że

a) permutacja jest inwolucją wtedy i tylko wtedy gdy ma sygnaturę $1^{\alpha_1}2^{\alpha_2}$

b) każda permutacja jest złożeniem dwóch inwolucji.

Rozwiązanie:

a) Gdy permutacja jest inwolucją, to po podwójnym zastosowaniu jej na ciągu otrzymamy początkowy ciąg, zatem w ciągu są cykle o długości maksymalnie dwa. Zatem sygnatura takiej permutacji to $1^{\alpha_1}2^{\alpha_2}$. Gdy permutacja ma sygnaturę $1^{\alpha_1}2^{\alpha_2}$ to znaczy, że ma cykle o długości jeden i o długości dwa, zatem po dwukrotnym zastosowaniu tej permutacji otrzymujemy początkowy ciąg. Permutacja jest więc inwolucją.

b) Permutację można podzielić na cykle i rozważać inwolucje tylko w obrębie konkretnego cyklu. Pierwszą inwolucją będzie $f(a_k) = a_{n-k+1}$, natomiast drugą będzie $g(a_k) = a_{n-k+2}$ dla cyklu $[a_1, a_2, \dots, a_n]$. Czyli inaczej $f = [1, n][2, n-1][3, n-2]\dots[\lfloor\frac{n}{2}\rfloor, \lceil\frac{n}{2}\rceil]$ oraz $g = [2, n][3, n-1]\dots[\lceil\frac{n}{2}\rceil, \lfloor\frac{n}{2}\rfloor + 1]$.

Zadanie 4.3.
Dane są liczby naturalne $n \geq k > 0$. Jakie jest prawdopodobieństwo, że w losowej n-permutacji jedynka należy do cyklu o długości k?

Rozwiązanie:
Wszystkich permutacji jest $n!$. Policzmy ile jest możliwości, że 1 jest w k-cyklu. Do jedynki dobieramy $k-1$ elementów na $\binom{n-1}{k-1}$ sposobów. Następnie ustawiamy je w cyklu na $(k-1)!$ sposobów, a pozostałe ustawiamy dowolnie. Permutację pozostałych elementów możemy wykonać na $(n-k)!$ sposobów. Zatem tych możliwości jest $\binom{n-1}{k-1} \cdot (k-1)! \cdot (n-k)!$. Wówczas prawdopodobieństwo wynosi $\frac{1}{n!} \cdot \binom{n-1}{k-1} \cdot (k-1)! \cdot (n-k)! = \frac{1}{n!} \cdot \frac{(n-1)!}{(k-1)!(n-1l)!} \cdot (n-k)! = \frac{1}{n}$.

Zadanie 4.4.
Pokaż, że losowa n-permutacja z prawdopodobieństwem $\frac{H_{n-1}}{n}$ składa się dokładnie z dwóch cykli.

Rozwiązanie:
Policzmy prawdopodobieństwo tego, że losowa n-permutacja ma dwa cykle. Liczbę takich możliwości policzymy sumując po długości cyklu z jedynką. Liczby do jedynki dobieramy na $\binom{n-1}{k-1}$ sposobów. Ustawiamy je w cykl na $(k-1)!$ sposobów. Następnie ustawiamy pozostałe elementy na $\frac{(n-k)!}{n-k}$ sposoby. Liczba takich możliwości wynosi więc

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

$$=\sum_{k=1}^{n-1}\frac{(n-1)!}{(n-k)}=(n-1)!\sum_{k=1}^{n-1}\frac{1}{n-k}=H_{n-1}\cdot(n-1)!$$

Zatem prawdopodobieństwo wynosi $\frac{H_{n-1}\cdot(n-1)!}{n!}=\frac{H_{n-1}}{n}$.

Zadanie 4.5.
Mamy n skarbonek i n kluczy, przy czym każdy klucz pasuje do dokładnie jednej skarbonki. Wrzucamy losowo po jednym kluczu do każdej skarbonki, po czym rozbijamy k skarbonek, $1\le k\le n$. Oblicz prawdopodobieństwo tego, że dzięki temu będzie można otworzyć wszystkie pozostałe skarbonki.

Rozwiązanie:
Klucze w skarbonkach wraz z odpowiadającymi im skarbonkami tworzą cykle. Aby można było otworzyć skarbonki, to przede wszystkim musi być nie więcej niż k cykli. Uda się nam otworzyć wszystkie skarbonki, gdy największy z najmniejszych elementów we wszystkich cyklach jest nie większy niż k. Wystarczy więc aby pierwsza liczba w $SUPERNAPISIE$ była mniejsza od k. Zatem szukane prawdopodobieństwo wynosi $\frac{k}{n}$.

Zadanie 4.6.
Pokaż tożsamość $x^n=\sum_k \left\{{n \atop k}\right\} x^{\underline{k}}$ przez interpretacje kombinatoryczną.

Rozwiązanie:

1. $\left\{{n \atop k}\right\}$ oznacza liczbę możliwych podziałów n-elementowego zbioru na k bloków.
2. $x^{\underline{k}}=|\{f:\{1,\ldots,k\}\to\{1,\ldots,x\}\ f\text{różnowartościowe}\}|$
3. $\left\{{n \atop k}\right\}\cdot x^{\underline{k}}$ oznacza ile różnych wartości przybierze funkcja, gdzie k to liczba różnych wartości funkcji.

Rozbijamy zbiór $\{1,\ldots,n\}$ na k bloków, które będą miały te same wartości, a następnie blokom tym przypisujemy wartości z $\{1,\ldots,x\}$ (każdy blok ma inną wartość). Liczba możliwych sposobów podziału zbioru $\{1,\ldots,n\}$ na k bloków to $\left\{{n \atop k}\right\}$, zaś liczba sposobów przypisania blokom różnych wartości z $\{1,\ldots,n\}$ to $x^{\underline{k}}$. Sumując po k otrzymujemy liczbę wszystkich możliczych funkcji z $\{1,\ldots,n\}$ do $\{1,\ldots,n\}$, czyli $x^n = |\{f : \{1,\ldots,n\} \to \{1,\ldots,n\}|$. Zatem $x^n = \sum_k \left\{ n \atop k \right\} x^{\underline{k}}$.

Zadanie 4.7.

Pokaż następujące wzory:

$$\left\{ n \atop k \right\} = \sum_{i_1,\ldots,i_{n-k}} i_1 \cdot i_2 \ldots i_{n-k} \cdot [1 \leq i_1 \leq i_2 \leq \ldots \leq i_{n-k} \leq k]$$

$$\left[n \atop k \right] = \sum_{i_1,\ldots,i_{n-k}} i_1 \cdot i_2 \ldots i_{n-k} \cdot [0 < i_1 < i_2 < \ldots < i_{n-k} < n]$$

Ćwiczenia 5

Funkcje tworzące

Zadanie 5.1.
Znajdź funkcje tworzące ciągów $\langle H_n \rangle$ i $\langle n^2 \rangle$.

Rozwiązanie:
Niech $A(x)$ to funkcja tworząca ciągu $\langle H_n \rangle$.

$$A(x) = \sum_{n \geq 0} H_n x^n = \sum_{n \geq 0} \sum_{k \leq n} \frac{1}{k} \cdot x^n = \sum_{n} \sum_{k} a_k \cdot b_{n-k} \cdot x^n$$

gdzie $a_k = \frac{1}{k}$ oraz $a_0 = 0$ i $b_k = 1$. Mamy tu więc splot dwóch funkcji $B(x) = \sum\limits_{n \geq 0} a_n x^n$ i $C(x) = \sum\limits_{n \geq 0} b_n x^n$, czyli

$$A(x) = B(x) \cdot C(x) = \sum_{n \geq 1} \frac{1}{n} \cdot x^{n-1} \cdot \sum_{n \geq 0} x^n = \frac{1}{x} \cdot \sum_{n \geq 1} \frac{x^n}{n} \cdot \sum_{n \geq 0} x^n = \frac{1}{x} \cdot \left(\ln \frac{1}{1-x} \right) \cdot \left(\frac{1}{1-x} \right)$$

$$A(x) = -\frac{\ln(1-x)}{(1-x)x}$$

Niech $D(x)$ to funkcja tworząca ciągu $\langle n^2 \rangle$. Wówczas

$$D(x) = x + 4x^2 + 9x^3 + 16x^4 + \ldots \quad | \cdot x$$

$$x \cdot D(x) = 0 + x^2 + 4x^3 + 9x^2 + \ldots$$

Po odjęciu stronami mamy

$$D(x)(1-x) = x + 3x^2 + 5x^3 + 7x^4 + \ldots \quad | \cdot x$$

$$D(x)(1-x) \cdot x = 0 + x^2 + 3x^3 + 5x^4 + \ldots$$

Po odjęciu stronami mamy

$$D(x)((1-x) - (1-x)x) = x + 2x^2 + 2x^3 + 2x^4 + \ldots$$

$$D(x)(x^2 - 2x + 1) = x + 2x^2(1 + x + x^2 + \ldots)$$

$$D(x)(x-1)^2 = x + \frac{2x^2}{1-x}$$

$$D(x) = \frac{x(x+1)}{(1-x)^3}$$

Zadanie 5.2.
Oblicz $a_n = \sum\limits_{0 \leq i \leq n} F_i \cdot F_{n-i}$.

Rozwiązanie:
Funkcja tworząca tego ciągu to $F(x) = \sum\limits_n \sum\limits_k F_k \cdot F_{n-k} \cdot x^n$. Mamy tu splot dwóch funkcji tworzących. $F(x) = \left(\sum\limits_{n\geq 0} F_n x^n\right) \cdot \left(\sum\limits_{n\geq 0} F_n x^n\right)$. Oznaczmy przez $S = \sum\limits_{n\geq 0} F_n x^n$. Wówczas

$$S = 1 + x + 2x^2 + 3x^3 + 5x^4 + 8x^5 + 13x^6 + \ldots \qquad | \cdot x$$

$$xS = 0 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \ldots$$

Po odjęciu stronami mamy

$$S(1-x) = 1 + 0 + x^2 + x^3 + 2x^4 + 3x^5 + 5x^6 + \ldots$$

$$S(1-x) = 1 + x^2(1 + x + 2x^2 + 3x^3 + 5x^4 + \ldots)$$

$$S(1-x) = 1 + x^2 S \Leftrightarrow S = \frac{1}{1-x-x^2}$$

Funkcja tworząca ciągu a_n wygląda więc następująco $F(x) = \frac{1}{(1-x-x^2)^2} = \frac{1}{(x+\frac{1+\sqrt{5}}{2})(x-\frac{\sqrt{5}-1}{2})}$. Dalej mamy

$$F(x) = \frac{a}{(x+\frac{1+\sqrt{5}}{2})} + \frac{b}{(x-\frac{\sqrt{5}-1}{2})} \Leftrightarrow b\left(x + \frac{1+\sqrt{5}}{2}\right) + a\left(x - \frac{\sqrt{5}-1}{2}\right) = 1 - x - x^2$$

$$a = -\frac{1}{\sqrt{5}} \text{ oraz } b = \frac{1}{\sqrt{5}}$$

Mamy więc

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

$$F(x) = \left(-\frac{1}{\sqrt{5}}\right) \cdot \sum_{n\geq 0} \left(-\frac{1+\sqrt{5}}{2}\right)^n x^n + \left(\frac{1}{\sqrt{5}}\right) \cdot \sum_{n\geq 0} \left(\frac{\sqrt{5}-1}{2}\right)^n x^n$$

$$F(x) = \sum_{n\geq 0} \left(\left(-\frac{1}{\sqrt{5}}\right) \cdot \left(-\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1}{\sqrt{5}}\right) \cdot \left(\frac{\sqrt{5}-1}{2}\right)^n \right) x^n$$

zatem

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

Zadanie 5.3.
Niech $G_k(z) = \sum\limits_n \left\{ {n \atop k} \right\} \frac{z^n}{n!}$ będzie wykładniczą funkcją tworzącą dla liczb Stirlinga drugiego rodzaju, przy ustalonym dolnym wskaźniku. Pokaż, że $G_k(z) = \frac{(e^x-1)^k}{k!}$, dowodząc kolejno tożsamości:

a) $\left\{ {n+1 \atop k+1} \right\} = \sum\limits_m \binom{n}{m} \left\{ {m \atop k} \right\}$

b) $\left\{ {n+1 \atop k+1} \right\} = \left\{ {n \atop k+1} \right\} (k+1) + \left\{ {n \atop k} \right\}$

c) $G_k\ e^z = (k+1)\ G_{k+1} + G_k$

Znajdź zwarty wzór na wykładniczą funkcję tworzącą liczb Bella $B_n = \sum_k \left\{ {n \atop k} \right\}$.

Rozwiązanie:

a) Mamy $n+1$ królików i dzielimy je na $k+1$ zbiorów. Możemy to zrobić na $\left\{ {n+1 \atop k+1} \right\}$ sposobów. Dla najmłodszego królika wybieramy m królików z n królików, które nie będą z tym królikiem w pasztecie. Króliki te dzielimy na k pasztetów, a reszta jest wraz z najmłodszym w $k+1$-szym pasztecie. Możemy takie podziały zliczyć i otrzymamy $\sum_m \binom{n}{m} \left\{ {m \atop k} \right\}$.

b) $\left\{ {n \atop k} \right\}$ odpowiada tym podziałom, gdzie $(n+1)$-szy królik jest sam. $\left\{ {n \atop k+1} \right\} \cdot (k+1)$ odpowiada podziałowi n królików na $k+1$ zbiorów i dobiorze na $(k+1)$ spobów zbiór do którego pójdzie $(n+1)$-szy królik. Otrzymujemy podział $n+1$ królików na $k+1$ zbiorów, czyli $\left\{ {n+1 \atop k+1} \right\}$.

c)

$$\sum_{n\geq 0} \left\{ {n+1 \atop k+1} \right\} \frac{x^n}{n!} \overset{a)}{=} \sum_{n\geq 0}\sum_m \binom{n}{m} \left\{ {m \atop k} \right\} \frac{x^n}{n!} = \left(\sum_{n\geq 0} \left\{ {n \atop k} \right\} \frac{x^n}{n!} \right) \left(\sum_{n\geq 0} \frac{x^n}{n!} \right) = G_k \cdot e^2$$

$$\sum_{n\geq 0} \left\{ {n+1 \atop k+1} \right\} \frac{x^n}{n!} \overset{b)}{=} \sum_{n\geq 0} \left(\left\{ {n \atop k+1} \right\} (k+1) + \left\{ {n \atop k} \right\} \right) \frac{x^n}{n!} =$$

$$= (k+1) \sum_{n\geq 0} \left\{ {n \atop k+1} \right\} \frac{x^n}{n!} + \sum_{n\geq 0} \left\{ {n \atop k} \right\} \frac{x^n}{n!} = (k+1)G_{k+1} + G_k$$

Zatem $(k+1)G_{k+1} = G_k(e^x - 1)$, czyli inaczej $G_k = G_{k-1} \cdot \frac{(e^x-1)}{k}$. Zatem

$$G_k = G_{k-1}\frac{(e^x-1)}{k} = G_{k-2}\frac{(e^x-1)^2}{k\cdot(k-1)} = \ldots = G_0 \cdot \frac{(e^x-1)^k}{k!}$$

gdzie $G_0 = 1$. Wzór zwarty na wykładniczą funkcję tworzącą liczb Bella $B_n = \sum_k \left\{ {n \atop k} \right\}$ to $B_n = e^{e^x-1}$, bo mamy $B_n = \sum_k \frac{(e^x-1)^k}{k!} = e^{e^x-1}$.

Zadanie 5.4.

Permutacja f jest inwolucją, gdy złożenie f ze sobą jest identycznością. Pokaż, że wykładniczą funkcję tworzącą dla liczby inwolucji jest $e^{z+\frac{z^2}{2}}$.

Ćwiczenia 6

Enumeratory

Zadanie 6.1.
Oblicz, na ile sposobów można zapisać liczbę naturalną n jako sumę k nieujemnych całkowitych składników, gdzie rozkłady $n = s_1 + \ldots + s_k$ i $n = t_1 + \ldots + t_k$ są różne, gdy $s_i \neq t_i$ dla pewnego $1 \leq i \leq k$.

Zadanie 6.2.
Niech n będzie liczbą naturalną. Znajdź liczbę rozwiązań równania $x_1 + 2 \cdot x_2 + 2 \cdot x_3 = n$ w liczbach naturalnych x_1, x_2, x_3.

Rozwiązanie:
Enumerator będzie wyglądał następująco

$$(1 + x + x^2 + \ldots (1 + x^2 + x^4 + \ldots)(1 + x^2 + x^4 + \ldots) = (1 + x + x^2 + \ldots)\frac{1}{(1-x^2)^2} =$$

$$= (1 + x + x^2 + \ldots) \cdot \sum_{n \geq 0} (n+1)x^{2n} = (1 + x + x^2 + x^3 + \ldots)(1 + 2x^2 + 3x^4 + \ldots) =$$

$$\sum_{n \geq 0} \left(\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (k+1) \right) x^n = \sum_{n \geq 0} \binom{\lfloor \frac{n}{2} \rfloor + 2}{2} x^n$$

Zadanie 6.3.
Niech a_n oznacza liczbę ciągów długości n złożonych z liter A, B, C i nie zawierających dwóch sąsiednich liter A, ani dwóch sąsiednich liter B. Znajdź zwarty wzór na a_n.

Zadanie 6.4.
Z kostek o wymiarach 1×2 układamy prostokąt o pionowej krawędzi długości 2 i poziomej krawędzi długości n. Kostki nie mogą na siebie nachodzić; każda z połówek kostki może być pomalowana na jeden z dwóch kolorów (biały lub czarny). Kostki układamy od strony lewej do prawej: pierwszą kostkę kładziemy pionowo, a pozostałe tak, aby cała lewa krawędź każdej nowo kładzionej kostki dotykała kostek ułożonych wcześniej. Obowiązuje przy tym zasada, że kładziona kostka wzdłuż lewej krawędzi musi mieć takie same kolory, jak występujące na sąsiadujących z nią z lewej strony polach. Oblicz, na ile sposobów można ułożyć taki prostokąt.

Rozwiązanie:
Jeśli a_n to liczba ułożeń kostek dla prostokąta $2 \times n$, to $a_n = a_{n-1} + 4 \cdot a_{n-2}$. Pierwszy składnik a_{n-1} to przypadek kiedy kostka jest ułożona pionowo (musimy ją pokolorować jak te poprzednio). Drugi skladnik $4 \cdot a_{n-2}$ to przypadek kiedy kostki są ułożnone poziomo (możemy je pokolorować na cztery sposoby, bo te co stykają się z poprzednimi to musimy pokolorować jak te poprzednie, natomiast te dwa co się nie stykają możemy pokolorować dwoma kolorami. Możemy to zrobić na $2^2 = 4$ sposoby). Warunki początkowe to $a_0 = 0, a_1 = a_2 = 4$. (Trzeba rozwiązać teraz brzydkie równanie rekurencyjne.)

Zadanie 6.5.
Niech h_n oznacza liczbę sposobów pokolorowania szczebli n-szczeblowej drabiny na cztery kolory (czerwony, biały, niebieski i zielony) tak, że liczba szczebli czerwonych jest parzysta, a białych jest nieparzysta. Znajdź wykładniczą funkcję tworzącą ciągu h_n i oblicz h_{2001}.

Rozwiązanie:
Wykładnicza funkcja tworząca kolorowań drabiny czerwoną farbą to

$$x + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots = \frac{e^x + e^{-x}}{2}$$

Wykładnicza funkcja tworząca kolorowań drabiny białą farbą to

$$x + x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots = \frac{e^x - e^{-x}}{2}$$

Dla pozostałych dwóch kolorowań będzie to

$$1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots = e^x$$

Zatem wykładnicza funkcja tworząca ciągu to

$$\left(x + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots\right)\left(x + x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots\right)\left(1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots\right)^2 =$$

$$= \frac{e^x + e^{-x}}{2} \cdot \frac{e^x - e^{-x}}{2} \cdot e^x \cdot e^x = \frac{e^{4x} - 1}{4}$$

Mamy $\frac{e^{4x}-1}{4} = \sum\limits_{n\geq 1} 4^{n-1}\frac{x^n}{n!}$, czylu $h_n = 4^{n-1}$ i $h_0 = 0$, bo na zero sposobów możemy pokolować nieparzystą liczbę białych szczebli.

Zadanie 6.6.
Na ile sposobów można rozdzielić 33 tys. zł. premii pomiędzy 22 pracowników firmy, w tym prezesa i jego zastępcę, jeśli szeregowy pracownik może dostać 1000 lub 1500 zł., a członek kierownictwa - nic, 1500 lub 3000 zł.?

Rozwiązanie:
Enumerator będzie wyglądał następująco

$$(1 + x^{1500} + x^{3000})^2 \cdot (x^{1000} + x^{1500})^{20}$$

Szukamy tego, co stoi przy x^{33000}. Podstawiając za x^{500} wyrażenie x mamy

$$(1 + x^3 + x^6)^2 \cdot (x^2 + x^3)^{20}$$

i szukamy tego co stoi przy x^{66}. Zatem mamy

$$(x^2 + x^3)^{20} \cdot (1 + 2x^2 + 3x^6 + 2x^9 + x^{12}) = x^{40} \cdot \sum_{i\geq 0} \binom{20}{i} x^i =$$

$$= x^{40} \cdots \left(1 + \binom{20}{1} x + \binom{20}{2} x^2 + \ldots + \binom{20}{20} x^{20}\right) \cdot (1 + 2x^2 + 3x^6 + 2x^9 + x^{12})$$

Przy x^{66} będzie stało wyrażenie $3 + 2\binom{20}{17} + \binom{20}{14}$

Ćwiczenia 7

Zasada włączania-wyłączania, wieżomiany

Zadanie 7.1.
Udowodnij, że liczba elementów zbioru X należących do co najmniej $r > 0$ spośród zbiorów $A_1, \ldots, A_n$, gdzie $A_i \subseteq X$ dla $i = 1, \ldots, n$, wynosi

$$\sum_{k=r}^{n} (-1)^{k-r} \binom{k-1}{r-1} S_k$$

gdzie $S_k = \sum_{1 \leq i_i < \ldots < i_k \leq n} |a_{i_1} \cap \ldots \cap A_{i_k}|$.

Rozwiązanie:
Chcemy udowodnić, że

$$D(\geq r) = \sum_{j=r}^{n} \binom{j-1}{r-1} (-1)^{j-r} S_j$$

Wiemy jednak, że zachodzi

$$D(r) = \sum_{j=r}^{n} \binom{j}{r} (-1)^{j-r} S_j$$

Pokażemy przez indukcję, że $D(\geq r) - D(\geq r+1) = D(r)$. Najpierw baza indukcyjna

$$D(\geq 1) = \sum_{j=1}^{n} \binom{j-1}{0} (-1)^{j-1} S_j = -\sum_{j=1}^{n} (-1)^j S_j = S_1 - S_2 + \cdots - (-1)^n S_n = |X| - D(0)$$

A następnie krok indukcyjny

$$D(\geq r) - D(\geq r+1) = \sum_{j=r}^{n} \binom{j-1}{r-1} (-1)^{j-r} S_j - \sum_{j=r+1}^{n} \binom{j-1}{r} (-1)^{j-r-1} S_j$$

$$D(\geq r) - D(\geq r+1) = S_r + \sum_{j=r+1}^{n} (-1)^{j-r} \binom{j-1}{r-1} S_j + \sum_{j=r+1}^{n} (-1)^{j-r} \binom{j-1}{r} S_j$$

$$D(\geq r) - D(\geq r+1) = S_r + \sum_{j=r+1}^{n} (-1)^{j-r} S_j \left(\binom{j-1}{r-1} + \binom{j-1}{r} \right)$$

$$D(\geq r) - D(\geq r+1) = S_r + \sum_{j=r+1}^{n} (-1)^{j-r} S_j \binom{j}{r}$$

$$D(\geq r) - D(\geq r+1) = D(r)$$

Zadanie 7.2.
Oblicz, ile jest liczb 8-cyfrowych nie zawierających cyfry 0 ani ciągu kolejnych cyfr $\ldots 121 \ldots$.

Rozwiązanie:
Niech X to wszystkie ciągi ośmiocyfrowe bez zera. Mamy

$$|X| = 9^8$$

Niech A_i to liczby które mają 121 na pozycjach $(i, i+1, i+2)$. Musimy określić moce poszczególnych przecięć. Mamy

$$|A_i| = 9^5$$

bo trzy miejsca są zajęte przez liczby 121, a pozostałe pięć wybieramy dowolnie. Mamy więc

$$S_1 = |A_1| + \ldots + |A_6| = 6 \cdot 9^5$$

Rozważmy teraz przecięcia dwóch zbiorów A_i. Jeśli A_i są sąsiednie, to mamy zero takich ciągów (nie da się, bo jeden wygląda tak $**121***$ a drugi tak $***121**$). Gdy są to zbiory o dwa, to zajmujemy pięć miejsc przez liczby 12121, a pozostałe trzy ustawiamy dowolnie (przykładowy ciąg $**12121*$. Daje nam więc to 9^3 możliwych sposobów. Jeżeli różnica jest większa niż dwa, to zajmujemy sześć miejsc przez liczby 121 i 121, a pozostałe dwa dowolnie (przykładowy ciąg $121*121*$). Daje nam to 9^2 możliwych sposobów. Zatem dla par mamy

$$|A_i \cap A_j| = \begin{cases} 0 \text{ jeśli } j = i+1 \\ 9^3 \text{ jeśli } j = i+2 \\ 9^2 \text{ jeśli } j > i+2 \end{cases}$$

Mamy więc

$$S_2 = (|A_1 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_5| + |A_4 \cap A_6|) +$$
$$+ (|A_1 \cap A_4| + |A_1 \cap A_5| + |A_1 \cap A_6| + |A_2 \cap A_5| + |A_2 \cap A_6| + |A_3 \cap A_6|) = 4 \cdot 9^3 + 6 \cdot 9^2$$

Rozpatrzmy teraz przecięcia trzech zbiorów. Trójki mogą być takie, że wszystkie trzy zachodzą jednym elementem i wówczas pozostaje jedno miejsce na dowolny element (przykładowy ciąg $1212121*$. Mamy więc 9^1 możliwości. Druga możliwość jest taka, że tylko dwie trójki nachodzą jednym elementem, a trzecia trójka jest od nich rozłączna. Wówczas nie ma żadnego miejsca na dowolny element (przykładowy ciąg 12121121). Daje nam to 9^0 możliwości. Zatem dla trójek mamy

$$S_3 = (|A_1 \cap A_3 \cap A_5| + |A_2 \cap A_4 \cap A_6|) + (|A_1 \cap A_3 \cap A_6| + |A_1 \cap A_4 \cap A_6|) = 2 \cdot 9 + 2 \cdot 1 = 20$$

Dla przecięcia czterech i pięciu zbiorów nie ma żadnych możliwości, zatem łączna liczba takich ciągów to

$$|X| - S_1 + S_2 - S_3 = 9^8 - 6 \cdot 9^5 + 4 \cdot 9^3 + 6 \cdot 9^2 - 20 = 42695809$$

Zadanie 7.3.
Znajdź liczbę permutacji zbioru $\{1, \ldots, 7\}$ nie zawierających czterech kolejnych elementów w porządku rosnącym.

Zadanie 7.4.
Pokaż, że wielomiany $ax + 1,\ ax^2 + (a+2)x + 1,\ abx^2 + (a+b+1)x + 1$ są wieżowe dla dowolnych a, b naturalnych.

Rozwiązanie:
Pierwszy wieżomian, czyli $ax + 1$ jest wieżomianem planszy prostokątnej $1 \times a$. Drugi wieżomian, czyli $ax^2 + (a+2)x + 1$ jest wieżomianem planszy z jednym wierszem o długości $a+1$ i doklejonym nad nim jednym polem. Łącznie pól mamy $a+2$, czyli jedną wieżę stawiamy na $a+2$ sposoby. Dwie wieże stawiamy na a sposobów, bo jedna będzie znajdować się w doklejonym kwadraciku, a druga na którymś z n pól (bo nie pod tym doklejonym). Trzeci wieżomian, czyli $abx^2 + (a+b+1)x + 1$ to wieżomian planszy w kształcie litery L, gdzie jeden bok ma długość $a+1$, a drugi bok ma długość $b+1$.

Zadanie 7.5.
Znajdź liczbę n-nieporządków za pomocą wieżomianow (liczba rozstawień wież na dopełnieniu przekątnej).

Zadanie 7.6.
7 krasnoludków $k_1, \dots, k_7$ ma codziennie do wykonania 7 prac $p_1, \dots, p_7$, przy czym:

k_1 nie umie wykonać p_2, p_3

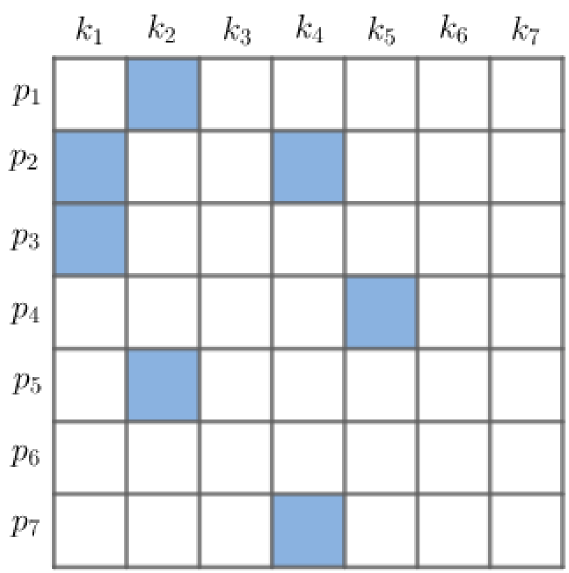
k_2 nie umie wykonać p_1, p_5

k_4 nie umie wykonać p_2, p_7

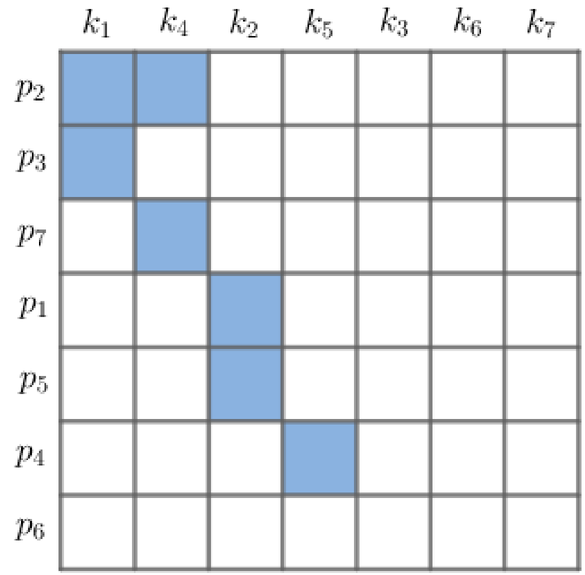
k_5 nie umie wykonać p_4

Przez ile dni mogą rozdzielać prace codziennie inaczej?

Rozwiązanie:
Rozważmy rozstawienia wież na planszy



Wówczas liczba dni przez ile krasnoludki mogą pracować równa będzie liczbie rozstawień wież na szachownicy. Łatwiej jednak będzie, jak policzymy wieżomian dopełniania tej planszy, czyli na ile sposobów można ustawić wieże na niebieskich polach. Wiadomo, że permutacja wierszy i kolumn nie zmienia wieżomianu, zatem będzie on taki sam jak wielomian poniższej szachownicy.



Wieżomiana dla planszy p_2, p_3, p_7 to $1 + 4x + 3x^2$. Wieżomiana dla planszy p_1, p_5 to $1 + 2x$. Wieżomiana dla planszy p_4 to $1 + x$. Musimy wymnożyć te wieżomiany. Otrzymujemy

$$r'_B(x) = 1 + 7x + 17x^2 + 17x^3 + 6x^4$$

Jest to wieżomian dopełnienia planszy, zatem wieżomian planszy obliczymy ze wzoru

$$r_B(n) = \sum_{0 \le k \le n} (-1)^k r'_B(k)(n-k)!$$

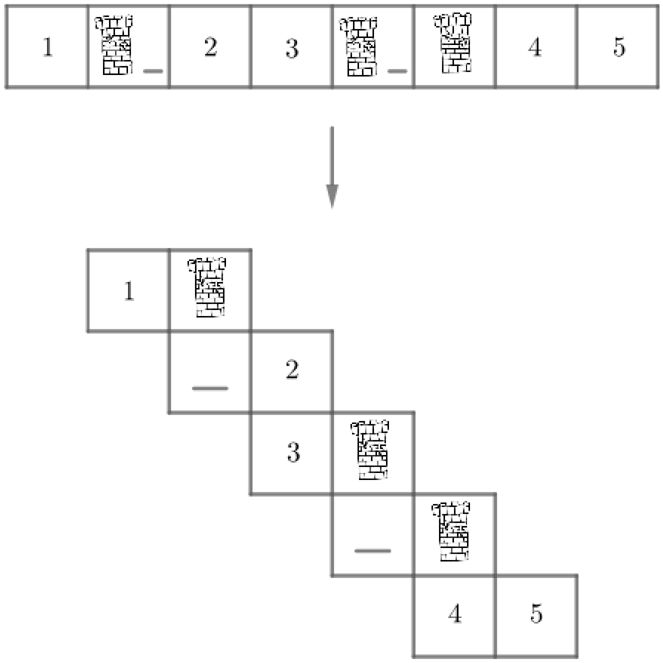
czyli mamy

$$r_B(7) = 7! \cdot r'_B(0) - 6! \cdot r'_B(1) + \ldots - 0! \cdot r'_B(7) = 7! \cdot 1 - 6! \cdot 7 + 5! \cdot 17 - 4! \cdot 17 + 3! \cdot 6 = 1668$$

Zadanie 7.7.
Udowodnij, że wielomianem wieżowym planszy $\{(i,i), (i, i+1) \mid i = 1, \ldots, n\}$ jest

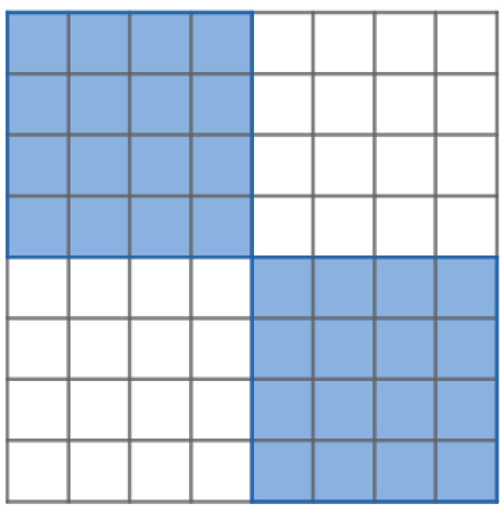
$$\sum_{k=0}^{n} \binom{2n+1-k}{k} x^k$$

Rozwiązanie:
W tablicy o wymiarze $2n + 1 - k$ wybieramy k miejsc. W pierwszych $k - 1$ miejscach wstawiamy wieże i puste pole, a w k-tym miejscu wstawiam samą wieżę. Otrzymuję tablicę o rozmiarze $2n_1 - k + (k-1) = 2n$ w której jest k wież, ale wieże nie stoją obok siebie. Takie ustawienie mogę zrobić na $\binom{2n-(k-1)}{k} = \binom{2n+1-k}{k}$ sposobów.



Zadanie 7.8.
Na ile sposobów można rozstawić 6 nie atakujących się wież na czarnych polach szachownicy 8×8?

Rozwiązanie:
Wieżomian tej planszy będzie taki sam jak wielomian poniższej planszy, ponieważ permutacja wierszy i kolumn nie zmienia wieżomianu.



Wieżomian tej planszy jest równy kwadratowi wieżomianu planszy 4×4. Wieżomian planszy 4×4 jest równy $(24x^4 + 96x^3 + 72x^2 + 16^x + 1)^2$, zatem wieżomian dużej planszy to

$$r(x) = \left(\sum_{i=0}^{4} \binom{4}{i} \cdot \binom{4}{i} i! \cdot x^i \right)^2$$

Zatem liczba rozstawień 6 wież na szachownicy 8×8 to 12672.

Ćwiczenia 8

Podziały liczby

Zadanie 8.1.
Pokaż następujące rekurencje na liczby $p_k(n)$ (liczba podziałów n na k składników):

$$p_k(n) = p_{k-1}(n-1) + p_k(n-k)$$

Rozwiązanie:
Po lewej mamy podziały liczby n na dokładnie k składników. $p_{k-1}(n-1)$ to liczba tych podziałów, które mają jedynkę, natomiast $p_k(n-k)$ to liczba tych podziałów, które nie mają jedynki. Sumując to otrzymujemy liczbę podziałów n na dokładnie k składników.

Zadanie 8.2.
Oblicz $p_2(n)$ i $p_3(n)$.

Rozwiązanie:
$p_2(n)$ to liczba podziałów liczby n na dwa składniki. Mniejszy składnik może być co najwyżej równy $\lfloor \frac{n}{2} \rfloor$, zatem jego wartość możemy wybrać na $\lfloor \frac{n}{2} \rfloor$ sposoby. Mamy więc

$$p_2(n) = \lfloor \frac{n}{2} \rfloor$$

$p_3(n)$ to liczba podziałów liczby n na trzy składniki. Najmniejszy składnik wybieramy na $\lfloor \frac{n}{3} \rfloor$ sposoby. Załóżmy, że najmniejszy składnik ma i elementów. Do średniego i największego również dajemy po i elementów. Pozostaje $n-3i$ elementów, które rozkładamy na dwa składniki na $p_2(n-3i)$ sposoby. Musimy dodać jeszcze 1, bo przecież drugi i trzeci składnik mogą być sobie równe. Mamy więc

$$p_3(n) = \sum_{i=1}^{\lfloor \frac{n}{3} \rfloor} p_2(n-3i) + 1 = \sum_{i=1}^{\lfloor \frac{n}{3} \rfloor} \lfloor \frac{n-3i}{2} \rfloor + 1$$

Zadanie 8.3.
Pokaż oszacowanie

$$\frac{1}{k!} \cdot \binom{n-1}{k-1} \leq p_k(n) \leq \frac{1}{k!} \cdot \binom{n + \frac{k(k-1)}{2} - 1}{k-1}$$

Zadanie 8.4.
Pokaż, że liczba $P(n) - P(n-1)$ jest równa liczbie podziałów n na składniki większe niż 1.

Rozwiązanie:
Od wszystkich podziałów $P(n)$ odejmujemy podziały z jedynką, a ich jest $P(n-1)$, bo do dowolnego podziału $n-1$ dostawiamy jedynkę i mamy podział z jedynką. Otrzymujemy więc podziały w których nie ma składników równych 1.

Zadanie 8.5.
Niech $D(n; a_1, \ldots, a_m)$ oznacza liczbę podziałów n na części rozmiarów należących do zbioru $\{a_1, a_2, \ldots, a_m\}$.

a) Pokaż, że ten ciąg ma $\frac{1}{(1-t^{a_1})(1-t^{a_2})\ldots(1-t^{a_m})}$ jako swoją funkcję tworzącą.

b) Z rozkładu na ułamki proste

$$\frac{1}{(1-t)(1-t^2)} = \frac{1}{2(1-t)^2} + \frac{1}{4(1-t)} + \frac{1}{4(1+t)}$$

wyprowadź wzór na $D(n;1,2)$.

Rozwiązanie:

a) Funkcja tworząca podziałów to

$$\sum_{n\geq 0} P(n)x^n = (1+x+x^2+\ldots)(1+x^2+x^4+\ldots)\ldots$$

Zatem ciąg ten ma funkcję tworzącą

$$(1+x^{a_1}+x^{2a_1}+\ldots)(1+x^{a_2}+x^{2a_2}+\ldots)\ldots(1+x^{a_n}+x^{2a_n}+\ldots) =$$

$$= \frac{1}{1-x^{a_1}} \cdot \frac{1}{1-x^{a_2}} \cdot \ldots \cdot \frac{1}{1-x^{a_m}}$$

b) Funkcja tworząca $D(n,1,2)$ to

$$\frac{1}{1-x} \cdot \frac{1}{1-x^2} = \frac{1}{2(1-x)^2} + \frac{1}{4(1-x)} + \frac{1}{4(1+t)} =$$

$$= \frac{1}{2}\sum_{n\geq 0}(n+1)x^n + \frac{1}{4}\sum_{n\geq 0}x^n + \frac{1}{4}\sum_{n\geq 0}(-1)^n x^n =$$

$$= \sum_{n\geq 0} x^n \left(\frac{2n+3+(-1)^n}{4}\right)$$

Zatem przy x^n stoi $D(n;1,2) = \lfloor \frac{n}{2} \rfloor + 1 = \lceil \frac{n+1}{2} \rceil$

Zadanie 8.6.

Wykaż, że łączna liczba składników we wszystkich podziałach liczby n jest równa $\sum_{k=0}^{n-1} P(k)\tau(n-k)$, gdzie $P(k)$ to liczba podziałów k, a $\tau(m) = \sum_{d|m} 1$ jest liczbą (dodatnich) dzielników m.

Ćwiczenia 9

Powtórka przed kolokwium

Zadanie 1.

Udowodnij, że dla $x, y, n \in \mathbb{N}$ zachodzi tożsamość $(x+y)^{\overline{n}} = \sum_k \binom{n}{k} x^{\overline{k}} y^{\overline{n-k}}$

Rozwiązanie:

Zinterpretujmy kombinatorycznie lewą stronę. Mamy sobie stado n królików. Do stada przybył kucharz, który sprzedaje x rodzajów zup oraz y rodzajów dań głównych. Pozwala on każdemu królikowi wybrać sobie jedną potrawę w zamian za nowy przepis. Tak więc pierwszy królik wybiera potrawę na $x+y$ sposobow, drugi którlik wybiera potrawę na $x+y+1$ sposobów itd.. Wszystkich możliwych wyborów jest więc $(x+y)^{\overline{n}}$.

Zinterpretujmy teraz kombinatorycznie prawą stronę. Dla ustalonego k wybieramy z n królików k królików, które będą musiały jeść zupę. Pozostałe będą jadły danie główne. Mając wybrane k królików postępujemy jak poprzednio. Króliki które jedzą zupę, dają kucharzowi przepis na zupę, natomiast pozostałe króliki dają kucharzowi przepis na danie główne. Dla ustalonego k mamy więc możliwych sposobów $\binom{n}{k} x^{\overline{k}} y^{\overline{n-k}}$. Sumując po k otrzymujemy $\sum_k \binom{n}{k} x^{\overline{k}} y^{\overline{n-k}}$.

Zadanie 2.

Udowodnij tożsamość $\sum_{k=0}^{m} k^n = \sum_{k=0}^{n} k! \binom{m+1}{k+1} \left\{ {n \atop k} \right\}$

Rozwiązanie:

Zauważmy, że

$$\sum_{k=0}^{n} k! \binom{m+1}{k+1} \left\{ {n \atop k} \right\} = \sum_{k=0}^{n} \left(\binom{m}{k+1} + \binom{m}{k} \right) \left\{ {n \atop k} \right\} =$$

$$= \sum_{k=0}^{n} k! \binom{m}{k+1} \left\{ {n \atop k} \right\} + \sum_{k=0}^{n} k! \binom{m}{k} \left\{ {n \atop k} \right\}$$

Udowodnijmy więc, że teza zachodzi dla $n=1$. Mamy $\sum_{k=0}^{m} k = \frac{m(m+1)}{2}$ oraz $\sum_{k=0}^{n} k! \binom{m+1}{k+1} \left\{ {1 \atop k} \right\}$ $= m \cdot 0 + 1 \cdot \frac{m(m+1)}{2} \cdot 1 = \frac{m(m+1)}{2}$. Zatem dla $n=1$ teza zachodzi.

Udowodnijmy teraz, że teza zachodzi dla $n>1$, zakładając, że zachodzi dla $n-1$. Mamy

$$\sum_{k=0}^{m} k^n = m^n + \sum_{k=0}^{m-1} k^n = m^n + \sum_{k=0}^{n} k! \binom{m}{k+1} \left\{ {n \atop k} \right\} =$$

$$= \sum_{k=0}^{n} k! \binom{m+1}{k+1} \left\{ {n \atop k} \right\} - \sum_{k=0}^{n} k! \binom{m}{k} \left\{ {n \atop k} \right\} + m^n$$

Aby teza była prawdziwa, to musi zachodzić $m^n = \sum_{k=0}^{n} k! \binom{m}{k} \left\{ {n \atop k} \right\}$.

Zinterpretujmy tą równość kombinatorycznie. Z lewej dzielimy n królików na m pasztetów według przydatności do spożycia. Z prawej strony dla ustalonego k wybieramy sobie z m różnych jakości dokładnie k na które będziemy dzielić pasztety. Robimy to na $\binom{m}{k}$ sposobów. Mamy więc sobie

k lad na które będą wykładane pasztety z królików. Każda lada odpowiada innej jakości pasztetu. Dalej n królików dzielimy na k części. Robimy to na $\left\{ n \atop k \right\}$ sposobów. Następnie z królików robimy pasztety, które układamy na ladach na $k!$ sposobów. Zatem dla ustalonego k liczba sposobów zrobienia k różnych pasztetów to $k! \binom{m}{k} \left\{ n \atop k \right\}$. Łącznie podziałów n królików na m pasztetów jest $\sum_{k=0}^{n} k! \binom{m}{k} \left\{ n \atop k \right\}$.

II sposób:

Zinterpretujmy kombinatorycznie lewą stronę. Mamy m różnych rodzajów pasztetów królików. Dzielimy n królików na dowolną liczbę pasztetów różnych rodzajów, nie większą od m. Dla ustalonego k liczba podziałów n królików na k pasztetów to k^n. Zatem sumując po liczbie rodzajów pasztetów, otrzymujemy wzór na łączą liczbę podziałów $\sum_{k=0}^{m} k^n$.

Zinterpretujmy kombinatorycznie prawą stronę. Mamy sobie $m+1$ rodzajów pasztetów, z czego jeden to będzie pasztet królewski. Mamy sobie n królików. Mamy sobie też króla, który zawsze będzie lądował sam w królewskim pasztecie. Dla ustalonego k z $m+1$ rodzajów pasztetów losujemy $k+1$ rodzajów. Pierwszy z nich idzie dla króla królików, a pozostałe k idzie dla n królików. Wykonujemy to na $\binom{m+1}{k+1}$ sposobów. Następnie n królików dzielimy na k grupek. Wykonujemy to na $\left\{ n \atop k \right\}$ sposobów. Grupki królików przyporządkowujemy do różnych rodzajów pasztetów na $k!$ sposobów. Sumując po liczbie królewskiego, mamy $\sum_{k=0}^{n} k! \binom{m+1}{k+1} \left\{ n \atop k \right\}$.

Zadanie 3.

Niech a_n oznacza liczbę n-ciągów zerojedynkowych nie zawierających spójnego podciągu 011. Znajdź funkcję tworzącą i zwarty wzór na a_n.

Rozwiązanie:

Znajdźmy wzór rekurencyjny na ciąg a_n, oznaczający na ile sposobów możemy otrzymać ciąg zerojedynkowy. Zero można dopisać do każdego ciągu, jedynkę można dopisać do ciągu jeśli cały ciąg jest jedynkami lub jeśli ostatnia cyfra to zero. Ciągów do których możemy dopisać 0 jest a_{n-1}. Ciągów do których możemy dopisać 1 składających się z samych jedynek jest oczywiście 1. Ciągów do których możemy dopisać 1, które kończą się na 0 jest a_{n-2}, ponieważ do dowolnego ciągu o długości $n-2$ dopiszemy na końcu 0.

Zatem rekurencyjny wzór na a_n to $a_n = a_{n-1} + a_{n-2} + 1$, gdzie $a_0 = 1$, $a_1 = 2$, $a_2 = 4$.

$$\begin{aligned}
&a_0 = 0 + 0 + 1 \\
&a_1 = a_0 + 0 + 1 \\
&a_2 = a_1 + a_0 + 1 \\
&... \\
&a_{n-1} = a_{n-2} + a_{n-3} + 1 \\
&a_n = a_{n-1} + a_{n-2} + 1
\end{aligned}$$

Po pomnożeniu stronami przez x^i dla $i = 0, 1, 2, ..., n$ i zsumowaniu stronami otrzymujmemy.

$\sum\limits_{n\geq 0} a_n x^n = \sum\limits_{n\geq 0} a_n x^{n+1} + \sum\limits_{n\geq 0} a_n x^{n+2} + \sum\limits_{n\geq 0} x^n$. Niech $A(x)$ to funkcja tworząca ciągu a_n. Wówczas mamy $A(x) = xA(x) + x^2A(x) + \frac{1}{1-x}$. Czyli $A(x)(1-x-x^2) = \frac{1}{1-x}$, skąd $A(x) = \frac{1}{(1-x-x^2)(1-x)}$. Wyrażenie $\frac{1}{1-x-x^2}$ to funkcja tworząca liczb Fibonacciego, przy czym $F_0 = 1$ i $F_1 = 1$. Mamy więc $A(x) = \left(\sum\limits_n F_n x^n\right) \cdot \left(\sum\limits_n x^n\right) = \sum\limits_{n\geq 0}\left(\sum\limits_{k=0}^{n} F_k\right) x^n$. Zatem $a_n = \sum\limits_{k=0}^{n} F_k$. Ponadto mamy $F_n = F_{n+1} - F_{n-1}$, zatem mamy

$$
\begin{aligned}
F_0 &= F_1\\
F_1 &= F_2 - F_0\\
F_2 &= F_3 - F_1\\
F_3 &= F_4 - F_2\\
&...\\
F_{n-1} &= F_n - F_{n-2}\\
F_n &= F_{n+1} - F_{n-1}
\end{aligned}
$$

Zatem mamy $a_n = \sum\limits_{k=0}^{n} F_n = F_{n+1} + F_n - F_0 = F_{n+2} - 1$.

Zadanie 4.
Niech a_n oznacza liczbę uporządkowanych podziałów n-zbioru, których kolejność elementów w bloku jest bez zbaczenia, natomiast istotna jest kolejność bloków (np. $a_2 = 3 : \langle\{1,2\}\rangle, \langle\{1\},\{2\}\rangle, \langle\{2\},\{1\}\rangle$).

a) Udowodnij, że ciąg $\langle a_n\rangle$ spełnia zależność rekurencyjną $a_n = \sum\limits_{i=0}^{n-1}\binom{n}{i} a_i$, $a_0 = 1$

b) Udowodnij, że $a_n = \frac{1}{2}\sum\limits_{k=0}^{\infty}\frac{k^n}{2^k}$, gdzie przyjmujemy, że $0^0 = 1$.

Rozwiązanie:

a) Udowodnimy to przez interpretację kombinatoryczną. Mamy sobie króliki ponumerowane od 1 do n. Chcemy je podzielić na grupki w jakiej będą się ustawiać w kolejce po lody. Króliki lubią tworzyć gangi, dlatego część z nich będzie w większych grupkach a inne w mniejszych. Istnieją też króliki które stoją same w kolejce po lody. Chcemy obliczyć na ile sposobów można ustawić n takich królików. Dla danego i wybieramy z n królików i królików, które będą stały z przodu, a następnie na a_i sposobów porządkujemy je. Pozostałe $n-i$ królików będzie stało na końcu kolejki w oddzielnej grupce. Zatem dla ustalonego i liczba sposobów na ile możemy ustawić te króliki to $\binom{n}{i} a_i$. Łącznie możliwych ustawień n królików jest więc $\sum\limits_{i=0}^{n-1}\binom{n}{i} a_i$.

b) Mamy $a_n = \sum\limits_{i=0}^{n-1}\binom{n}{i} a_i = \sum\limits_{i=0}^{n}\binom{n}{i} a_i - a_n$, zatem $a_n = \frac{1}{2}\sum\limits_{i=0}^{n}\binom{n}{i} a_i + \frac{1}{2}\cdot[n=0]$. Wykładnicza funkcja tworząca ciągu a_n to $A(x) = \sum\limits_n a_n \cdot \frac{x^n}{n!} = \sum\limits_n \left(\frac{1}{2}\cdot\sum\limits_i \binom{n}{i} a_i + \frac{1}{2}\cdot[n=0]\right)\cdot\frac{x^n}{n!} =$

$\sum_n \frac{1}{2} \cdot \sum_i \binom{n}{i} a_i \cdot \frac{x^n}{n!} + \frac{1}{2} = \left(\frac{1}{2} \cdot \sum_n a_i \frac{x^n}{n!}\right) \cdot \left(\sum_n \frac{x^n}{n!}\right) + \frac{1}{2} = \frac{1}{2}A(x) \cdot e^x + \frac{1}{2}$. Mamy więc $A(x) = \frac{1}{2}A(x) \cdot e^x + \frac{1}{2}$, czyli $A(x) = \frac{1}{2\left(1-\frac{e^x}{2}\right)} = \frac{1}{2} \cdot \sum_k \frac{e^{kx}}{2^k}$. No a przecierz $e^{kx} = \sum_n \frac{(kx)^n}{n!}$, zatem $A(x) = \frac{1}{2}\sum_k \sum_n \frac{k^n x^n}{2^k n!} = \sum_n \left(\frac{1}{2}\sum_k \frac{k^n}{2^k}\right)\frac{x^n}{n!}$. Zatem jako, że a_n to jest to co stoi przy $\frac{x^n}{n!}$ w wykładniczej funkcji tworzącej, toteż $a_n = \frac{1}{2}\sum_k \frac{k^n}{2^n}$.

Zadanie 5.
Niech s_n będzie liczbą wszystkich skończonych ciągów $\langle x_1, ..., x_k\rangle$ liczb naturalnych, takich że $\forall_i \ 1 \leq x_i \leq n$ oraz $x_{i+1} \geq 2x_i$ (długość ciągu k może być dowolna, w szczególności równa 0). Udowodnij, że s_n spełnia równanie rekurencyjne $s_n = s_{n-1} + s_{\lfloor \frac{n}{2} \rfloor}$ dla $n \geq 1$ i $s_0 = 1$. Wykaż, że funkcja tworząca $S(z)$ ciągu s_n spełnia zależność $(1-z)S(z) = (1+z)S(z^2)$.

Rozwiązanie:
Rozważmy ciągi o długości n o wyrazach ze zbioru $\{0, 1, 2, ..., n\}$ w których 0 oznacza brak elementu, natomiast pozostałe liczby to wyrazy ciągu. Mając ciąg o długości $n-1$ możemy na początku dopisać 0 otrzymując ciąg długości n. Do $\lfloor \frac{n}{2} \rfloor$ ciągów o długości $n-1$ możemy dopisać na końcu liczbę n, aby spełniony był warunek $x_{i+1} \geq 2x_i$, ponieważ właśnie tyle jest ciągów, których ostatni element jest nie większy niż $\lfloor \frac{n}{2} \rfloor$. Zatem wzór rekurencyjny na s_n, czyli liczbę ciągów długości n, to $s_n = s_{n-1} + s_{\lfloor \frac{n}{2} \rfloor}$.
Znajdźmy teraz funkcję tworzącą tego ciągu. Po przemnożeniu s_i-tego wyrazu ciągu stronami przez x_i i zsumowaniu tych wyrażeń, dostajemy

$$\sum_{n\geq 0} s_n x^n = \sum_{n\geq 0} s_n x^{n+1} + \sum_{n\geq 0} s_{\lfloor \frac{n}{2} \rfloor} x^n$$

Jeśli przez $S(x)$ oznaczymy funkcję tworzącą ciągu s_n, to mamy

$$S(x) = xS(x) + \sum_{n\geq 0} s_{\lfloor \frac{n}{2} \rfloor} x^n$$

czyli

$$S(x)(1-x) = \sum_{n\geq 0} s_{\lfloor \frac{n}{2} \rfloor} x^n$$

Aby udowodnić tezę, musimy wykazać, że mamy

$$\sum_{n\geq 0} s_{\lfloor \frac{n}{2} \rfloor} x^n = (1+x)S(x^2)$$

Chcemy więc znaleźć funkcję tworzącą ciągu $s_{\lfloor \frac{n}{2} \rfloor}$. Dla n podzielnego przez 2 mamy $\sum_{n\geq 0} s_n x^{2n}$, natomiast dla n nie podzielnego przez 2 mamy $\sum_{n\geq 0} s_n x^{2n+1}$. Funkcja tworząca ciągu s_n to

$$\sum_{n\geq 0} s_n x^{2n} + \sum_{n\geq 0} s_n x^{2n+1}$$

zatem mamy

$$\sum_{n\geq 0} s_{\lfloor \frac{n}{2} \rfloor} x^n = \sum_{n\geq 0} s_n x^{2n} + \sum_{n\geq 0} s_n x^{2n+1} = S(x^2) + xS(x^2)$$

czyli

$$\sum_{n\geq 0} s_{\lfloor \frac{n}{2} \rfloor} x^n = (1+x)S(x^2)$$

Zatem mamy

$$(1-x)S(x) = (1+x)S(x^2)$$

Zadanie 6.
Udowodnij, że dla $n > 0$ liczba permutacji $\langle a_1, ..., a_n \rangle$ zbioru $\{1, ..., n\}$ takich, że $a_{i+1} - a_i \neq 1$ dla $i = 1, ..., n-1$, jest równa $D_n + (n-1)D_{n-2} + (-1)^{n-1} (= D_n + D_{n-1})$, gdzie D_n to liczba n-nieporządków.

Rozwiązanie:
Wzór na n-nieporządek to $D_n = \sum\limits_{k=0}^{n} (-1)^k \cdot \frac{n!}{k!}$.
Udowodnimy najpierw przez interpretację kombinatoryczną, że liczba takich permutacji jest równa

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

Policzmy dla ustalonego k ile jest takich permutacji (mogą się powtarzać), że co najmniej k par spośród $n-1$ par jest niepoprawna. Z $n-1$ par wybieramy sobie k par, w których będzie zachodziło $a_{i+1} = a_i + 1$. Następnie $n-k$ liczb rozdzielamy na $(n-k)!$ sposobów. Rozkładamy liczby po kolei, a jeśli natrafimy na komórkę, która jest w jakieś parze, to od razu do następnej komórki wkładamy liczbę o jeden większą. Zatem dla ustalonego k liczba takich permutacji, że co najmniej k par spośród $n-1$ jest niepoprawna to $\binom{n-1}{k} \cdot (n-k)!$. Z zasady włączania-wyłączania mamy

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

Udowodnijmy teraz, że

$$\sum_{k=0}^{n} (-1)^k \cdot \binom{n-1}{k} \cdot (n-k)! = D_n + D_{n-1}$$

Mamy

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

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

$$= \sum_{k=0}^{n} (-1)^k \cdot \frac{n!}{k!} - \left(0 + \sum_{k=1}^{n} (-1)^k \cdot \frac{(n-1)!}{k!} \cdot k \right) = D_n + \sum_{k=1}^{n} (-1)^{k-1} \cdot \frac{(n-1)!}{(k-1)!} =$$

$$= D_n + \sum_{k=0}^{n-1} (-1)^k \cdot \frac{(n-1)!}{k!} = D_n + D_{n-1}$$

Zadanie 7.
Uporządkowanym podziałem dodatniej liczby całkowitej n, czyli n-kom-pozycją nazywamy przedstawienie n w postaci sumy dodatnich składników, przy czym kolejność składników w tym przedstawieniu jest istotna (np. wszystkie 3-kompozycje to: $1+1+1$, $1+2$, $2+1$, 3). Udowodnij, że uporządkowanych podziałów liczby n na składniki ≤ 2 jest tyle samo, co uporządkowanych podziałów liczby $n+2$ na składniki ≥ 2.

Rozwiązanie:
Oznaczmy przez a_n liczbę uporządkowanych podziałów liczby n na składniki ≤ 2. Mając podział liczby $n-1$ możemy uzyskać podział liczby n przez dopisanie jedynki na końcu. Mając podział liczby $n-2$ możemy uzyskać podział liczby n przez dopisanie dwójki na końcu. Zatem rekurencyjny wzór na a_n to $a_n = a_{n-1} + a_{n-2}$ dla $n \geq 2$, gdzie $a_0 = a_1 = 1$.

Oznaczmy przez b_n liczbę uporządkowanych podziałów liczby n na składniki ≥ 2. Mając podziały liczb k, gdzie $k \in \{0, 1, 2, ..., n-2\}$ możemy otrzymać podział liczby n, dodając do danego podziału liczbę $n-k$. Zatem rekurencyjny wzór na b_n to $b_n = \sum\limits_{k=0}^{n-2} b_k$ dla $n \geq 2$, gdzie $b_0 = 1$, $b_1 = 0$. Zauważmy, że

$$b_n = b_{n-2} + \sum_{k=0}^{n-3} b_k = b_{n-2} + b_{n-1}$$

Zatem mamy $b_{n+2} = b_{n-1+2} + b_{n-2+2}$, gdzie $b_{1+2} = 1$ oraz $b_{0+2} = 1$.

Jako, że wzór rekurencyjny na liczbę uporządkowanych podziałów liczby $n+2$ na składniki ≥ 2 jest taki sam jak wzór rekurencyjny na liczbę uporządkowanych podziałów liczby n na składniki ≤ 2 oraz warunki brzegowe są takie same, to teza jest prawdziwa.

Zadanie 8.
Niech $W_k(n)$ oznacz liczbę podziałów n na składniki większe bądź równe k, zaś $M_k(n)$ oznacza liczbę podziałów n na składniki mniejsze bądź równe k, w szczególności $W_k(0) = M_k(0) = 1$ dla $k > 0$. Udowodnij, że dla $n > 0$ zachodzi $\sum\limits_{k\geq 1}(M_k(n-k) - W_k(n-k)) = 0$.

Rozwiązanie:
Równoważnie możemy napisać

$$\sum_{k\geq 1} M_k(n-k) = \sum_{k\geq 1} W_k(n-k)$$

Mając podział liczby $n-k$ na składniki większe, bądź równe k, dodając do tego składnik o wielkości k otrzymujemy podział liczby n. Zatem podziałów liczby $n-k$ na skłądniki większe, bądź równe k jest tyle samo, co podziałów liczby n, gdzie najmniejszy składnik ma wielkość k.

Mając podział liczby $n-k$ na składniki mniejsze, bądź równe k, dodając do tego składnik o wielkości k otrzymujemy podział liczby n. Zatem podziałów liczby $n-k$ na skłądniki mniejsze, bądź równe k jest tyle samo, co podziałów liczby n, gdzie największy składnik ma wielkość k.

Po lewej i po prawej stronie zliczamy więc wszystkie podziały liczby n. Zatem

$$\sum_{k\geq 1} M_k(n-k) = \sum_{k\geq 1} W_k(n-k)$$

Zadanie 9.
Rozwiąż równanie rekurencyjne $f_n = \frac{2n-1}{n} f_{n-1} - \frac{n-1}{n} f_{n-2} + 1$, $f_0 = 0$, $f_1 = 1$.

Rozwiązanie:
Uprośćmy wyrażenie, mnożąc stronami przez n. Mamy

$$nf_n = (2n-1)f_{n-1} - (n-1)f_{n-2} + n$$

czyli

$$n(f_n - f_{n-1}) = (n-1)(f_{n-1} - f_{n-2}) + n$$

Podstawmy teraz $a_n = n \cdot (f_n - f_{n-1})$. Wówczas mamy $a_n = a_{n-1} + n$ gdzie $a_1 = 1$, zatem mamy

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

Dalej mamy

$$n \cdot (f_n - f_{n-1}) = \frac{n \cdot (n+1)}{2} \Leftrightarrow f_n = f_{n-1} + \frac{n+1}{2} = \frac{n(n+3)}{4}$$

Zadanie 10.
Jakie jest prawdopodobieństwo, że w losowej 6-permutacji 1 i 2 są w tym samym cyklu, a 3 w innym?

Rozwiązanie:
Rozważmy SUPERNAPIS. Aby 1 i 2 były ze sobą w cyklu, to muszą być w kolejności 1 2. Aby trójka nie była z nimi w cyklu, to musi być przed nimi, czyli kolejność tych trzech elementów będzie następująca 3 1 2. Po między tymi elementami mogą znaleźć się dowolne inne elementy. Permutacji liczb 1 2 i 3 jest oczywiście $3! = 6$, zatem prawdopodobieństwo tego, że 1 i 2 są w tym samym cyklu, a 3 w innym wynosi $\frac{1}{6}$. Jest ono niezależne od liczby elementów w permutacji.

Zadanie 11.
Udowodnij tożsamość $\binom{i+j}{i} \left\{ {n \atop i+j} \right\} = \sum_{k=0}^{n} \binom{n}{k} \left\{ {k \atop j} \right\} \left\{ {n-k \atop j} \right\}$.

Rozwiązanie:
Zinterpretujmy kombinatorycznie lewą stronę. Dzielimy stado n królików na $i+j$ pasztetów, a następnie z $i+j$ pasztetów wybieramy i, które będą zjedzone dziś na kolację. Pozostałe j pasztetów będzie zjedzona jutro na kolację. Mamy więc $\binom{i+j}{i} \left\{ {n \atop i+j} \right\}$ sposobów podziału.
Zinterpretujmy kombinatorycznie prawą stronę. Mamy sobie n królików. Dla ustalonego k, wybieramy z n królików k królików, które będą w dzisiejszym pasztecie, a pozostałe $n-k$ królików będzie w jutrzejszym pasztecie. Następnie dzisiejsze króliki dzielimy na i pasztetów, a jutrzejsze króliki dzielimy na j pasztetów. Dla ustalonego k mamy więc $\binom{n}{k} \left\{ {k \atop j} \right\} \left\{ {n-k \atop j} \right\}$ sposobów podziału.
Sumując po liczbie królików w dzisiejszym pasztecie otrzymujemy $\sum_{k=0}^{n} \binom{n}{k} \left\{ {k \atop j} \right\} \left\{ {n-k \atop j} \right\}$.

Zadanie 12.
Znajdź $\sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{F_{2k} F_{n-k}}{10^n}$, gdzie F_n to n-ta liczba Fibonacciego.

Rozwiązanie:
Jeśli $x = \frac{1}{10}$, to mamy

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n} F_{2k}F_{n-k}x^n = \left(\sum_{n=0}^{\infty} F_{2n}x^n\right) \cdot \left(\sum_{n=0}^{\infty} F_n x^n\right)$$

Funkcją tworzącą liczb Fibonacciego, gdzie $F_0 = F_1 = 1$ jest $\frac{1}{1-x-x^2}$. Wyznaczmy funkcję tworzącą ciągu F_{2n}.
Niech $G_n = F_{2n}$ oraz $H_n = F_{2n+1}$. Mamy więc

$$\begin{cases} G_n = G_{n-1} + H_{n-1} + [n = 0] \\ H_n = H_{n-1} + G_n \end{cases}$$

Jeśli przez $G(x)$ oznaczymy funkcję tworzącą G_n oraz przez $H(x)$ oznaczymy funkcję tworzącą H_n, to mamy

$$\begin{cases} G(x)(1 - x) = xH(x) + 1 \\ H(x)(1 - x) = G(x) \end{cases}$$

skąd otrzymujemy

$$\begin{cases} G(x) = \frac{1-x}{x^2-3x+1} \\ H(x) = \frac{1}{(1-x^2)-x} \end{cases}$$

Zatem mamy

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n} F_{2k}F_{n-k}x^n = \frac{1-x}{x^2-3x+1} \cdot \frac{1}{1-x-x^2}$$

gdzie $x = \frac{1}{10}$.

Zadanie 13.
Udowodnij tożsamość: $\sum\limits_{i=0}^{k} \binom{n}{i} = \sum\limits_{i=0}^{k} \binom{n-1-i}{k-i} 2^i$ dla $0 \le k \le n$.

Rozwiązanie:
Zinterpretujmy kombinatorycznie lewą stronę. Dzielimy n króliki na dwa pasztety, przy czym chcemy, aby w dzisiejszym pasztecie nie było więcej niż k królików. Dla ustalonego i, z n królików wybieramy i, które będą w dzisiejszym pasztecie. Robimy to na $\binom{n}{i}$ sposobów. Zatem łączna liczba podziałów jest równa $\sum\limits_{i=0}^{k} \binom{n}{i}$.
Zinterpretujmy kombinatorycznie prawą stronę. Ustawiamy króliki w szereg. Dla ustalonego i przechodzimy od lewej do prawej i dla pierwszysch i królików wybieramy te które pójdą do pasztetu dzisiejszego i te które pójdą do pasztetu jutrzejszego. Następnie $i + 1$ królik pójdzie do pasztetu jutrzejszego i z pozostałych $n - 1 - i$ króliów wybieramy $k - i$ królików które pójdą do pasztetu dzisiejszego.
Chcemy podzielić n królików na dzisiejszy pasztet wielkości co najwyżej k. Ustalmy więc wielkość tego pasztetu jako k. Gdy dla pierwszych i królików wybieramy królika, to nie zmniejszamy wielkości pasztetu. Gdy królika nie wybieramy, to zmniejsza się nam rozmiar pasztetu o 1. Gdybyśmy próbowali utworzyć taki sam pasztet dla innego i, to wielkość pasztetu by się zmieniła, ponieważ

$i+1$ królik nie jest w pasztecie dzisiejszym. Zatem otrzymujemy różne wybory co najwyżej k królików na dzisiejszy pasztet z n królików. Liczba wyborów co najwyżej k królików na pasztet dzisiejszy jest więc równa $\sum_{i=0}^{k}\binom{n-1-i}{k-i}2^i$.

Zadanie 14.
Uprość sumę $\sum_{p+q+r=n} 2^p3^q5^r$ dla $p,g,r\in\mathbb{N}$. Zakładamy, że $0\in\mathbb{N}$.

Rozwiązanie:
Funkjca tworząca ciągu $a_n=\sum_{p+q+r=n}2^p3^q5^r$ to $A(x)=\sum_{n=0}^{\infty}\left(\sum_{p+q+r=n}2^p3^q5^r\right)x^n$. Mamy tu splot trzech funkcji tworzących, zatem

$$A(x)=\left(\sum_{n=0}^{\infty}2^nx^2\right)\cdot\left(\sum_{n=0}^{\infty}3^nx^2\right)\cdot\left(\sum_{n=0}^{\infty}5^nx^2\right)=\frac{1}{1-2x}\cdot\frac{1}{1-3x}\cdot\frac{1}{x-5x}=$$

$$=-\frac{1}{30}\cdot\frac{1}{\left(x-\frac{1}{2}\right)\left(x-\frac{1}{3}\right)\left(x-\frac{1}{5}\right)}$$

Chcemy znaleźć takie a,b,c, że $A(x)=-\frac{1}{30}\left(\frac{a}{x-\frac{1}{2}}+\frac{b}{x-\frac{1}{3}}+\frac{c}{x-\frac{1}{5}}\right)$. Czyli

$$a\left(x-\frac{1}{3}\right)\left(x-\frac{1}{5}\right)+b\left(x-\frac{1}{2}\right)\left(x-\frac{1}{5}\right)+c\left(x-\frac{1}{2}\right)\left(x-\frac{1}{3}\right)=1$$

czyli

$$a\left(x^2-\frac{8}{15}x+\frac{1}{15}\right)+b\left(x^2-\frac{7}{10}x+\frac{1}{10}\right)+c\left(x^2-\frac{5}{6}x+\frac{1}{6}\right)=1$$

Po rozwiązaniu układu trzech równań z trzema niewiadomymi mamy $a=20$, $b=-45$ oraz $c=25$, zatem

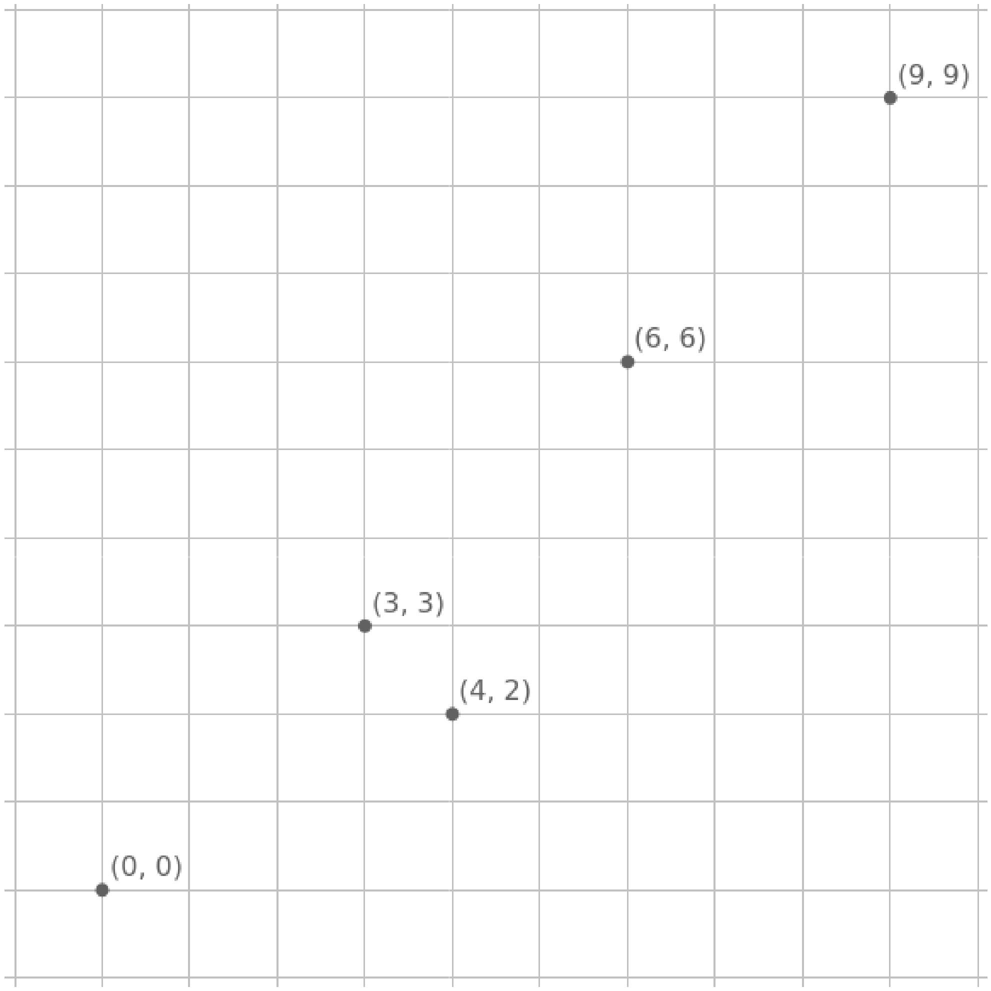
$$A(x)=\frac{1}{30}\left(40\cdot\frac{1}{1-2x}-135\cdot\frac{1}{1-3x}+125\cdot\frac{1}{1-5x}\right)=$$

$$=\frac{1}{30}\left(40\cdot\sum_{n=0}^{\infty}2^nx^2-135\sum_{n=0}^{\infty}3^nx^2+125\sum_{n=0}^{\infty}5^nx^n\right)=\sum_{n=0}^{\infty}\left(\frac{40}{30}2^n-\frac{135}{30}3^n+\frac{125}{30}5^n\right)x^n$$

skąd otrzymujemy $\sum_{p+q+r=n}2^p3^q5^r=\frac{40}{30}2^n-\frac{135}{30}3^n+\frac{125}{30}5^n$.

Zadanie 15.
Znajdź liczbę przechodzących w prawo i do góry dróg na kratownicy o początku $\langle 0,0\rangle$ i końcu $\langle 9,9\rangle$, które przechodzą przez dokładnie jeden z punktów $\langle 3,3\rangle$, $\langle 4,2\rangle$, $\langle 6,6\rangle$.

Rozwiązanie:



Wszystkich dróg z $\langle 0,0\rangle$ do $\langle 9,9\rangle$ przechodzących przez punkt $\langle 3,3\rangle$ jest $d(3,3)\cdot d(6,6)$. Wszystkich dróg z $\langle 0,0\rangle$ do $\langle 9,9\rangle$ przechodzących przez punkt $\langle 4,2\rangle$ jest $d(4,2)\cdot d(5,7)$. Wszystkich dróg z $\langle 0,0\rangle$ do $\langle 9,9\rangle$ przechodzących przez punkt $\langle 6,6\rangle$ jest $d(6,6)\cdot d(3,3)$.

Wszystkich dróg z $\langle 0,0\rangle$ do $\langle 9,9\rangle$ przechodzących przez punkt $\langle 3,3\rangle$ i punkt $\langle 6,6\rangle$ jest $d(3,3)\cdot d(3,3)\cdot d(3,3)$. Wszystkich dróg z $\langle 0,0\rangle$ do $\langle 9,9\rangle$ przechodzących przez punkt $\langle 4,2\rangle$ i punkt $\langle 6,6\rangle$ jest $d(4,2)\cdot d(2,4)\cdot d(3,3)$. Nie ma natomiast dróg przechodzących przez punkty $\langle 3,3\rangle$ i punkt $\langle 4,2\rangle$.

Nie ma dróg przechodzących przez wszystkie trzy punkty.

Z zasady Włączania-Wyłączania mamy więc $d(3,3)\cdot d(6,6)+d(4,2)\cdot d(5,7)+d(6,6)\cdot d(3,3)-d(3,3)\cdot d(3,3)\cdot d(3,3)-d(4,2)\cdot d(2,4)\cdot d(3,3)-0+0=36340$.

Zadanie 16.
Oblicz prawdopodobieństwo tego, że w losowej n-permutacji żadne dwie liczby parzyste nie są w tym samym cyklu.

Rozwiązanie:
Rozważmy zmodyfikowany SUPERNAPIS. Jeśli w cyklu jest liczba parzysta, to ustawiamy cykl tak, że najmniejsza liczba parzysta stoi na początku. Jeśli w cyklu nie ma liczby parzystej, to na początku stoi po prostu najmniejsza liczba. Następnie cykle sortujemy po w porządku malejącym,

po pierwszym elemencie z cyklu.

$$[3\ 2\ 5\ 6]\ [1\ 4\ 7]\ [8]\ [11\ 9]\ [10] = [2\ 5\ 6\ 3]\ [4\ 7\ 1]\ [9\ 11]\ [10] = 10\ 9\ 11\ 4\ 7\ 1\ 2\ 5\ 6\ 3$$

Aby liczby żadne dwie liczby parzyste nie były w jednym cyklu, to liczby parzyste muszą być w porządku malejącym. Wszystkich n-permutacji jest $n!$, natomiast (jako, że liczb parzystych jest $\lfloor \frac{n}{2} \rfloor$) liczba n-permutacji, gdzie liczby parzyste są w porządku malejącym, jest równa $\frac{n!}{\lfloor \frac{n}{2} \rfloor !}$. Zatem prawdopodobieństwo tego, że żadne dwie liczy parzyste nie są w tym samym cyklu jest równe $\frac{1}{\lfloor \frac{n}{2} \rfloor !}$.

Zadanie 17.
Znajdź liczbę przedstawień liczby naturalnej n w postaci sumy pewnej liczby nieujemnych składników całkowitych, przy czym istotna jest kolejność składników, a z każdych dwóch kolejnych składników co najmniej jeden jest dodatni. PRZYKŁAD: dla $n = 2$ jest 12 takich przedstawień: $0+1+0+1$, $0+1+0+1+0$, $0+1+1$, $0+1+1+0$, $0+2$, $0+2+0$,$1+0+1$ $1+0+1+0$, $1+1$, $1+1+0$, 2, $2+0$.

Rozwiązanie:
Liczbę n podzielimy najpierw na k składników, a następnie w $k+1$ miejsc będziemy mogli wpisać 0. Podziałów liczby n na k dodatnich składników jest $\binom{n-1}{k-1}$. Wyborów miejsc dla 0 dla ustalonego k mamy 2^{k+1}, ponieważ dla każdego miejsca, można wybrać, czy zero się tam wstawia czy nie. Zatem dla ustalonego k mamy $\binom{n-1}{k-1} \cdot 2^{k+1}$ takich przedstawień. Sumując po k otrzymujemy

$$\sum_{k=0}^{n} \binom{n-1}{k-1} \cdot 2^{k+1} = 4 \cdot \sum_{k=1}^{n} \binom{n-1}{k-1} 2^{k-1} = 4 \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} 2^{k} = 4 \cdot 3^{n-1}$$

Ćwiczenia 10

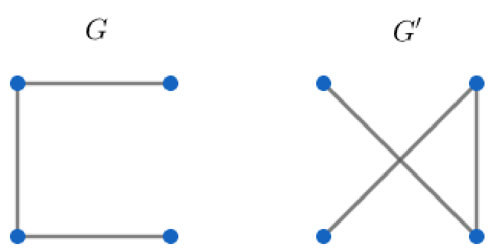
Grafy - podstawowe pojęcia

Zadanie 10.1.
Udowodnij, że na każdym przyjęciu są dwie osoby o takiej samej liczbie znajomych.

Rozwiązanie:
Niech osoby na imprezie oznaczają wierzchołki grafu oraz niech krawędzie grafu to znajomości osób. Chcemy pokazać, że istnieją wierzchołki, które mają taki sam stopień. Załóżmy więc przeciwnie, że taki wierzchołek nie istnieje. Wówczas mamy wierzchołki o stopniach odpowiednio $0, 1, 2, ..., n-1$. Skoro istnieje osoba, która zna $n-1$ osób, to zna wszystkich pozostałych, zatem nie może istnieć osoba, która będzie miała 0 znajomych.

Zadanie 10.2.
Udowodnij, że przynajmniej jeden z grafów G, G' (dopełnienie) jest spójny.
Niech $diam(G)$ oznacza średnicę grafu G (nieskończoność jeśli G jest niespójny) i niech $f(G) = min(diam(G), diam(G'))$. Znajdź $sup f(G)$ po wszystkich grafach G.

Rozwiązanie:
Udowodnijmy najpierw, że przynajmniej jeden z grafów G, G' jest spójny. Rozważmy spójne składowe grafu G, który nie jest spójny, wówczas istnieje spójna która nie łączy się z pozostałymi. Weźmy teraz dwa wierzchołki z różnych spójnych składowych v, w. Są one połączone w dopełnieniu G', ponieważ nie były połączone w grafie G. Dwa wierzchołki v, u leżące w jednej spójnej składowej są połącznone wierzchołkiem w leżącym w innej spójnej składowej. Zatem dopełnienie jest spójne. Wiemy zatem, że $\text{diam}(G) < \infty$ lub $\text{diam}(G') < \infty$, zatem $\min(\text{diam}(G), \text{diam}(G')) < \infty$. Istnieje ponadto graf taki, że $\text{diam}(G) = 3$ oraz $\text{diam}(G') = 3$.

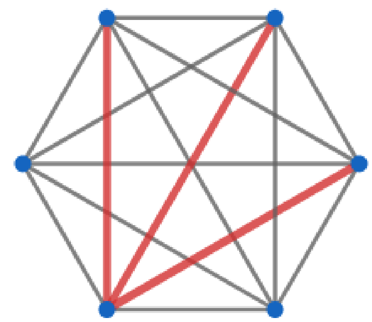


Udowodnijmy teraz, że nie istnieje graf, w którym $\min(\text{diam}(G), \text{diam}(G') > 3$. Czyli skoro wiemy, że $\min(\text{diam}(G), \text{diam}(G') \geq 3$, to wystarczy pokazać, że $\min(\text{diam}(G), \text{diam}(G') \leq 3$. Załóżmy więc, że $\min(\text{diam}(G), \text{diam}(G') \leq 3$. Weźmy więc dwa wierzchołki v, w w grafie G oddalone od siebie o 3. Każdy wierzchołek u w grafie G może być połączony z maksymalnie jednym z wierzchołków v, w, ponieważ w przeciwnym razie odległość wierzchołków v, w byłaby nie większa niż 2. Zatem każdy wierzchołek w grafie G' jest połączony z v lub z w. W grafie G' wierzchołki v, w są połączone ze sobą, ponieważ nie były połączone ze sobą w grafie G. Czyli dla dowolnych wierzchołków u, t mamy ścieżki (u, v, t) lub (u, w, t) lub (u, v, w, t). Zatem $\text{diam}(G') \geq 3$. Skąd $\min(\text{diam}(G), \text{diam}(G') \leq 3$, czyli $\sup f(G) = 3$.

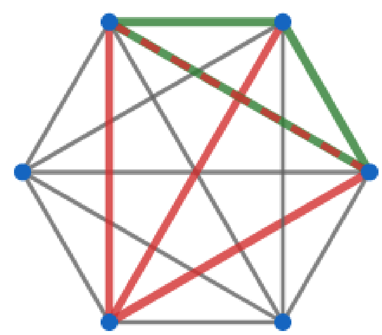
Zadanie 10.3.
Udowodnij, że w K_6 dowolnie pokolorowanym krawędziowo na 2 kolory jest monochromatyczny

trójkąt (są nawet dwa!), ale w K_5 niekoniecznie.

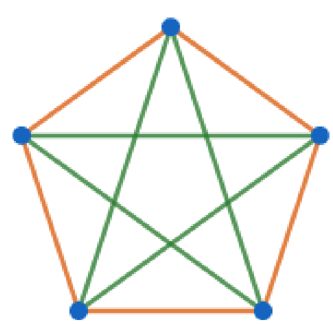
Rozwiązanie:
Z każdego wierzchołka wychodzi 5 krawędzi, zatem co najmniej 3 muszą mieć taki sam kolor.



Bierzemy końce tych trzech krawędzi i teraz one tworzą trójkąt. Jak nie pomalujemy go całego na drugi kolor, to domkniemy pierwszy trójkąt, natomiast jak pomalujemy to i tak otrzymamy trójkąt.



Podamy przykład takiego kolorowania K_5 na dwa kolory, że nie ma w nim trójkąta monochromatycznego.



Zadanie 10.4.
Rozstrzygnij, czy istnieje:

a) graf o ciągu stopni wierzchołków (3 3 3 3 5 6 6 6 6 6 6)

b) (3 3 3 3 3 5 6 6 6 6 6 6)

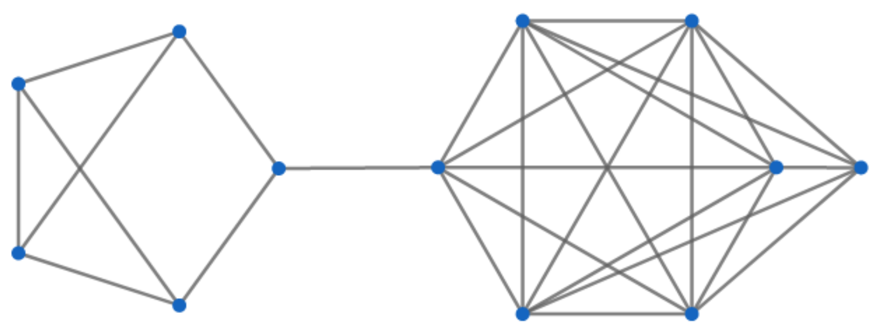
c) dwudzielny (3 3 3 3 3 5 6 6 6 6 6 6)

d) drzewo (dowolny ciąg długości n o sumie $2n-2$)

Rozwiązanie:

a) W grafie każda krawędź ma dwa końce, zatem suma stopni wierzchołków musi być parzysta. Nie może istnieć zatem graf, gdzie wierzchołki mają stopnie (3 3 3 3 5 6 6 6 6 6 6).

b) Taki graf istnieje.

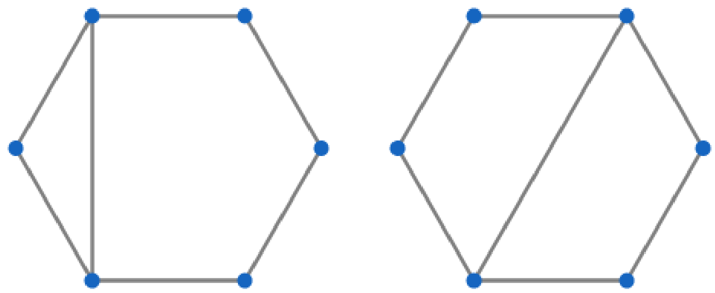


c) Każda krawędź ma jeden koniec z lewej strony i jeden koniec z drugiej strony grafu, zatem suma stopni po obu stronach jest jednakowa. Musimy więc mulitizbiór (3 3 3 3 3 5 6 6 6 6 6 6) podzielić na dwie części o równej sumie. Mamy jedną liczbę niepodzielną przez 3, zatem jedna z części będzie miała sumę podzielną przez 3, a druga będzie miała sumę niepodzielną przez 3. Te części nie będą więc sobie równe. Zatem taki graf nie istnieje.

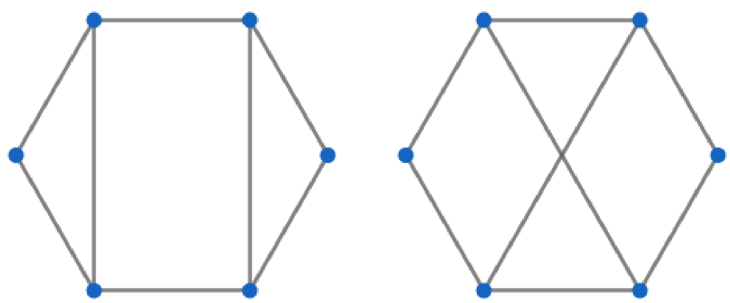
d) Chcemy pokazać, że dla dowolnego ciągu $(d_1\ d_2\ ...\ d_n)$ takiego, że $\sum\limits_i d_i = 2n-2$ oraz $d_i > 0$ i $n > 1$ istnieje drzewo o takim ciągu stopni wierzchołków. Udowodnimy to przez indukcję. Niech $P(n)$ oznacza, że dla dowolnego n ciągu liczb naturalnych dodatnich sumujących się do $2n-2$ istnieje drzewo o takim ciągu stopni. Dla $n = 2$ mamy ciąg (1 1), czyli po prostu dwa wierzchołki połączone krawędzią. Zatem prawdziwe jest $P(2)$. Załóżmy więc, że $P(n)$ jest prawdziwe dla pewnego n. Chcemy udowodnić, że prawdziwe jest $P(n+1)$. Mamy ciąg $d_1\ d_2\ ...\ d_n$ taki, że $\sum\limits_i d_i = 2n$ oraz $d_i > 0$. Chcemy pokazać, że istnieje drzewo o takim ciąfu stopni wierzchołków. W ciągu istnieje 1, bo gdyby wszystkie stopnie były co najmniej 2, to suma stopnie byłaby co najmniej równa $2(n+2)$. W ciągu największa liczba jest równa co najmniej 2, bo w przeciwnym razie suma stopni byłaby równa $n+1$. Mamy więc sobie ciąg $d_1\ d_2\ ...\ d_n\ d_{n+1}$. Z tego ciągu zabieramy d_k o stopniu 1 oraz maksymalny stopień zmniejszamy o 1. Otrzymaliśmy teraz ciąg n elementowy, zatem wiemy, że istnieje dla niego drzewo z założenia indukcyjnego. Robimy więc z tego ciągu drzewo, a następnie dodajemy liść do tego wierzchołka, któremu zmniejszyliśmy stopień. W ten sposób dostajemy drzewo o ciągu stopni $(d_1\ d_2\ ...\ d_n)$. Zatem prawdziwe jest również $P(n) \Rightarrow P(n+1)$.

Zadanie 10.5.
Podaj przykład dwóch nieizomorficznych grafów spójnych o takich samych ciągach stopni wierzchołków.

Rozwiązanie:
Przykładowe grafy znajdują się na poniższych rysunkach.



Oba grafy mają stopnie wierzchołków odpowiednio równe 2 2 2 2 3 3. Jednak te grafy nie są izomorficzne.



Oba grafy mają stopnie wierzchołków odpowiednio równe 2 2 3 3 3 3. Jednak te grafy nie są izomorficzne.

Zadanie 10.6.
Graf niezorientowany jest orientowalny, jeśli można na jego krawędziach dorysować strzałki tak, żeby dostać digraf silnie spójny. Pokaż, że graf spójny jest orientowalny wtedy i tylko wtedy, gdy nie ma mostów.

Rozwiązanie:
Pokażemy najpierw, że jeśli graf spójny jest orientowalny to nie ma w nim mostów. Załóżmy nie wprost, że w grafie orientowalnym istnieje most. Skoro istnieje most to z jednej części da się przejść do drugiej, jednak z tej drugiej nie da się przejść do pierwszej, czyli graf nie jest silnie spójny. Otrzymując sprzeczność, wykazaliśmy że jeśli graf spójny jest orientowalny to nie ma w nim mostów.

Pokażemy teraz, że jeśli graf nie ma mostów to jest orientowalny. Skoro graf nie ma mostów, to między dowolnymi dwoma wierzchołkami istnieją dwie różne ścieżki, czyli równoważnie każda krawędź należy do jakiegoś cyklu. Weźmy więc dowolną krawędź w grafie. Wiemy, że należy ona do jakiegoś cyklu, zatem orientujemy sobie wszystkie krawędzie w tym cyklu w jedną stronę. Następnie bierzemy niezorientowaną krawędź, która będzie incydentna z jakąś zorientowaną krawędzią. Ta krawędź również należy do jakiegoś cyklu. Orientujemy więc ten cykl, zgodnie z orientacją zorientowanej krawędzi. Graf nasz będzie podzielony na dwie części: tę zorientowaną, która jest silnie spójna, ponieważ każda krawędź leży w jakimś zorientowanym cyklu; oraz tę niezorientowaną. Orientujemy więc krawędzie nieskierowane zgodnie z powyższą metodą. Po skończonej liczbie powtórzeń powyższej procedury dostajemy zorientowany graf, w którym każda krawędź należy do jakiegoś zorientowanego grafu. Otrzymaliśmy więc graf silnie spójny.

Ćwiczenia 11

Drzewa, cykle Eulera i Hamiltona

Zadanie 11.1.
Centrum grafu G to zbiór wierzchołków v, dla których $\max_w d(v, w)$ jest najmniejsze. Udowodnij, że centrum drzewa to pojedynczy wierzchołek albo para wierzchołków połaczonych krawędzią.

Rozwiązanie:
W drzewie istnieje choć jeden liść. Liść nie może być centrum, ponieważ od jego jedynego sąsiada jest bliżej do pozostałych wierzchołków. Zatem usuwając wszystkie liście z grafu, na pewno nie usuwamy jego centrum. Zawuażmy, że maksimum odległości od dowolnego wierzchołka v jest w jakimś liściu. Usuwając wszystkie liście zmniejszamy tę wartość o 1. Zmienia się ona dla każdego wierzchołka, zatem nadal jest najmniejsza w centrum grafu. Po usunięciu liści z drzewa, zostaje nam drzewo, które też ma liście. Będziemy więc usuwać liście do momentu aż w grafie nie zostanie jeden lub dwa wierzchołki. Te wierzchołki to centrum grafu.

Zadanie 11.2.
Udowodnij twierdzenie Cayleya o zliczaniu drzew etykietowanych: K_n ma n^{n-2} drzew rozpinających wskazując bijekcję między takimi drzewami a $(n-2)$-ciągami o elementach ze zbioru $\{1, ..., n\}$ (kody Prufera);

Rozwiązanie:
(Z wikipedii) Kod Prüfera – kod pozwalający na zapisywanie drzewa (w rozumieniu teorii grafów) w formie skompresowanego ciągu (bez wypisywania całego zbioru krawędzi) długości $n - 2$, gdzie n stanowi liczbę wierzchołków grafu.

Wyznaczanie kodu Prüfera
Algorytm wyznaczania kodu Prüfera na podstawie opisu drzewa. Z danego drzewa o zbiorze wierzchołków opisanym jako $\{1, 2, ..., n\}$ prowadzi do kodu Prüfera stanowiącego $n - 2$ wyrazowy ciąg liczb ze zbioru $\{1, 2, ..., n\}$.

1. Jeśli w drzewie jest więcej niż jedna krawędź, szukamy w drzewie wierzchołka stopnia jeden o jak najniższym numerze ze zbioru $\{1, 2, ..., n\}$ nazwijmy go v. Znajdujemy jedynego sąsiada tego wierzchołka, nazwijmy go w.
2. Do ciągu wyjściowego dopisujemy w, usuwamy krawędź $\{v, w\}$
3. Jeśli w drzewie została więcej niż jedna krawędź to przejść ponownie do punktu pierwszego. W przeciwnym wypadku, zapisany dotychczas ciąg jest ciągiem wyjściowym.

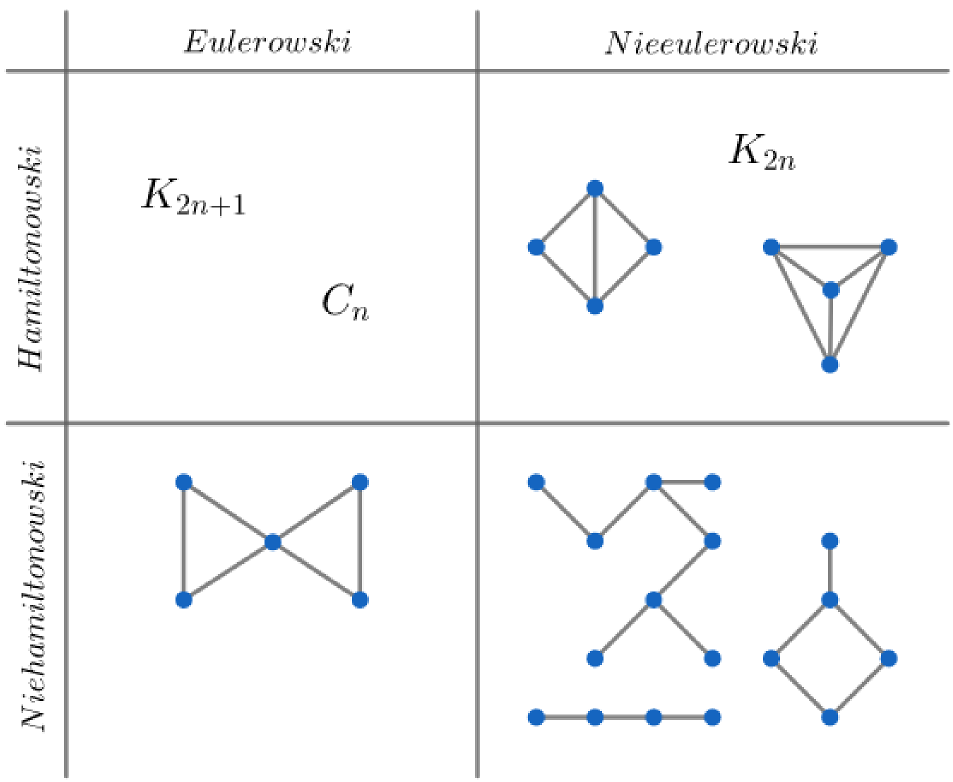
Wyznaczanie drzewa z kodu Prüfera
Algorytm wyznaczania opisu grafu na podstawie kodu Prüfera. Z danego kodu Prüfera stanowiącego $n - 2$ wyrazowy ciąg liczb $(a_1, a_2, ..., a_{n-2})$ ze zbioru $\{1, 2, ..., n\}$ prowadzi do opisu drzewa o zbiorze wierzchołków $\{1, 2, ..., n\}$ z kodem Prüfera $(a_1, a_2, ..., a_{n-2})$.

1. Tworzymy dwie listy $L_1 = (a_1, a_2, ..., a_{n-2})$, $L_2 = \{1, 2, ..., n\}$. Drzewo zaczynamy tworzyć od grafu o wierzchołkach $\{1, 2, ..., n\}$ i wyłącznie trywialnych składowych (pusty zbiór krawędzi). Wyznaczmy sobie liczbę $c := 1$.

2. Wyznaczamy w L_2 najmniejszą wartość, która nie występuje w liście L_1 nazwijmy ją i.
3. Dodajemy do drzewa krawędź $\{i, a_c\}$. Z listy L_1, usuwamy a_c. Z listy L_2, usuwamy i.
4. Jeśli L_1 jest niepuste to definiujemy $c := c + 1$ i wracamy do punktu 2. W przeciwnym wypadku L_2 zawiera jeszcze dwa elementy, nazwijmy je l_1 i l_2. Do zbioru krawędzi drzewa dodajemy krawędź $\{l_1, l_2\}$ i kończymy działanie algorytmu.

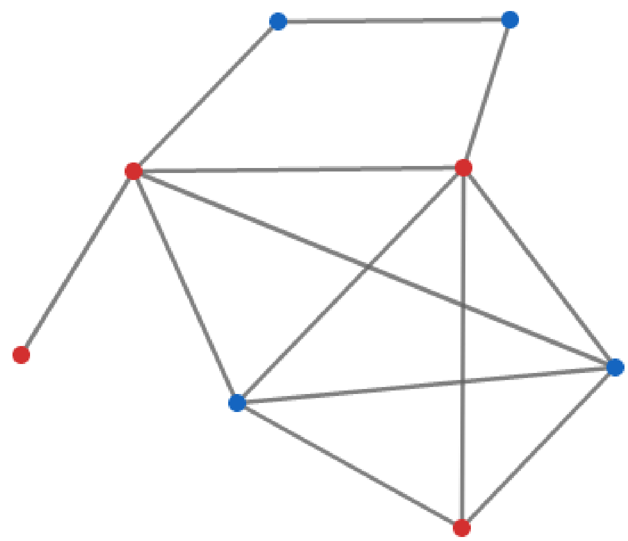
Zadanie 11.3.
Podaj przykłady grafów na wszystkie cztery kombinacje: (istnieje/nie istnieje)×(cykl Eulera/cykl Hamiltona)

Rozwiązanie:

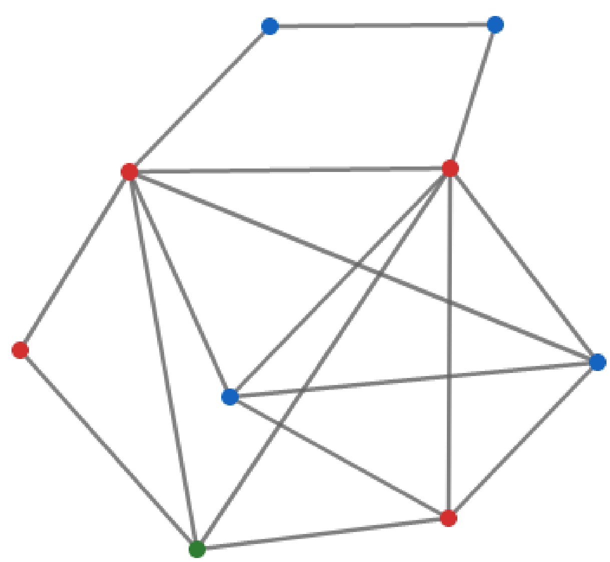


Zadanie 11.4.
Udowodnij, ze jeśli G jest spójny o $k > 0$ wierzchołkach nieparzystych stopni, to k jest parzyste i $\frac{k}{2}$ jest najmniejszą liczbą krawędziowo rozłącznych łańcuchów pokrywających wszystkie krawędzie grafu G.

Rozwiązanie:
W grafie suma stopni wierzchołków musi być parzysta, zatem wierzchołków o nieparzystych stopniach jest parzyście wiele. Ścieżka niebędąca cyklem musi zaczynać się w wierzchołku o stopniu nieparzystym oraz kończyć w wierzchołku o stopniu nieparzystym. Zatem ścieżek w grafie mamy co najmniej $\frac{k}{2}$.



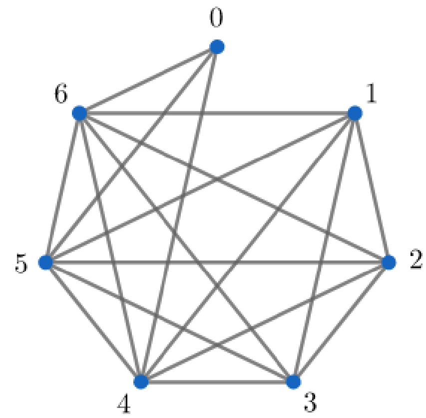
Dorysowujemy do naszego grafu dodatkowy wierzchołek i łączymy go z wierzchołkami o stopniu nieparzystym.



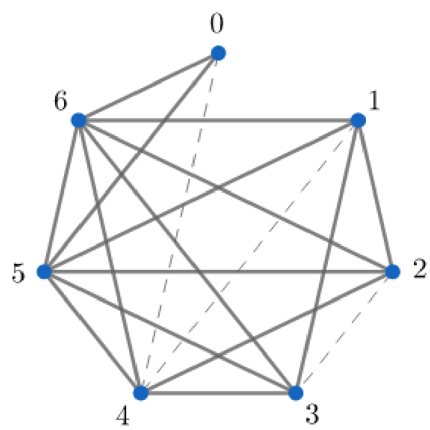
W ten sposób otrzymujemy graf, w którym każdy wierzchołek ma parzysty stopień, a zatem istnieje w nim cykl Eulera. Usuwając dodatkowy wierzchołek otrzymujemy graf, który ma co najwyżek $\frac{k}{2}$ ścieżek. Zatem $\frac{k}{2}$ jest najmniejszą liczbą krawędziowo rozłącznych łańcuchów pokrywających wszystkie krawędzie.

Zadanie 11.5.
Z kompletu 28 kamieni domina (od $0-0$ do $6-6$) usuwamy kamienie $0-1$, $0-2$, $0-3$. Ile jeszcze trzeba usunąć, żeby resztę dało się ułożyć w łańcuch zamknięty?

Rozwiązanie:
Potraktujemy liczby jak wierzchołki grafu oraz płytki jako krawędzie.



Chcemy usunąć kilka krawędzi tak, aby można było przejść potem po wszystkich krawędziach. Chcemy więc usunąć krawędzie tak, aby w grafie otrzymać cykl Eulera. Każdy wierzchołek musi mieć stopień parzysty. Musimy więc zabrać jedną krawędź wychodzącą z wierzchołka 0. Wierzchołek ten łączy się z wierzchołkami 4, 5 oraz 6, zatem usuwamy jedną z krawędzi $0-4$, $0-5$ lub $0-6$. Załóżmy że usunęliśmy krawędź $0-4$. Teraz wierzchołek 4 ma stopień nieparzysty. Nieparzyste stopnie mają też wierzchołki 1, 2 oraz 3. Usuńmy więc krawędzie $1-4$ oraz $2-3$ by uzyskać graf w którym istnieje cykl Eulera.



Trzeba więc usunąć co najmniej trzy krawędzie.

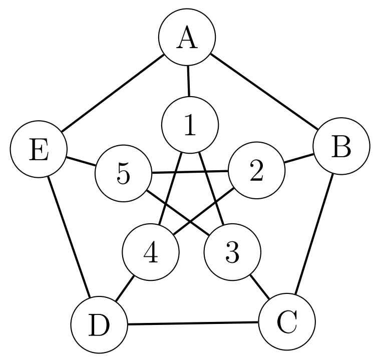
Zadanie 11.6.
Które pełne grafy dwudzielne i trójdzielne są eulerowskie, a które hamiltonowskie?

Rozwiązanie:
Aby graf pełny dwudzielny $K_{n,m}$ był eulerowski, to po obu stronach musi być parzyście wiele wierzchołków, bo graf jest eulerowski wtedy i tylko wtedy gdy każdy wierzchołek ma parzysty stopień. Zatem $2|m$ oraz $2|n$.
Aby graf pełny dwudzielny $K_{n,m}$ był hamiltonowski, to po obu stronach musi być tyle samo wierzchołków, bo przechodząc po cyklu zmieniamy na zmianę strony. Zatem $m = n$.
Aby graf pełny trójdzielny $K_{a,b,c}$ był eulerowski, odpowiednie pary grup muszą mieć parzyście wiele wierzchołków, bo te wierzchołki z trzeciej grupy są z nimi połączone. Zatem $2|a+b$, $2|b+c$ oraz $2|c+a$.

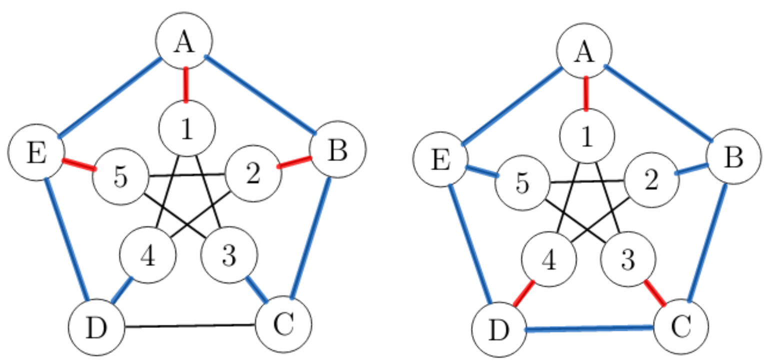
Rozważmy teraz grafy trójdzielne $K_{a,b,c}$ w których istnieje cykl hamiltona. Dla $a = b = c$ istnieje cykl, ponieważ możemy chodzić po grafie w kółko. Dla $a = b + c$ również istnieje cykl hamiltona, bo mamy wówczas graf dwudzielny, gdzie po jednej stronie mamy a wierzchołków, natomiast po drugiej stronie mamy $b + c$ wierzchołków. Gdy mamy $a \geq b \geq c$ oraz $b + c \geq a$ to istnieje cykl hamiltona, bo można przejść najpierw $b+c-a$ razy między wierzchołkami z grupy b i c, a następnie potraktować graf jako graf dwudzielny i przechodzić między wierzchołkami a oraz b lub a oraz c. Gdy $a > b + c$ to nie istnieje cykl hamiltona, bo za dużo krawędzi wychodzi z a.

Zadanie 11.7.
Pokaż, że graf Petersena jest maksymalny niehamiltonowski.

Rozwiązanie:

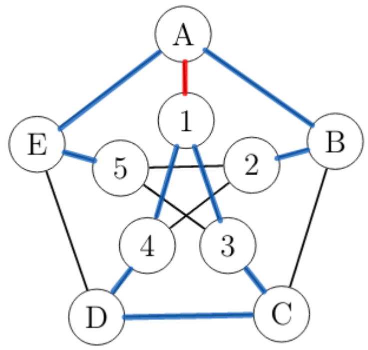


Krawędzie łącznikowe to krawędzie między wierzchołkami z liczbami a wierzchołkami z literami. Cykl Hamiltona używałby dwóch algo czterech krawędzi łącznikowych.
Rozważmy przypadek kiedy graf Petersena używa dwóch krawędzi łącznikowych.

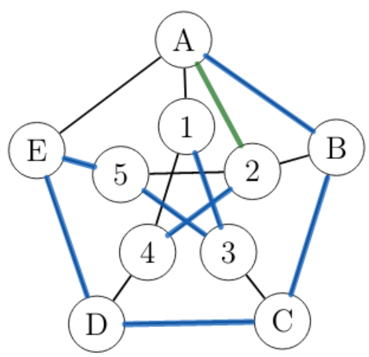


W pierwszym przypadku krawędzie łącznikowe są obok siebie. Cykl hamiltona musi używać niebieskich krawędzi. Wówczas mamy konflikt, ponieważ jeśli z wierzchołka 4 pójdziemy do wierzchołka 1 to potem będziemy musieli pójść do wierzchołka 3, czyli mamy cykl i nie przeszliśmy przez wierzchołki 2 i 5. Jeśli z wierzchołka 4 pójdziemy do wierzchołka 2, to potem idziemy do wierzchołka 5, a następnie do wierzchołka 3. Również mamy cykl i nie przeszliśmy przez wierzchołek 1. Zatem w tym przypadku nie istnieje cykl hamiltona.
W drugim przypadku krawędzie łącznikowe nie będą obok siebie. Wówczas cykl hamiltona musi używać niebieskich krawędzi i od razu mamy sprzeczność, ponieważ z wierzchołka E i z wierzchołka

B wychodzą trzy krawędzie które muszą należeć do cyklu. Zatem również w tym przypadku nie istnieje cykl hamiltona.
Rozważmy przypadek kiedy graf Petersena używa czterech krawędzi łącznikowych. Cykl hamiltona musi używać niebieskich krawędzi. Wówczas widać, że nie ma cyklu hamiltona.



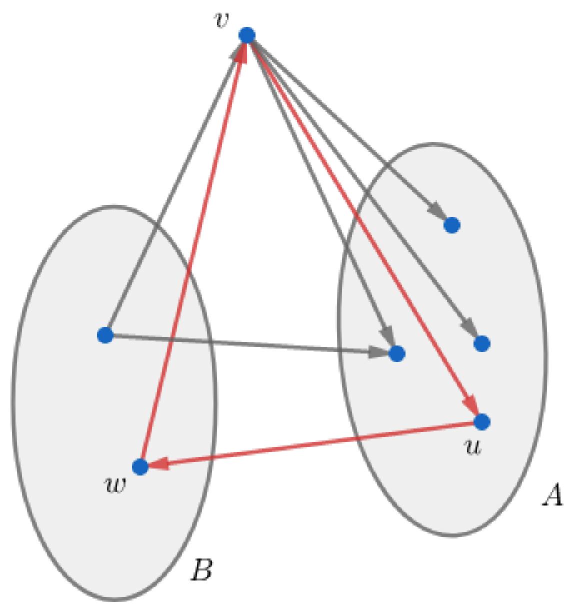
Pokazaliśmy więc, że graf Petersena jest niehamiltonowski. Aby pokazać że jest maksymalny niehamiltonowski pokażemy, że dodanie dowolnej krawędzi sprawia, że graf jest hamiltonowski.
Łatwo pokazać że dodanie krawędzi między dowolnymi wierzchołkami jest izomorficzne z dodaniem krawędzi między wierzchołkami A i 2 (wystarczy odpowiednio poprzestawiać wierzchołki).



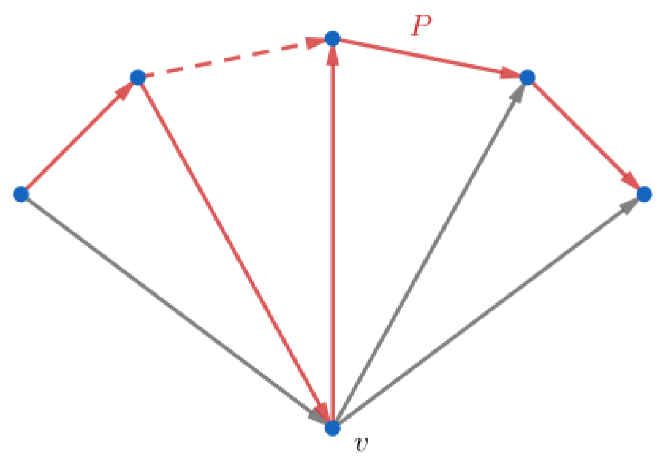
Wówczas w takim grafie istnieje cykl hamiltona, zatem graf jest hamiltonowski.

Zadanie 11.8.
Pokaż, że turniej jest hamiltonowski $\Leftrightarrow$ jest silnie spójny.

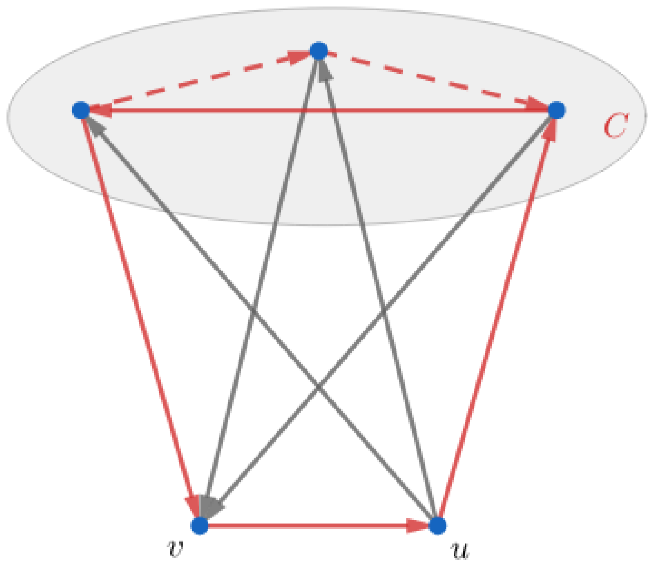
Rozwiązanie:
Jeśli turniej jest hamiltonowski, to istnieje w nim cykl przechodzący przez wszystkie wierzchołki, zatem z każdego wierzchołka da się dojść do każdego innego idąc właśnie po tym cyklu, zatem graf jest silnie spójny.
Dowód w drugą stronę pokażemy przez indukcję po k, gdzie k to długość cyklu w grafie. Ustalmy n wierzchołkowy silnie spójny turniej T. Udowodnijmy na początek, że istnieje w tym grafie cykl długości $k = 3$. Weźmy dowolny wierzchołek v. Niech A to będzie zbiór wierzchołków do których istnieje krawędź od v, natomiast niech B to zbiór wierzchołków od których istnieje krawędź do v. Z silnej spójności grafu wynika, że oba zbiory są niepuste oraz istnieje $u \in A$ oraz $w \in B$ takie że istnieje krawędź z u do w. Wówczas wierzchołki v, u, w tworzą cykl długości 3.



Pokażemy że każdy turniej zawiera ścieżkę hamiltona. Oczywiście turniej składający się z jednego wierzchołka nie zawiera krawędzi, więc istnieje w nim ścieżka hamiltona. Załóżmy że w każdym n-turnieju istnieje ścieżka hamiltona. Rozważmy $n+1$-turniej. Weźmy dowolny wierzchołek v i usuńmy go z grafu wraz z incydentnymi krawędziami. Wówczas w powstałym n-turnieju istnieje z założenia indukcyjnego ścieżka P. Teraz albo wierzchołek v miał wszystkie krawędzie wychodzące, czyli istnieje ścieżka długości n, ponieważ wierzchołek v będzie początkowym wierzchołkiem ścieżki. Albo wierzchołek v miał wszystkie krawędzie wchodzące i wówczas również istnieje ścieżka i wierzchołek v będzie ostatnim wierzchołkiem ścieżki. Albo wierzchołek v ma zarówno krawędzie wychodzace jak i wchodzące. W trzecim przypadku możemy bierzemy dwa sąsiednie wierzchołki na ścieżce P takie, że z jednego wychodzi krawędź do v, a z drugiego wchodzi krawędź od v. Usuwamy krawędź między nimi w ścieżce i wierzchołek v wstawiamy między dane wierzchołki.



Załóżmy teraz, że n-turniej ma cykl o długości $k < n$. Weźmy wierzchołek v nie należący do tego cyklu. Jeśli istnieją w C wierzchołki u i w takie że istnieje krawędź od v do u i od w do v, to włączamy wierzchołek do cyklu tak samo jak włączaliśmy wierzchołek do ścieżki hamiltona. Jeśli nie istnieje taki wierzchołek, to definiujemy zbiór A jako zbiór wierzchołków w takich, że istnieje krawędź od każdego wierzchołka z cyklu do w oraz definiujemy zbiór B jako zbiór wierzchołków takich, że dla w istnieje krawędź do każdego wierzchołka z cyklu. Oczywiście oba zbiory są nie puste. Weźmy więc $v \in A$ oraz $u \in B$ takie, że istnieje ścieżka od v do u. Włączmy teraz te dwa wierzchołki do cyklu usuwając jeden wierzchołek z cyklu między nimi. Otrzymaliśmy cykl długości $k+1$ co kończy krok indukcyjny.



Zadanie 11.9.
Udowodnij, że jeśli z kodu Graya zdefiniowanego rekurencyjnie $G(0) =$ pusty ciąg; $G(n+1) = (0G(n); 1G(n)^R)$ wypisać wektory zawierające k jedynek, to dwa sąsiednie (cyklicznie) wektory mają odległość Hamminga równą 2. Napisać wzór rekurencyjny na taki 'okrojony' kod Graya $G(n, k)$.

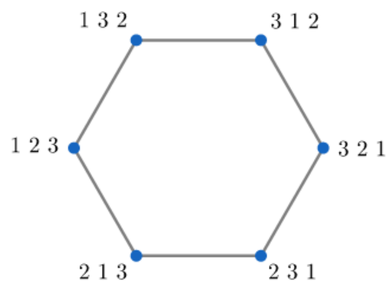
Ćwiczenia 12

Planarność, kolorowanie

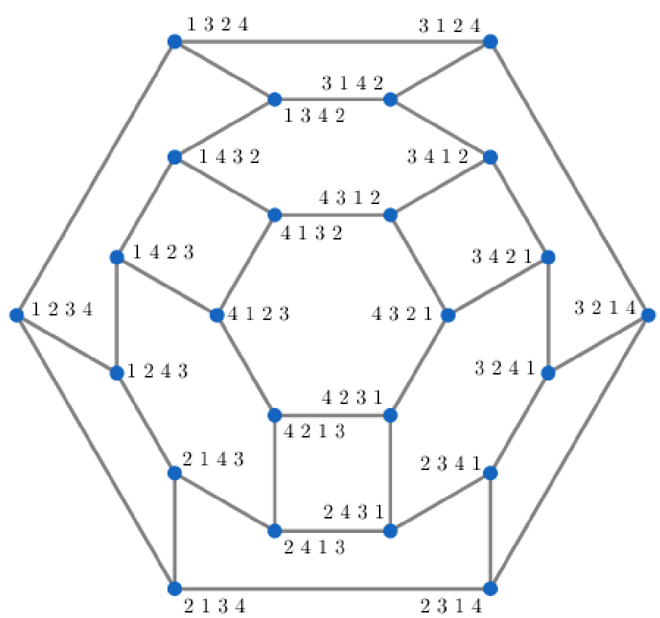
Zadanie 12.1.
Wierzchołki grafu permutacji G_n są etykietowane permutacjami zbioru n-elementowego. Dwa wierzchołki w tym grafie są połączone krawędzią, jeśli odpowiadające im permutacje różnią się transpozycją sąsiednich elementów. Dla jakich n graf G_n jest planarny?

Rozwiązanie:
G_2 to po prostu odcinek.

Rozważmy graf G_n. Oczywiście n-permutacji jest $n!$, zatem graf ma $n!$ wierzchołków. W ciągu o długości n możemy dokonać $n-1$ transpozycji sąsiednich elementów, zatem stopień każdego wierzchołka w grafie G_n to $n-1$. Czyli łącznie krawędzi w grafie mamy $\frac{n!(n-1)}{2}$. Zauważmy, że w grafie G_n nie będzie cykli o długości 3, zatem możemy skorzystać ze wzoru $m \leq 2n-4$, by z góry oszacować jakie może być n aby graf był planarny. Mamy $\frac{n!(n-1)}{2} \leq 2n! - 4$, czyli $(n-1) \leq 4 - \frac{8}{n!}$. Graf G_n może być więc planarny dla $n \leq 4$. Graf G_3 jest oczywiście planarny, gdyż wygląda następująco.



Rysowanie G_4 zaczniemy od dopisania 4 na początku każdego wierzchołka z G_3. Następnie dla każdego wierzchołka znajdujemy jego sąsiadów. Zatem również G_4 jest planarny.



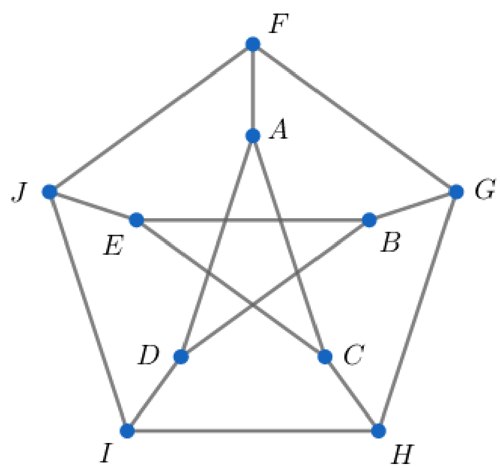
Zadanie 12.2.
Pokaż nieplanarność grafu Petersena

a) z twierdzenia Kuratowskiego (zawiera podgraf homeomorficzny z $K_{3,3}$ lub K_5);

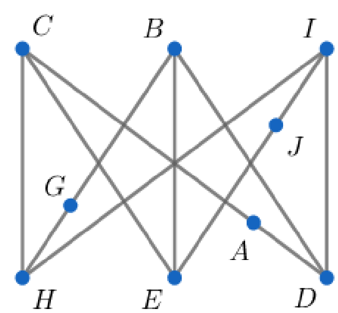
b) wyprowadzając ograniczenie górne na liczbę krawędzi dla grafów planarnych o obwodzie r.

Rozwiązanie:

a) Mamy graf Petersena o wierzchołkach w zbiorze $\{A, B, ..., J\}$.



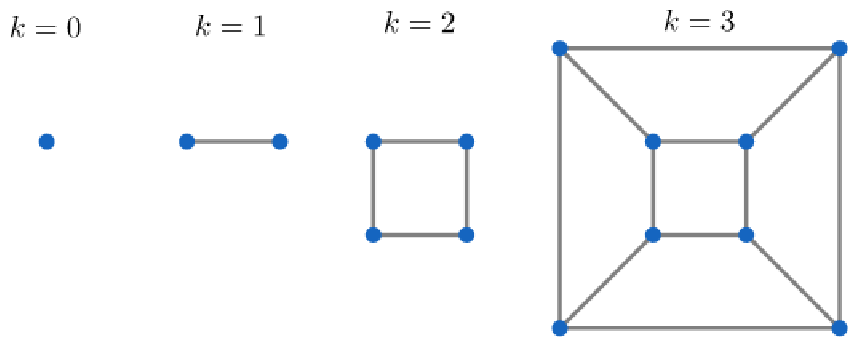
Usuwając wierzchołek F oraz incydentne z nim krawędzie oraz po odpowiednim przestawieniu wierzchołków, otrzymujemy graf homeomorficzny z grafem $K_{3,3}$.



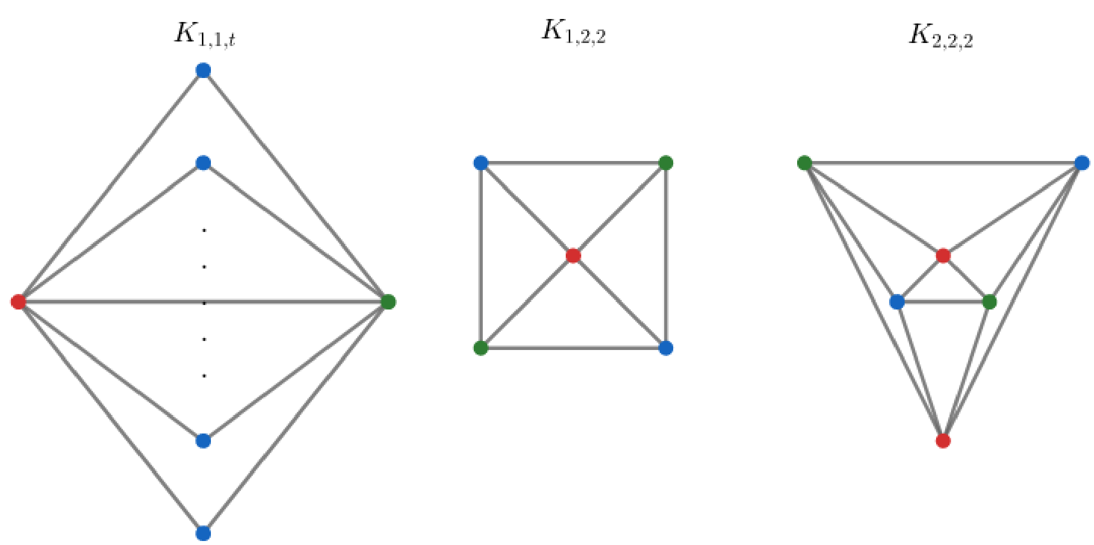
b) Obwód grafu to długość najkrótszego cyklu w grafie. Zatem jeśli obwód grafu to r, to każda ściana sąsiaduje z przynajmniej r krawędziami. Każda krawędź dodyka dwóch ścian, zatem aby graf był planarny, musi być spełniona nierówność $f \cdot r \leq 2m$. Trudno jest policzyć liczbę ścian, jednak jeśli graf jest planarny, to ze wzoru Eulera mamy $f = 2+m-n$, czyli zachodzi nierówność $(2+m-n) \leq 2m$, czyli $m(r-2) = (n-2)r$. W grafie Petersena mamy $n = 10$ oraz $m = 15$. Najkrótszy cykl ma długość 5, zatem $r = 5$. Czyli aby graf Petersena był planarny, to musi być spełniona nierówność $15 \cdot 3 \leq 8 \cdot 5$, czyli $45 \leq 40$, co oczywiście nie jest prawdziwe, zatem graf Petersena nie jest planarny.

Zadanie 12.3.
Dla jakich k hiperkostka Q_k jest planarna? Dla jakich r, s, t pełny graf trojdzielny $K_{r,s,t}$ jest planarny?

Rozwiązanie:
Oczywiście kostka Q_k jest planarna dla $k \in \{0, 1, 2, 3\}$, ponieważ możemy ją narysować na płaszczyźnie tak aby krawędzie się nie przecinały.



Pokażemy, że kostka Q_4 planarna nie jest. Najkrótszy cykl w kostce Q_4 ma długość 4, zatem aby była planarna trzeba musi zachodzić nierówność $m \leq 2n - 4$. Dla kostki Q_4 mamy $n = 16$ oraz $m = 32$, zatem nie jest prawdziwa dana nierówność.
Każda kolejna kostka Q_k dla $k \geq 4$ zawiera w sobie jako podgraf kostkę Q_4, zatem one również nie będą planarne.
Rozważmy teraz grafy trójdzielne. Dla ustalenia uwagi załóżmy, że $1 \leq r \leq s \leq t$.
Grafy $K_{1,1,t}, K_{1,2,2}, K_{2,2,2}$ są planarne, ponieważ można je narysować na płaszczyźnie tak, aby krawędzie się nie przecinały.

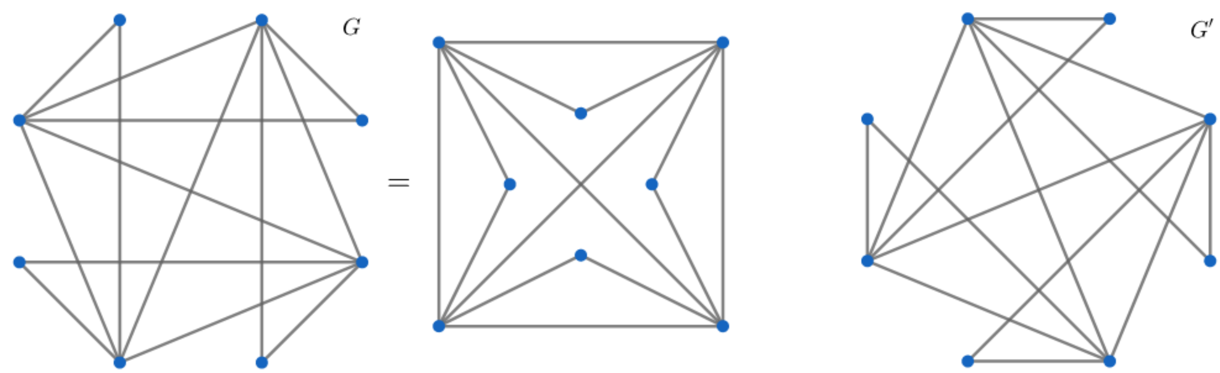


Jeśli $r + s \geq 3$, to możemy potraktować je jak jedną składową w grafie i wówczas graf $K_{r,s,t}$ będzie zawierał w sobie podgraf homeomorficzny z grafem $K_{3,3}$, czyli nie będzie to graf planarny.

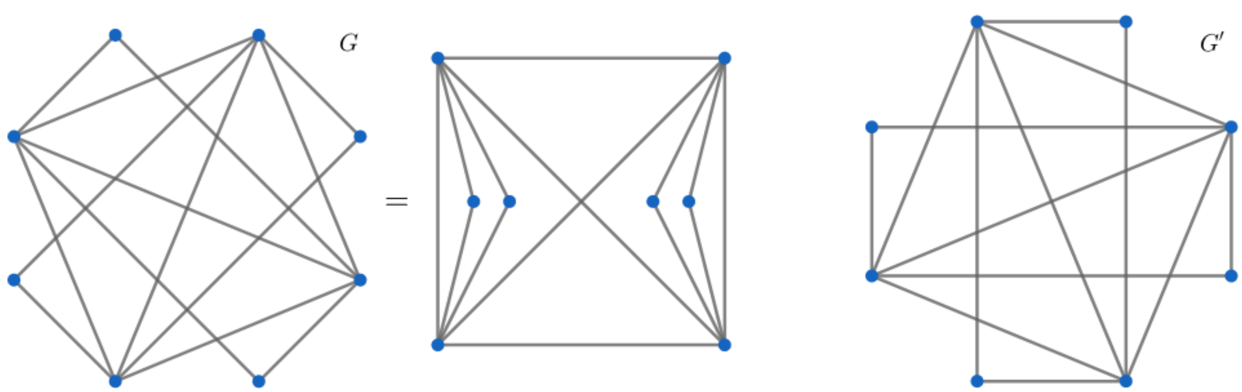
Zadanie 12.4.

Pokaż, że jeśli G ma co najmniej 11 wierzchołków, to G i dopełnienie G nie mogą być jednocześnie planarne. Podaj przykład 8-wierzchołkowego G takiego, że G i dopełnienie G są planarne.

Rozwiązanie:
Jeśli przez m_G oznaczymy liczbę krawędzi w grafie G, natomiast przez $m_{G'}$ oznaczymy liczbę krawędzi w dopełnieniu grafu G, to mamy $m_G + m_{G'} = \frac{n(n-1)}{2}$, gdzie n to liczba wierzchołków w grafie G. Załóżmy, że G jast planarny. Wówczas $m_G \leq 3n - 6$. Z równości $m_G + m_{G'} = \frac{n(n-1)}{2}$, mamy $m_{G'} = \frac{n(n-1)}{2} - m_G$, zatem mamy $m_{G'} \geq \frac{n(n-1)}{2} + 6 - 3n = \frac{n^2-7n+12}{2}$, co jest większe od $3n - 6 = \frac{6n-12}{2}$ dla $n \geq 11$. Zatem $m_{G'} \geq 3n - 6$, czyli graf G' nie jest planarny.
Przykładem grafu planarnego 8-wierzchołkowego, którego dopełnienie jest planarne, jest graf G, ponieważ jest to graf samodopełniający się.



Inny przykład



Zadanie 12.5.
Ile co najwyżej krawędzi może mieć n-wierzchołkowy graf zewnętrznie planarny? Pokaż, że każdy graf zewnętrznie planarny można pokolorować 3 kolorami.

Zadanie 12.6.
Udowodnij "twierdzenie o 7 barwach"dla torusa:

a) K_7 można narysować na torusie $\Rightarrow$ czasem trzeba użyć 7 kolorów.

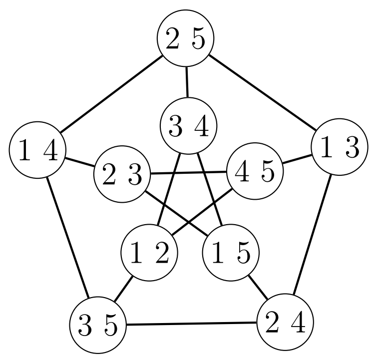
b) odpowiednik wzoru Eulera: $n - m + f = 0$

c) odpowiednik $m \leq 3n - 6 : m \leq 3n$

d) odpowiednik faktu o istnieniu wierzchołka stopnia nie większego od 5: istnieje wierzchołek stopnia nie większego 6

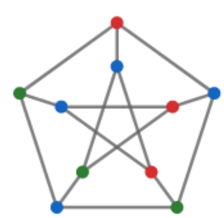
e) 7 kolorow zawsze wystarczy.

Zadanie 12.7.
Graf Knesera $K(r, n)$: $V = \{r\text{-podzbiory}\{1, ..., n\}\}$
$\{A, B\}$ jest krawędzią wtedy i tylko wtedy, gdy część wspólna A i B jest pusta.
Na przykład $K(2, 5)$ to graf Petersena.



Pokaż, że $\chi(K(2, 5)) = 3$, $\chi(K(2, 6)) = 4$ oraz ogólnie $\chi(K(r, n)) \leq n - 2r + 2$.

Rozwiązanie:
Grafu Petersena nie da się pokolorować dwoma kolorami, ponieważ zawiera cykl długości 5. Da się jednak pokolorować trzema kolorami.



Dokładamy pięć wierzchołków $\{1, 6\}, \{2, 6\}, \{3, 6\}, \{4, 6\}, \{5, 6\}$. Są one nie połączone ze sobą, ponieważ każde dwa zbiory mają wspólny element 6. Wierzchołki te możemy pokolorować czterema kolorami, zatem mamy $\chi(K(2, 6)) \leq 4$.
Każdy nowy wierzchołek sąsiaduje z trzema wierzchołkami, które są na zewnątrz grafu Petersena, przy czym nie sąsiaduje z trzema kolejnymi wierzchołkami, bo w trzech kolejnych wierzchołkach znajdują się wszystkie liczby ze zbioru $\{1, 2, 3, 4, 5\}$. Trzy wierzchołki z pięciu możemy wybrać na $\binom{5}{3} = 10$ sposobów. Trzy sąsiadujące wierzchołki możemy wybrać na $10 - 5 = 5$ sposobów. Zatem łącznie trzy niesąsiednie wierzchołki wierzchołki możemy wybrać na 5 sposobów. Zewnętrzne wierzchołki kolorujemy w następny sposób $A\ B\ A\ B\ C$, ponieważ mamy cylk długości 5. Jedna z takich trójek będzie składała się więc z trzech różnych kolorów. Zatem ten wierzchołek, który z nimi sąsiaduje, musi być pomalowany na czwarty kolor.

Aby udowodnić nierówność $\chi(K(r,n)) \leq n-2r+2$, zrobimy indukcję po n dla ustalonego r. Aby w ogóle graf mógł istnieć, musi być spełniona nierówność $n \geq 2r$. Dla $n = 2r$ mamy po prostu graf dwudzielny, zatem możemy pokolorować go 2 kolorami. Mamy $\chi(K(r,2r)) \leq 2r-2r+2 = 2$, czyli prawdziwa jest nierówność. Załóżmy więc, że teza zachodzi dla n. Do grafu $K(r,n)$ dokładładamy wierzchołki, które mają w sobie element $n+1$, zatem możemy je pokolorować na nowy kolor, ponieważ nie sąsiadują one ze sobą. Mamy więc $\chi(K(r,(n+1))) \leq \chi(K(r,n))+1 = n-2r+2+1 = (n+1)-2r+2$. Zatem teza jest prawdziwa.

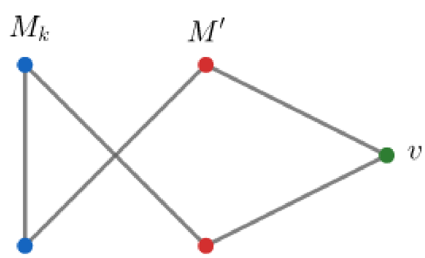
Zadanie 12.8.
Graf Mycielskiego M_n : M_2 = krawędź, M_{k+1} : do M_k dokładamy kopię M' samych wierzchołków z M_k. Każdy wierzchołek-kopia w M' jest połączony z sąsiadami swojego oryginału w M_k. Dokładamy jeszcze nowy wierzchołek połączony ze wszystkimi w M'. Pokaż, że

a) w M_k nie ma trójkątów

b) $\chi(M_k) = k$.

Rozwiązanie:

a) Udowodnimy to przez indukcję. W grafie M_2 nie ma oczywiście żadnego cyklu, zatem nie ma też cyklu o długości 3, czyli nie ma trójkątów. Załóżmy więc, że trójkątów nie ma w grafie M_k.



Zauważmy, że w M' żadne dwa wierzchołki nie są połączone. Wierzchołek v nie jest też połączony z wierzchołkami z M_k. Wierzchołek v nie może być więc częścią trójkąta. Jeśli wierzchołek x' z M' będący kopią wierzchołka x z M_k jest połączony z wierzchołkami v, w z M_k, to wynika z tego, że skoro $x'v$ jest krawędzią to xv jest krawędzią i skoro $x'w$ jest krawędzią, to xw jest krawędzią. Zatem gdyby istniał trójkąt o wierzchołkach x', v i w, to musiałby też istnieć trójkąt o wierzchołkach x, v i w, co jest sprzeczne z założeniem indukcyjnym. Ale w takiej sytuacji jedyną możliwością, aby powstał trójkąt jest to, że wszystkie wierzchołki trójkąta leżą w M_k, co jest nie możliwe z założenia indukcyjnego.

b) To również udowodnimy przez indukcję. W grafie M_2 będącym krawędzią, oczywiście mamy 2-kolorowanie. Załóżmy więc, że graf M_k można pokolorować k kolorami. Pokażemy, że M' można pokolorować tak samo jak graf M_k. Dla wierzchołka x' z M' będącego kopią wierzchołka x z M_k, wszyscy jego sąsiedzi to również wszystkimi sąsiadami wierzchołka x, zatem wierzchołki x oraz x' mogą mieć takie same kolory. Wierzchołek v sąsiaduje ze wszystkimi wierzchołkami z M', zatem musi zostać pokolorowany na $k+1$ kolor. Zatem do pokolorowania grafu wystarczy $k+1$ kolorów.

Aby pokazać, że do pokolorowania M_{k+1} potrzeba $k+1$ kolorów, pokażemy, że do pokolorowania M' potrzeba k kolorów. Załóżmy, że da się pokolorować M' na mniej niż k kolorów i połączyć z wierzchołkami M_k tak żeby wszystko było poprawnie. Weźmy dowolny kolor A, który występował w M_k, ale nie występował w M'. Weźmy dowolny wierzchołek x w M_k, który ma kolor A. Niech wierzchołek x' w M' będzie kopią wierzchołka x. Skoro x' jest połączony ze wszystkimi wierzchołkami z którymi połączony jest x, to oznacza, że wierzchołek x wcale nie musi być koloru A, lecz może być koloru takiego jak x'. Postępując tak ze wszystkimi kolorami otrzymujemy tezę.

Zadanie 12.9.
Udowodnij twierdzenie Koniga: kolorowanie krawędziowe grafu dwudzielnego o maksymalnym stopniu D wymaga tylko D kolorów.

Zadanie 12.10.
Znajdź wielomian chromatyczny cyklu C_n, „koła o n szprychach”, grafu $K_{n,m}$.

Rozwiązanie:
Znajdźmy wielomian chromatyczny cyklu. Skorzystamy ze wzoru $f_G(x) = f_{G\cup(v,w)}(x) + f_{G\setminus(v,w)}$. Znajdźmy więc wielomian chromatyczny dla ścieżki. Jeśli dwa końce ścieżki mają różny kolor, to łączymy je i otrzymujemy cykl o n wierzchołkach. Jeśli dwa końce ścieżki mają jednakowy kolor, to łączymy je i otrzymujemy cykl o $n-1$ wierzchołkach. Zatem mamy $f_{\text{ścieżka}_n}(x) = f_{\text{cykl}_n}(x) + f_{\text{cykl}_{n-1}}(x)$. Wielomian chromatyczny dla ścieżki to $f_{\text{ścieżka}_n}(x) = x\cdot(x-1)^{n-1}$, ponieważ pierwszy wierzchołek kolorujemy na x sposobów, a każdy kolejny na $x-1$, bo musi być inny niż ten poprzedni. Mamy więc $f_{\text{cykl }n}(x) = x(x-1)^{n-1} - f_{\text{cykl }n-1}(x)$. Po rozwinięciu do sumy wychodzi szereg geometryczny, który daje się zwinąć, zatem $f_{\text{cykl}_n}(x) = (x-1)^n + (-1)^n(x-1)$.
Znajdźmy wielomian chromatyczny "koła o n szprychach". Mając wielomian chromatyczny cyklu $f_{\text{cykl}_{n-1}}(x)$ możemy wyznaczyć łatwo wielomian chromatyczny dla "koła o n szprychach". Najpierw na x sposobów wybieramy kolor dla środka koła, a następnie kolorujemy koło $x-1$ kolorami na $f_{\text{cykl}_{n-1}}(x-1)$ sposobów, zatem mamy $f_{\text{koło}_n}(x) = x\cdot f_{\text{cykl}_{n-1}}(x-1)$
Znajdźmy wielomian chromatyczny grafu $K_{n,m}$. Zauważmy, że jeśli jakiś kolor występuje po lewej stronie grafu, to nie może wystąpić on po prawej stronie grafu. Zsumujemy więc po k i l, gdzie k to liczba kolorów użytych z lewej strony, natomiast l to liczba kolorów użytych z prawej strony. Dzielimy lewą stronę na k części na $\left\{ n \atop k \right\}$ sposobów. Dzielimy prawą stronę na l części na $\left\{ m \atop l \right\}$ sposobów. Każdej części nadajemy teraz jedne z x kolorów na $x^{\underline{k+l}}$ sposobów. Sumując po k i l otrzymujemy $f_{K_{n,m}}(x) = \sum_{k,l} \left\{ n \atop k \right\} \left\{ m \atop l \right\} x^{\underline{k+l}}$.

Ćwiczenia 13

Twierdzenie Halla i systemy różnych reprezentantów

Zadanie 13.1.

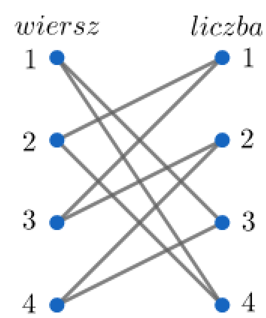
Udowodnij, że każdy prostokąt łaciński można rozszerzyć do kwadratu.

Rozwiązanie:

Mamy prostokąt wypełniony k kolumnami i chcemy dopełnić $k+1$ kolumnę.

	k	$k+1$	
1	2		
2	3		
3	4		
4	1		

Wystarczy znaleźć skojarzenie w grafie dwudzielnym, gdzie po lewej stronie będzie numer wiersza, a po prawej będą liczby. W grafie tym istnieje krawędź między wierzchołkiem i z lewej strony i wierzchołkiem j z prawej strony, jeśli w i-tym wierszu nie ma j-tej liczby.



Zadanie 13.2.

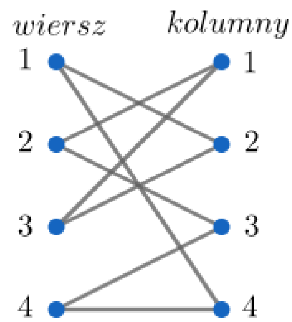
Do kwadratu $n \times n$ wpisano po n liczb $1, 2, ..., k$ (łącznie $k \cdot n$ liczb) w taki sposób, że w żadnym wierszu ani kolumnie nie ma dwóch takich samych liczb. Udowodnij, że można uzupełnić ten kwadrat do kwadratu łacińskiego (tzn. w każdym wierszu i w każdej kolumnie zawierającego permutację liczb $1, ..., n$).

Rozwiązanie:

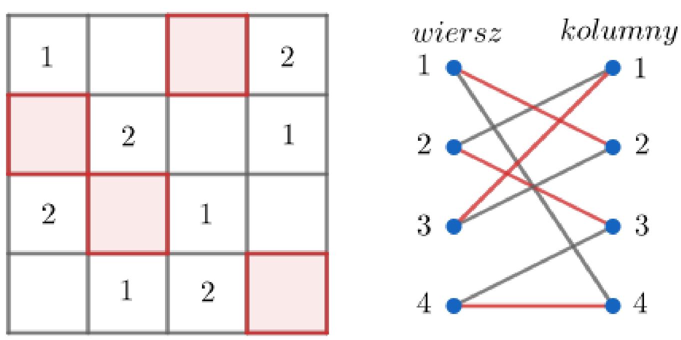
Mamy wpisane k rodzajów liczb.

1			2
	2		1
2		1	
	1	2	

Aby liczbę $k+1$, musimy znaleźć n pól, takich, że nie mają one wspólnego wiersza ani kolumny. Odpowiadać to będzie znalezieniu skojarzenia w grafie, gdzie po jednej stronie będą dwudzielnym, gdzie po jednej stronie będą wiersze, a po drugiej kolumny i wierzchołki będą ze sobą połączone wtedy, gdy pole będzie puste.



Takie skojarzenie oczywiście istnieje, ponieważ jest to graf $n-k$ regularny. Zatem taki kwadrat można dopełnić do kwadratu łacińskiego.



Zadanie 13.3.
Pokaż, że jeśli w grafie dwudzielnym (V_1, V_2) stopnie wierzchołków w V_1 są $\geq$ niż stopnie wierzchołków w V_2, to istnieje pełne skojarzenie z V_1 do V_2.

Rozwiązanie:
Suma stopni wierzchołków po obu stronach grafu jest taka sama. Zatem skoro stopnie wierzchołków w V_1 są $\geq$ niż stopnie wierzchołków w V_2 stopnie wierzchołków w V_1 są $\geq$ niż stopnie wierzchołków w V_2, to wierzchołków w V_2 jest nie mniej niż w V_1.

Niech $x = \min(\deg(v))$ dla $v \in V_1$, czyli najmniejszy stopień wierzchołków w V_1. Niech $y = \max(\deg(v))$ dla $v \in V_2$, czyli największy stopień wierzchołków w V_2. Mamy więc $x \geq y$. Weźmy dowolny podzbiór V wierzchołków w V_1 i niech $E(V)$ to liczba krawędzi wychodzących z wierzchołków tego podzbioru. Wówczas $E(V) \geq x \cdot n$, gdzie n to liczba wierzchołków podzbiorze V. Niech V' to zbiór wierzchołków będących sąsiadami wierzchołków z V. Wówczas liczba $E(V) \leq m \cdot y$, gdzie m oznacza liczbę wierzchołków w V'. Mamy więc $m \cdot y \geq E(V) \geq n \cdot x \geq n \cdot y$, skąd $m \geq n$. Zatem z twierdzenia Halla wynika teza.

Zadanie 13.4.
Udowodnij, że jeśli w grafie dwudzielnym (V_1, V_2) jest spełniony warunek Halla i stopień każdego wierzchołka w V_1 jest $\geq t$, to pełne skojarzenie z V_1 do V_2 można wybrać na co najmniej $t!$ sposobów, jeśli $t \leq |V_1|$ i na co najmniej $\frac{t!}{(t-|V_1|)!}$ sposobów jeśli $t > |V_1|$.

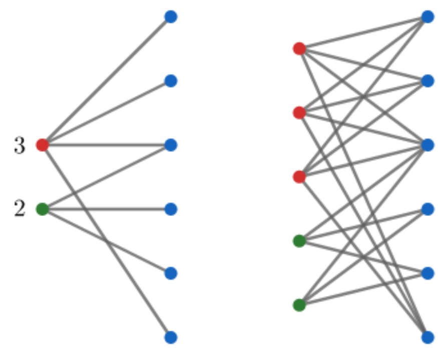
Rozwiązanie:
Pokażmy najpierw, że jeśli graf dwudzielny $G = (V_1, V_2, E)$ spełnia warunek Halla, to istnieje $v \in V_1$ takie, że każda krawędź incydentna z v należy do pewnego pełnego skojarzenia.

Udowodnimy to przez indukcję po mocy n zbioru wierzchołków z lewej strony. Jeśli $n = 1$, to teza jest prawdziwa, bo skojarzenie składa się wtedy tylko z jednej krawędzi. Niech $N(A)$ oznacza zbiór sąsiadów zbioru wierzchołków A. Jako A weźmy najmniejszy niepusty podzbiór V_1 taki, że $|N(A)| = |A|$. Jeśli taki zbiór nie istnieje, czyli $|N(B)| > |B|$ dla każdego niepustego zbioru $B \subseteq V_1$, to można wziąć dowolny wierzchołek z V_1 i dowolny sąsiedni z nim wierzchołek z V_2 i wyrzucić tę parę z grafu wraz z łączącą je krawędzią, a następnie skorzystać z założenia indukcyjnego. Analogiczną sytuację mamy gdy $A = V_1$. Pozostaje do rozpatrzenia przypadek, gdy $A \subset V_1$, czyli gdy $|A| < |V_1|$. Możemy więc skorzystać z założenia indukcyjnego dla podgrafu $H = (A, N(A), E(A))$, gdzie $E(A)$ to krawędzie między wierzchołkami z A oraz z $N(A)$. W grafie H z założenia indukcyjnego, istnieje wierzchołek v taki, że każda incydentna z nim krawędź należy do pewnego pełnego skojarzenia. Możemy wziąć więc ten wierzchołek i skojarzyć go z dowolnym wierzchołkiem z V_2, a następnie znaleźć skojarzenie w H. Skoro $|A| = |N(A)|$, to każde skojarzenie w G składa się ze skojarzenia w H oraz skojarzenia w pozostałej części grafu, ponieważ w pełnym skojarzeniu wierzchołki z $N(A)$ muszą być skojarzone z wierzchołkami z A.

Niech $f(t, n)$ oznacza na ile co najmniej sposobów można wybrać skojarzenie w grafie, gdzie n oznacza liczbę wierzchołków w V_1. Wybieramy więc wierzchołek z V_1, taki że każda krawędź incydentna z nim należy do pewnego pełnego skojarzenia. Kojarzymy go z kimś na co najmniej t sposobów, a następnie usuwamy go wraz z sąsiadem i krawędzią między nimi. Otrzymujemy graf, gdzie w V_1 jest $n-1$ wierzchołków i każdy ma stopień $\geq t-1$. Graf ten możemy skojarzyć na $f(t-1, n-1)$ sposobów. Jeśli $t \leq n$, to otrzymujemy $f(t, n) = t!$, natomiast jeśli $t > n$, to mamy $t^{\underline{n}}$.

Zadanie 13.5.
Problem haremu: jak wygląda warunek Halla w przypadku, kiedy i-ty chłopiec chce poślubić d_i dziewcząt?

Rozwiązanie:
Jeśli i-ty chłopiec chce mieć d_i dziewczyn, to musi dla każdej dziewczyny kupić samochód. Wystarczy więc skojarzyć $\sum\limits_{i \geq 0} d_i$ samochodów z dziewczynami, gdzie samochód jest połączony z tą dziewczyną, którą może poślubić i-ty chłopiec.



Jeśli warunek Halla brzmiał „istnieje skojarzenie od V_1 do V_2, gdy dla każdego podzbioru V wierzchołków ze zbioru V_1 liczba wierzchołków utworzona przez połączenie wierzchołków z V wszystkimi krawędziami z wierzchołkami z V_2 jest nie mniejsza niż liczba wierzchołków w V", to warunek Halla w przypadku, kiedy i-ty chłopiec chce poślubić d_i dziewcząt będzie brzmiał następująco „dla każdego podzbioru V wierzchołków ze zbioru V_1, suma d_i, gdzie sumujemy tylko po wierzchołkach z V, jest nie większa niż liczba wierzchołków utworzona przez połączenie wierzchołków z V wszystkimi krawędziami z wierzchołkami z V_2".

Zadanie 13.6.
Udowodnij, że przeliczalna rodzina zbiorów skończonych ma System Różnych Reprezentantów wtedy i tylko wtedy, gdy dla każdego naturalnego k dowolnych k zbiorów z tej rodziny zawiera w sumie co najmniej k elementów. Pokaż, że założenie o skończoności zbiorów jest istotne.

Zadanie 13.7.
Pokaż, że jeśli $n > 2$, to w sieci komutacyjnej Closa każdą permutację można zrealizować na przynajmniej dwa sposoby. Zaoprojektuj optymalny algorytm ustawiania przełączników.

Ćwiczenia 14

Teoria liczb - podzielność, NWD, kongruencje

Zadanie 14.1.
Udowodnij, że iloczyn k kolejnych liczb całkowitych jest podzielny przez $k!$.

Rozwiązanie:
Zauważmy, że $n(n-1)(n-2)\cdot ... \cdot(n-k+1) = n^{\underline{k}}$ jest iloczynem kolejnych liczb całkowitych. Aby teza była prawdziwa, to $\frac{n^{\underline{k}}}{k!}$ musi być liczbą całkowitą. Mamy $\frac{n^{\underline{k}}}{k!} = \binom{n}{k}$, zatem jest to oczywiście liczba całkowita.

Zadanie 14.2.
Udowodnij, że jeśli liczba $2^n - 1$ jest pierwsza, to liczba n jest pierwsza.

Rozwiązanie:
Teza jest równoważna temu, że jeśli n jest złożone to $2^n - 1$ jest złożone. Załóżmy więc że $n = p \cdot q$ dla $p, q > 1$. Wówczas mamy

$$2^n - 1 = 2^{p\cdot q} - 1 = (2^p - 1)(1 + 2^p + 2^{2p} + ... + 2^{p(q-1)})$$

Oba czynniki są całkowite i większe od 1, zatem liczba $2^n - 1$ jest złożona.

Zadanie 14.3.
Udowodnij, że jeśli liczba $2^n + 1$ jest pierwsza, to n jest potęgą 2. Niech $f_n = 2^{2^n} + 1$ oznacza n-tą liczbę Fermata. Uprość iloczyn $f_0 \cdot ... \cdot f_n$ i udowodnij, że każde dwie różne liczby Fermata są względnie pierwsze.

Rozwiązanie:
Pokażemy najpierw, że jeśli liczba $2^n + 1$ jest pierwsza, to n jest potęgą 2 lub równoważnie, że jeśli n nie jest potęgą 2, to $2^n + 1$ jest złożone. Skoro n nie jest potęgą 2, to $n = p \cdot q$ dla $2 \not| \, q$ oraz $q > 1$. Mamy

$$2^{p\cdot q} + 1 = (2^p + 1)(1 - 2^p + 2^{2p} - \ldots + 2^{p(q-1)})$$

Pierwszy czynnik jest większy od 1, bo jest sumą 1 i jakieś liczby dodatnie. Drugi składnik jest większy od 1, bo $2^{p(i+1)} - 2^{pi} > 1$. Zatem liczba $2^n + 1$ jest złożona.
Uprośćmy teraz wyrażenie

$$f_0 \cdot ... \cdot f_n = (2^1 + 1)(2^2 + 1)(2^4 + 1) \cdot ... \cdot (2^{2^n} + 1)$$

Mamy $(x + y)(x - y) = x^2 - y^2$, zatem po domnożeniu przez $1 = (2^1 - 1)$ mamy

$$(2^1 - 1)(2^1 + 1)(2^2 + 1) \cdot ... \cdot (2^{2^n} + 1) = (2^2 - 1)(2^2 + 1) \cdot ... \cdot (2^{2^n} + 1) = ... = 2^{2^{n+1}} - 1 = f_{n+1} - 2$$

Pokażemy teraz, że każde dwie liczby Fermata są względnie pierwsze. Wiemy, że $f_k \mid f_{n+1} - 2$ dla $k < n + 1$, zatem jeśli $d \mid f_k$, to $d \mid f_{n+1}$, czyli $d \not| \, f_{n+1}$.

Zadanie 14.4.
Udowodnij, że

a) $NWD(n^a - 1, n^b - 1) = n^{NWD(a,b)} - 1$

b) $NWD(F_a, F_b) = F_{NWD(a,b)}$, gdzie F_n to n-ta liczba Fibonacciego.

Rozwiązanie:

a) Mamy

$$NWD(n^a - 1, n^b - 1) = NWD(n^a - n^b, n^b - 1) = NWD(n^b(n^{a-b} - 1), n^b - 1$$

n^b oraz $n^b - 1$ są względnie pierwsze, zatem można podzielić pierwsze wyrażenie przez n^b. Otrzymujemy

$$NWD(n^a - 1, n^b - 1) = NWD(n^{a-b} - 1, n^b - 1)$$

Tak jak w zwykłym algorytmie euklidesa odejmowaliśmy mniejszą liczbę od większej, tak tutaj stosujemy algorytm euklidesa na wykładnikach. Otrzymujemy

$$NWD(n^a - 1, n^b - 1) = NWD(n^{NWD(a,b)} - 1, n^1 - 1) = n^{NWD(a,b)} - 1$$

b) Pokażemy najpierw przez indukcję po k, że

$$F_{n+k} = F_{n+1}F_k + F_nF_{k-1}$$

Dla $k = 0$ mamy

$$F_{n+1} = F_{n+1}F_1 + F_nF_0$$

przyjmując, że $F_0 = 0$. Dalej mamy

$$F_{n+k+1} = F_{n+k} + F_{n+k-1}$$
$$F_{n+k+1} = \big(F_{n+1}F_k + F_nF_{k-1}\big) + \big(F_{n+1}F_{k-1} + F_nF_{k-2}\big)$$
$$F_{n+k+1} = F_{n+1}\big(F_k + F_{k-1}\big) + F_n\big(F_{k-1} + F_{k-2}\big)$$
$$F_{n+k+1} = F_{n+1}F_{k+1} + F_nF_k$$

Teraz chcemy pokazać, że

$$NWD(F_a, F_b) = NWD(F_{a-b}, F_b)$$

Wystarczy, że pokażemy, że dla każdego p takiego, że $p \mid F_a$ i $p \mid F_b$ mamy też $p \mid F_{a-b}$.

Pokażemy, że $F_n \perp F_{n+1}$ dla każdego n. Jeśli x dzieli F_n i F_{n+1}, to dzieli też F_{n-1}, zatem indukcyjnie dowodzimy, że x dzieli $F_1 = 1$, co oznacza, że $x = 1$.

Korzystając z tego, że

$$F_{n+k} = F_{n+1}F_k + F_nF_{k-1}$$

i biorąc $k = b$ oraz $n = a - b$ mamy

$$F_a - F_{a-b+1}F_b = F_{a-b}F_{b-1}$$

Wynika z tego, że $p \mid F_{a-b}F_{b-1}$, i skoro $p \nmid F_{b-1}$, to mamy

$$NWD(F_{a-b}, F_b) = NWD(F_{a-b}F_{b-1}, F_b) = NWD(F_a - F_{a-b+1}F_b, F_b) = NWD(F_a, F_b)$$

Mając

$$NWD(F_a, F_b) = NWD(F_{a-b}, F_b)$$

postępując analogicznie jak w podpunkcie a) dostajemy

$$NWD(F_a, F_b) = F_{NWD(a,b)}$$

Zadanie 14.5.
Ile rozwiązań ma kongruencja $a \cdot x \equiv b \mod n$ w zbiorze $\{0, ..., n-1\}$. Jak je efektywnie znajdować?

Rozwiązanie:
Rozważmy przypadek $a \perp n$. Wówczas istnieje a^{-1} takie, że $a \cdot a^{-1} \equiv 1 \mod n$. Wówczas $a \cdot a^{-1} \cdot x \equiv b \cdot a^{-1} \mod n$. Skoro $a \cdot a^{-1}$ dają resztę 1 przy dzieleniu przez n, to $x \equiv b \cdot a^{-1} \mod n$. W takim przypadku kongruencja ma jedno rozwiązanie.
Rozważmy teraz przypadek $a \not\perp n$. Wówczas $NWD(a, n) = d > 1$. Jeśli więc $d \nmid b$, to kongruencja ma zero rozwiązań. Jeśli natomiast $d \mid b$, to całą kongruencję możemy podzielić przez d otrzymując kongruencję $a' \cdot x \equiv b' \mod n'$ Kongruencja ta ma jedno rozwiązanie, bo $a' \perp n'$. Zatem orginalna kongruencja ma d rozwiązań, bo do rozwiązania kongruencji $a' \cdot x \equiv b' \mod n'$ możemy dodać $i \cdot n'$ i wynik nadal będzie rozwiązaniem kongruencji $a \cdot x \equiv b \mod n$ dla $i \in \{0, ..., d-1\}$.

Zadanie 14.6.
Udowodnij twierdzenie Wilsona: liczba n jest pierwsza $\Leftrightarrow (n-1)! \equiv -1 \mod n$.

Rozwiązanie:
Pokażemy implikację w lewo. Załóżmy przeciwnie, że n nie jest pierwsze, czyli istnieje $1 < d < n$, że $d \mid n$. Wynika z tego, że $d \mid (n-1)!$. Z warunku $(n-1)! \equiv -1 \mod n$ wynika jednak, że $n \mid (n-1)! + 1$, czyli $d \mid (n-1)! + 1$. Otrzymujemy sprzeczność, ponieważ d nie może dzielić dwóch sąsiednich liczb. Zatem n musi być liczbą pierwszą.
Pokażemy implikację w prawą stronę. Rozpatrzmy zbiór $A = \{1, 2, ..., p-1\}$. Mamy kilka ważnych obserwacji

0) dla każdego $a \in A$ mamy $a \perp p$, zatem istnieją x, y takie że $ax + py = 1$

1) dla każdego $a \in A$ istnieje odwrotność modulo p, czyli takie $a^{-1} \in A$, że $a \cdot a^{-1} \equiv 1 \mod p$

2) dla każdego $a \in A$ istnieje maksymalnie jedna taka odwrotność (jeśli $a \cdot b \equiv 1 \mod p$ oraz $a \cdot c \equiv 1 \mod p$ dla $b, c \in A$, $b \neq c$, to wynika z tego, że $p \mid ab - ac$ i jako, że $a \perp p$, to $p \mid b - c$, czyli $b \equiv c \mod p$, skąd otrzymujemy $b = c$)

3) dla każdego $a \in A$, jeśli $a^2 \equiv 1 \mod p$, to $a \equiv 1 \mod p$ lub $a \equiv -1 \mod p$ (skoro $p \mid a^2 - 1$, to $p \mid (a+1)(a-1)$, przy czym p nie może dzielić jednocześnie $a+1$ oraz $a-1$)

Zauważmy, że $1^2 \equiv 1 \mod p$ oraz $(p-1)^2 \equiv 1 \mod p$. Zatem odwrotnością $p-1$ jest $p-1$. Skoro p jest pierwsze to $p-1$ jest parzyste, czyli możemy dobrać liczby od 2 do $p-2$ w pary tak, aby ich iloczyn dawał resztę 1 przy dzieleniu przez p. Mamy więc

$$1 \cdot 2 \cdot ... \cdot (p-2) \cdot (p-1) \equiv 1 \cdot 1 \cdot ... \cdot 1 \cdot (p-1) \equiv -1 \mod p$$

Ćwiczenia 15

Teoria liczb - chińskie twierdzenie o resztach, twierdzenie Eulera, algorytmy teorioliczbowe

Zadanie 15.1.

Oto konstrukcja drzewa Sterna-Brocota: zaczynamy od dwóch ułamków: $\frac{0}{1}$ i $\frac{1}{0}$ (ten drugi reprezentuje $+\infty$) między każde dwa kolejne elementy $\frac{m}{n}$ i $\frac{m'}{n'}$ wstawiamy ułamek $\frac{(m+m')}{(n+n')}$. Udowodnij, że w ten sposób uzyskamy wszystkie dodatnie ułamki nieskracalne, każdy dokładnie raz.

Zadanie 15.2.

Udowodnij, że iloczyn trzech kolejnych liczb naturalnych, z których środkowa jest sześcianem, dzieli się przez 504.

Rozwiązanie:

Teza jest równoważna temu

$$504 \mid (n^3-1)n^3(n^3+1)$$

Mamy $504 = 7 \cdot 8 \cdot 9$, zatem wystarczy pokazać, że

$$7 \mid (n^3-1)n^3(n^3+1)$$

$$8 \mid (n^3-1)n^3(n^3+1)$$

$$9 \mid (n^3-1)n^3(n^3+1)$$

Zajmijmy się pierwszym warunkiem. Możmna rozpisać reszty z dzielenia i zobaczyć że są równe 0, 1 lub -1

$n \mod 7$	0	1	2	3	4	5	6
$n^3 \mod 7$	0	1	1	-1	1	-1	-1

Można też z małego twierdzenia Fermata. Chcemy pokazać, że $7 \mid n^3(n^6-1)$. Jeśli $7 \mid n$, to $7 \mid n^3$. Jeśli $7 \nmid n$, to $6 \mid n^6-1$, bo z małego twierdzenia Fermata mamy $n^{7-1} \equiv 1 \mod 7$.

Zajmijmy się drugim warunkiem. Jeśli $2 \mid n$, to $8 \mid n^3$, natomiast gdy $2 \nmid n$, to n^3-1 oraz n^3+1 to dwie kolejne liczby parzyste, zatem jedna z nich dzieli się przez 2, a druga przez 4, czyli $8 \mid (n^3-1)(n^3+1)$.

Zajmijmy się trzecim warunkiem. Znowu można rozpisać reszty z dzielenia i zobaczyć że są równe 0, 1 lub -1

$n \mod 3$	0	1	2
$n^3 \mod 9$	0	1	-1

Można też z twierdzenia Eulera. Mamy $\phi(9) = 9-3 = 6$, zatem jeśli $3 \nmid n$, to $9 \mid n^6-1$. Jeśli zaś $3 \mid n$, to $9 \mid n^3$.

Pokazaliśmy więc, że $504 \mid (n^3-1)n^3(n^3+1)$

Zadanie 15.3.

Niech $n = 100$. Czy $\phi(n)$ to najmniejsza liczba λ o tej własności, że jeśli $a \perp n$, to $a^\lambda \equiv 1 \mod n$? Uogólnij tę obserwację.

Rozwiązanie:
Mamy $\phi(100) = \phi(4) \cdot \phi(25) = 2 \cdot 20 = 40$. Z twierdzenia Eulera mamy

$$a^{\phi(4)} \equiv 1 \mod 4 \Leftrightarrow a^2 \equiv 1 \mod 4$$

$$a^{\phi(25)} \equiv 1 \mod 25 \Leftrightarrow a^{20} \equiv 1 \mod 25$$

Z pierwszej kongruencji mamy również

$$a^{20} \equiv 1 \mod 4$$

Zatem mamy

$$a^{20} \equiv 1 \mod 100$$

Pokażemy teraz, że jeśli $a^b \equiv 1 \mod n$ oraz $a^c \equiv 1 \mod n$, to $a^{NWD(b,c)} \equiv 1 \mod n$. Mamy $a^{bx} \equiv 1 \mod n$ oraz $a^{cy} \equiv 1 \mod n$, zatem $a^{bx+cy} \equiv 1 \mod n$. Najmniejsza wartość wyrażenia $bx + cy$ to $NWD(b, c)$, zatem $a^{NWD(b,c)} \equiv 1 \mod n$.
Zatem najmniejsze λ musu dzielić 20. Kandydatami na λ są więc 2, 4, 5 oraz 10. Weźmy więc $a = 3$.

i	$3^i \mod 100$
2	9
4	81
5	43
10	49

Zatem najmniejsza możliwa λ to 20.

Zadanie 15.4.
Udowodnij, że istnieje 2011 kolejnych liczb naturalnych, z których każda jest podzielna przez sześcian liczby naturalnej > 1.

Rozwiązanie:
Chcemy znaleźć taką liczbę n, że $p_0^3 \mid n$, $p_1^3 \mid n+1$, ..., $p_i^3 \mid n+i$, czyli szukamy takiej liczby n, że $n \equiv -i \mod p_i^3$ dla $i \in \{0, 1, ..., 2010\}$ oraz dowolnych liczb p_i względnie pierwszych. Wystarczy, że weźmiemy jako p_i kolejne liczby pierwsze. Wówczas z chińskiego twierdzenia o reszcie istnieje dokładnie jedno rozwiązanie $n \in \{0, ..., p_0^3 \cdot p_1^3 \cdot ... \cdot p_{2010}^3 - 1\}$.

Zadanie 15.5.
Niech $F(1) = 2$, $F(k+1) = 2^{F(k)}$. Oblicz $F(5) \mod 2009$.

Rozwiązanie:
Mamy $F(5) = 2^{F(4)} = 2^{65536}$. Z twierdzenia Eulera mamy $2^{\phi(2009)} \equiv 1 \mod 2009$. Z tego, że $2^m \equiv 2^{m \mod \phi(n)} \mod n$ wynika, że wystarczy policzyć resztę z dzielenia 65536 przez $\phi(2009) = \phi(49) \cdot \phi(41) = 42 \cdot 40 = 1680$. Mamy

$$2^{65536} \equiv 2^{39 \cdot 1680} \cdot 2^{16} \equiv 1 \cdot 2^{16} \equiv 2^{16} \mod 2009$$

$$2^{16} \equiv 2048 \cdot 2^5 \equiv 39 \cdot 2^5 \equiv 1248 \mod 2009$$

Zadanie 15.6.
Znajdź najmniejszą liczbę o sumie cyfr 204 podzielną przez 204.

Rozwiązanie:
Mamy $204 = 4 \cdot 3 \cdot 17$, zatem szukana liczba musi dzielić się przez 4, przez 3 oraz przez 17. Szukana liczba będzie miała co najmniej 23 cyfry, bo $22 \cdot 9 = 198 < 204$. Ponadto $23 \cdot 9 = 207$, zatem większość cyfr tej liczby to będą dziewiątki. Aby liczba była podzielna przez 3 i przez 4 i miała 23 cyfry, to mamy tak na prawdę dwa przypadki. Jedna możliwość to 22 dziewiątki oraz 6 na końcu, a druga możliwość to 20 dziewiątek i 88 na końcu i jeszcze jedna ósemka gdzieś między dziewiątkami. Drugi przypadek da nam mniejszą liczbę więc nim będziemy się zajmować na początku.
Mamy liczbę 999...989...99988. Możemy ją zapisać w postaci $10^{23} - 12 - 10^k = 10^{23} - (10^k + 12)$, gdzie k zależy od pozycji ósemki w liczbie. Szukamy więc takiego k, że

$$10^k \equiv 10^{23} - 12 \mod 17$$

Z małego twierdzenia Fermata wiemy, że $10^{16} \equiv 1 \mod 17$, zatem $10^{23} \equiv 10^7 \mod 17$.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$10^x \equiv_{17}$	1	-7	-2	-3	4	6	-8	5	-1	7	2	3	-4	-6	8	-5	1

Zatem

$$10^{23} \equiv 10^7 \equiv 5 \mod 17$$

skąd mamy

$$10^{23} - 12 \equiv -7 \mod 17$$

daje nam to $k = 1$ lub $k = 17$. Pierwszą możliwość odrzucamy, bo $k > 1$, zatem szukana liczba to

$$10^{23} - 12 - 10^{17} = 99999899999999999999988$$

Zadanie 15.7.
Znajdź konstruktywny dowód chińskiego twierdzenia o resztach (czyli podaj efektywny algorytm znajdowania elementu spełniającego stosowny układ kongruencji).

Ćwiczenia 16

Teoria liczb - RSA, test Millera-Rabina

Zadanie 16.1.
W kryptosystemie RSA: niech $p = 11$, $q = 29$, klucz jawny $e = 3$. Znajdź klucz tajny d, zaszyfruj komunikat $M = 100$, a następnie zdeszyfruj go z powrotem.

Rozwiązanie:
Mamy $n = p \cdot q = 319$, wówczas $d = e^{-1} \mod \phi(n)$. Mamy $\phi(319) = \phi(11) \cdot \phi(29) = 10 \cdot 28 = 280$ oraz $3 \cdot x \equiv 1 \mod 280 \Leftrightarrow x \equiv 187 \mod 280$, zatem $d = 187$.
Szyfrujemy, mamy $100^3 \equiv 254 \mod 319$, czyli $S(100) = 254$.
Deszyfrujemy $254^{187} \equiv 100 \mod 319$

Zadanie 16.2.
Znajdź wszystkie rozwiązania kongruencji

a) $x^2 \equiv 1 \mod 784$

b) $x^2 \equiv -1 \mod 4225$

c) $10^x \equiv 8 \mod 17$

Rozwiązanie:

a) Mamy $784 = 2^4 \cdot 7^2$, zatem

$$\begin{cases} x^2 \equiv 1 \mod 16 \\ x^2 \equiv 1 \mod 49 \end{cases}$$

Z pierwszej kongruencji mamy $16 \mid x^2 - 1 \Leftrightarrow 16 \mid (x-1)(x+1)$

$$16 \mid x+1 \Leftrightarrow x \equiv -1 \mod 16$$

$$16 \mid x-1 \Leftrightarrow x \equiv 1 \mod 16$$

$$8 \mid x+1 \wedge 16 \nmid x+1 \Leftrightarrow x \equiv 7 \mod 16$$

$$8 \mid x-1 \wedge 16 \nmid x-1 \Leftrightarrow x \equiv -7 \mod 16$$

Z drugiej kongruencji mamy $49 \mid (x-1)(x+1)$

$$49 \mid x+1 \Leftrightarrow x \equiv -1 \mod 49$$

$$49 \mid x-1 \Leftrightarrow x \equiv 1 \mod 49$$

Mamy więc

$$\begin{cases} x \equiv \pm 1 \mod 16 \\ x \equiv \pm 7 \mod 16 \\ x \equiv \pm 1 \mod 49 \end{cases}$$

Mamy $16 \perp 49$, zatem istnieją takie liczby x, y, że $16x + 49y = 1$. Dla $a = 49$ i $b = 16$ mamy

a	b	$\lfloor \frac{a}{b} \rfloor$	x	y
49	16	3	1	-3
16	1	16	0	1
1	0			

zatem mamy

$$\begin{cases} a \cdot 49 - b \cdot 48 = a \mod 16 \\ a \cdot 49 - b \cdot 48 = b \mod 49 \end{cases}$$

Pod a podstawiamy ± 1 oraz ± 7, natomiast pod b podstawiamy ± 1, otrzymujemy

$x \equiv_{49} \setminus x \equiv_{16}$	1	-1	7	-7
1	1	-97	295	-391
-1	97	-1	391	-295

b) Mamy $4225 = 5^2 \cdot 13^2$, zatem

$$\begin{cases} x^2 \equiv -1 \mod 25 \\ x^2 \equiv -1 \mod 169 \end{cases}$$

Z pierwszej kongruencji mamy $25 \mid x^2 + 1$ czyli również $5 \mid x^2 + 1$

x	0	1	2	3	4
$x^2 \equiv_5$	0	1	-1	-1	1

Zatem $x = 5n \pm 2$. Mamy więc

$$(5n \pm 2)^2 \equiv -1 \mod 25 \Leftrightarrow 25n^2 \pm 20n + 4 \equiv -1 \mod 25 \Leftrightarrow \pm 4n \equiv -1 \mod 5$$

Po pomnożeniu przez ± 1 mamy

$$4n \equiv \mp 1 \mod 5$$

Mnożymy teraz przez odwrotność 4, czyli -1. Mamy

$$n \equiv \pm 1 \mod 5$$

skąd ostatecznie otrzymujemy

$$x \equiv 5 \cdot (\pm 1) \pm 2 \mod 25 \Leftrightarrow x \equiv \pm 7 \mod 25$$

Z drugiej kongruencji mamy $169 \mid x^2 + 1$ czyli $13 \mid x^2 + 1$

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \equiv_{13}$	0	1	4	-4	3	-1	-3	-3	-1	3	-4	4	1

Zatem mamy $x \equiv 13n \pm 5 \mod 169$. Mamy więc

$$(13n \pm 5)^2 \equiv -1 \mod 169 \Leftrightarrow 169n^2 \pm 130n + 25 \equiv -1 \mod 169$$

$$\pm 10n \equiv -2 \mod 13 \Leftrightarrow 10n \equiv \mp 2 \mod 13$$

Po przemnożeniu przez odwrotność 10, czyli 4 mamy

$$n \equiv \mp 8 \mod 13 \Leftrightarrow n \equiv \pm 5 \mod 13$$

skąd ostatecznie otrzymujemy

$$x \equiv 13 \cdot (\pm 5) \pm 5 \mod 169 \Leftrightarrow x \equiv \pm 70 \mod 169$$

Daje nam więc to układ równań

$$\begin{cases} x \equiv \pm 7 \mod 25 \\ x \equiv \pm 70 \mod 169 \end{cases}$$

Teraz trzeba znaleźć rozwiązanie $25x + 169y = 1$ używając rozszerzonego algorytmu Euklidesa. Dla $a = 169$ oraz $b = 25$ mamy

a	b	$\lfloor \frac{a}{b} \rfloor$	x	y
169	25	6	4	-27
25	19	1	-3	4
19	6	3	1	-3
6	1	6	0	1
1	0			

Zatem mamy

$$\begin{cases} a \cdot 676 - b \cdot 675 \equiv a \mod 25 \\ a \cdot 676 - b \cdot 675 \equiv b \mod 169 \end{cases}$$

Podstawiamy teraz pod a liczbe ± 7, natomiast pod b liczbę ± 70 otrzymując

$x \equiv_{169} \setminus x \equiv_{25}$	-7	7
-70	268	1282
70	-1282	-268

c) Rozwiązanie będzie w postaci $x \equiv a \mod b$, gdzie b będzie najmniejszą liczbą taką, że $10^b \equiv 1 \mod 17$. Z małego twierdzenia Fermata wiemy, że $10^{16} \equiv 1 \mod 17$, zatem b jest dzielnikiem 16.

b	1	2	4	8	16
$10^b \equiv_{17}$	-7	-2	4	-1	1

Dostajemy $b = 16$. Sprawdzamy resztę $10^x \mod 17$ dla kolejnych x-ów

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$10^x \equiv_{17}$	1	-7	-2	-3	4	6	-8	5	-1	7	2	3	-4	-6	8

Zatem

$$x \equiv 14 \mod 16$$

Zadanie 16.3.
Wiedząc, że $n = 3598057$ jest iloczynem dwóch różnych liczb pierwszych oraz że 20779 jest pierwiastkiem z 1 modulo n, znajdź rozkład n na czynniki pierwsze.

Rozwiązanie:
Wiemy, że

$$x^2 \equiv 1 \mod n \Leftrightarrow (x-1)(x-2) \equiv 0 \mod n$$

Niech $n = p_1 \cdot p_2$, wówczas $p_1 \mid x-1$ oraz $p_2 \mid x+1$ Wówczas $p_1 = NWD(x-1, n)$ oraz $p_2 = NWD(x+1, n)$.

Zadanie 16.4.
Uogólnij chińskie twierdzenie o resztach na przypadek, kiedy moduły niekoniecznie są względnie pierwsze.

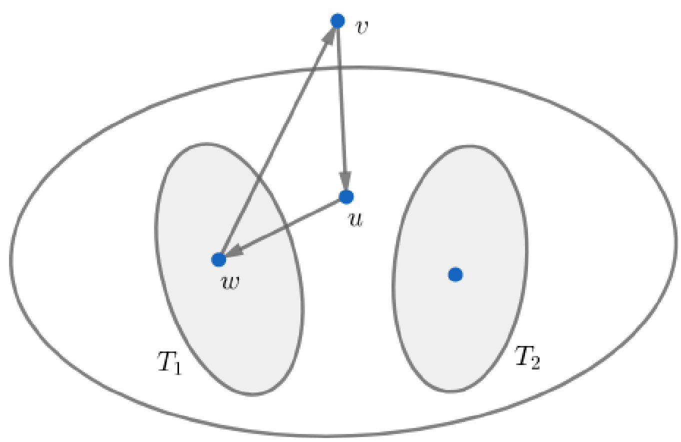
Zadanie 16.5.
Rozważmy system kryptograficzny RSA z modułem $n = 71 \cdot 103$ i wykładnikiem publicznym $e = 19$. Oblicz, ile komunikatów $M \in \{0, ..., n-1\}$ jest punktami stałymi szyfrowania, tzn. spełnia warunek $S(M) = M$.

Ćwiczenia 17

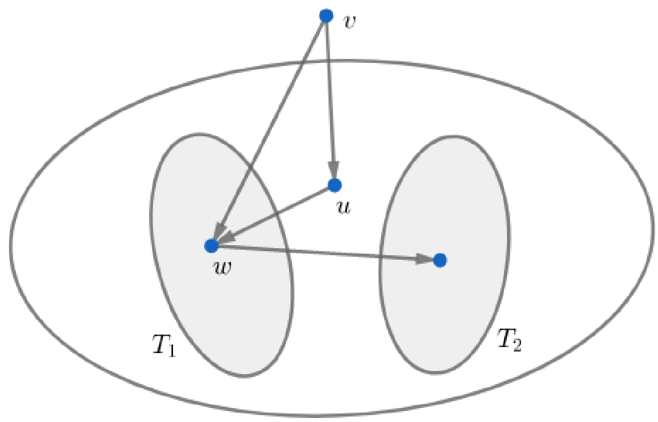
Powtórka przed kolokwium

Zadanie 1.
Pokaż, że w każdym turnieju istnieje wierzchołek, z którego można dojść do każdego innego ścieżką długości 1 lub 2.

Rozwiązanie:
Dowód pokażemy przez indukcję po wierzchołkach. Dla $n = 1$ teza jest oczywista. Załóżmy, że teza zachodzi dla n. Rozważmy graf G o $n+1$ wierzchołkach. Weźmy dowolny wierzchołek v z tego grafu i usuńmy go wraz z incydentnymi krawędźmi. Otrzymujemy graf T o n wierzchołkach, który z założenia indukcyjnego ma wierzchołek u spełniający tezę. Jeśli istnieje krawędź z u do v to teza jest spełniona w oczywisty sposób. Załóżmy więc że taka krawędź nie istnieje, czyli istnieje krawędź z v do u. Graf T możemy podzielić na dwie części. Pierwsza część to T_1 czyli zbiór wierzchołków do których da się dojść z u ścieżką długości 1. Druga część to T_2 czyli zbiór wierzchołków do których da się dojść z u ścieżką długości 2. Jeśli istnieje wierzchołek w w T_1 taki że istnieje ścieżka z w do v, to teza jest spełniona, bo z wierzchołka u da się dojść do wierzchołka v ścieżką długości 2 przechodzącą przez wierzchołek w.



Załóżmy więc że nie istnieje taki wierzchołek. Do każdego wierzchołka z T_2 dochodzimy ścieżką przechodzącą przez wierzchołek z T_1. Zatem z wierzchołka v do wierzchołka u można dojść ścieżką długości 1, do każdego wierzchołka z T_1 można dojść ścieżką długości 1, natomiast do każdego wierzchołka z T_2 można dość ścieżką długości 1 gdy istnieje bezpośrednia krawędź lub ścieżką długości 2 przechodzącą przez wierzchołek z T_1. Zatem w grafie G o $n+1$ wierzchołkach tezę spełnia wierzchołek u lub wierzchołek v.



Zadanie 2.
Turniej T nazywamy *silnie regularnym* jeśli moce zbiorów $D_v = \{w : v \to w \in E(T)\}$ oraz $C_{v,u} = \{w : v \to w, u \to w \in E(T)\}$ nie zależą od wyboru wierzchołków $v, u \in V(T)$. Udowodnij, że jeśli silnie regularny turniej n-wierzchołkowy istnieje, gdzie $n > 1$, to $4|n-3$.

Rozwiązanie:
Warunek że moc zbioru D_v nie zależy od wyboru wierzchołka v oznacza, że każdy wierzchołek ma tyle samo krawędzi wychodzących.
W klice jest $\binom{n}{2}$ krawędzi. Chcemy podzielić te krawędzie pomiędzy wierzchołki tak, aby każdy wierzchołek dostał tyle samo krawędzi.

$$n \mid \frac{n(n-1)}{2} \Leftrightarrow 2 \mid n-1$$

Z kolei jeśli każdy wierzchołek jest nieparzysty, to ma przyście wiele krawędzi z nim incydentnych, zatem istnieje w nim ścieżka Eulera, czyli można odpowiednio skierować krawędzie przechodząc po ścieżce. Każdy wierzchołek ma więc stopień wyjściowy i wejściowy równy równy $\frac{n-1}{2}$.
Warunek, że moc zbioru $C_{v,u}$ nie zależy od wyboru wierzchołków v i u oznacza, że każde dwa dowolne wierzchołki mają tyle samo wspólnych sąsiadów.
Dla danego wierzchołka w liczba par których jest wspólnym sąsiadem wynosi $\binom{\frac{n-1}{2}}{2}$. Mamy n wierzchołków, zatem łącznie takich par jest $n \cdot \binom{\frac{n-1}{2}}{2} = n \cdot \frac{(n-1)(n-3)}{8}$. Zatem

$$8 \mid n(n-1)(n-3)$$

Niech moc zbioru $C_{v,u} = x$. Parę wierzchołków możemy wybrać na $\binom{n}{2} = \frac{n(n-1)}{2}$ sposobów. Dla danej pary wierzchołek w będący ich wspólnym sąsiadem możemy wybrać na x sposobów, mamy więc

$$x \cdot \frac{n(n-1)}{2} = n \cdot \frac{(n-1)(n-3)}{8} \Leftrightarrow x = \frac{n-3}{4}$$

zatem

$$4 \mid n-3$$

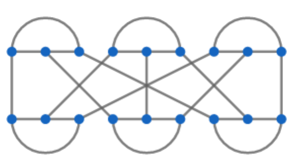
Zadanie 3.
Znajdź liczbę drzew rozpinających grafu $K_n \setminus \{e\}$ dla $n \geq 3$, gdzie $e \in E(K_n)$ jest pewną istaloną krawędzią.

Rozwiązanie:
Liczbę drzew rozpinających klikę K_n możemy wyznaczyć znajdując bijekcję między drzewami oraz $(n-2)$-ciągami o elementach ze zbioru $\{1, ..., n\}$. Wyznaczmy liczbę drzew zawierających krawędź e. Niech krawędź e łączy wierzchołki $n-1$ oraz n. Jak mamy sobie drzewo i tworzymy z niego kod Prufera, to usuwamy po kolei wierzchołki i krawędzie. Pozostają nam na koniec dwa wierzchołki. Jednym z nich jest wierzchołek n. W naszym przypadku chcemy, aby te dwa wierzchołki to były n oraz $n-1$. W przedostatnim kroku mamy trzy wierzchołki i oraz $n-1$ i n, przy czym $i < n-1$. Te trzy wierzchołki są połączone dwoma krawędziami. Chcemy, aby połączone były wierzchołki n oraz $n-1$, zatem wierzchołek i musi być liściem. Ostatnią liczbą w kodzie Prufera musi być więc liczba $n-1$ lub n. Takich ciągów mamy $2 \cdot n^{n-3}$. Zatem drzew rozpinających klikę K_n które zawierają w sobie krawędź e jest $2n^{n-3}$. Wszystkich drzew rozpinających w klice mamy n^{n-2}, zatem liczba drzew rozpinających grafu bez ustalonej krawędzi wynosi $n^{n-2} - 2n^{n-3}$.

Zadanie 4.
Udowodnij, że jeśli G jest grafem 100-wierzchołkowym, w którym 90 wierzchołków ma stopień nie większy niż 9, to $\chi(G) \leq 10$.

Rozwiązanie:
Pokażemy że $n+10$ wierzchołkowy graf, gdzie n wierzchołków ma stopień nie większy niż 9 ma liczbę chromatyczną nie większą niż 10. Niech zbiór wierzchołków o stopniu nie większym niż 9 to A. Dla $n = 1$ weźmy wierzchołek $v \in A$ i usuńmy go z grafu. Otrzymujemy graf 10 wierzchołkowy, który ma liczbę chromatyczną nie większą niż 10. Dokładając wierzchołek v do tego grafu, sąsiaduje on z co najwyżej dziewięcioma wierzchołkami, zatem może mieć kolor tego dziesiątego wierzchołka z którym nie sąsiaduje. Załóżmy więc że da sie pokolorować graf o $10+n$ wierzchołkach maksymalnie 10 kolorami. Rozważmy graf o $10+n+1$ wierzchołkach. Weźmy dowolny wierzchołek $v \in A$ i usuńmy go z grafu. Wówczas z założenia indukcyjnego dany graf o $10+n$ wierzchołkach da się pokolorować maksymalnie 10 kolorami. Dokładając wierzchołek v do grafu, sąsiaduje on z maksymalnie 9 wierzchołkami, zatem możemy go pokolorować na 10 kolor.
Wykazaliśmy więc że $n+10$ wierzchołkowy graf, gdzie n wierzchołków ma stopień nie większy niż 9 ma liczbę chromatyczną nie większą niż 10, zatem podstawiając $n = 90$ otrzymujemy tezę.

Zadanie 5.
Niech G_n będzie grafem powstającym przez zastąpienie każdego wierzchołka w grafie $K_{n,n}$ kliką K_n. Na przykład G_3 to



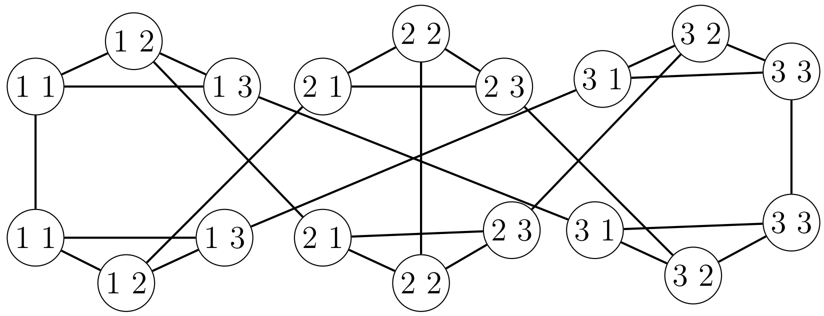
Formalnie

$$V(G_n) = \{x_{i,j} \; : \; 0 \leq i, j < n\} \cup \{y_{i,j} \; : \; 0 \leq i, j < n\}$$

$$E(G_n) = \bigcup_{0 \leq i < n} \bigcup_{0 \leq j \neq j' < n} \{\{x_{i,j}, x_{i,j'}\}\} \cup \bigcup_{0 \leq i < n} \bigcup_{0 \leq j \neq j' < n} \{\{y_{i,j}, y_{i,j'}\}\} \cup \bigcup_{0 \leq i < n} \{\{x_{i,j}, y_{j,i}\}\}$$

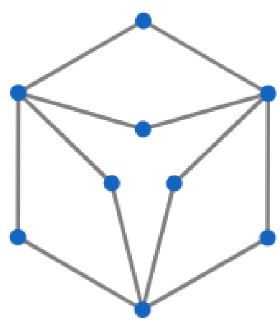
Znajdź liczbę chromatyczną i indeks chromatyczny grafu G_{2016}.

Rozwiązanie:



Wierzchołki w składowej na górze to $x_{i,j}$, natomiast w składowej na dole to $y_{i,j}$. Możemy pokolorować graf n kolorami. Niech kolory to odpowiednio liczby $1, 2, ..., n$, wówczas wierzchołek $x_{i,j}$ w składkowej na górze kolorujemy kolorme $i + j \mod n$, natomiast wierzchołek $y_{i,j}$ w składowej na dole kolorujemy kolorem $i + j + 1 \mod n$. Gwarantuje nam to że wierzchołki w klice mają różne kolory, oraz wierzchołki $x_{i,j}$ i $y_{j,i}$, czyli sąsiadujące ze sobą w różnych składowych, mają różne kolory. Graf G_n jest więc n kolorowalny.
Indeks chromatyczny kliki K_n to $n - [2|n]$. Dla n parzystych indeks chromatyczny wynosi n, bo $n - 1$ kolorami kolorujemy klikę, a krawędź łączącą składowe kolorujemy innym kolorem.

Zadanie 6.
Znajdź wielomian chromatyczny poniższego grafu:



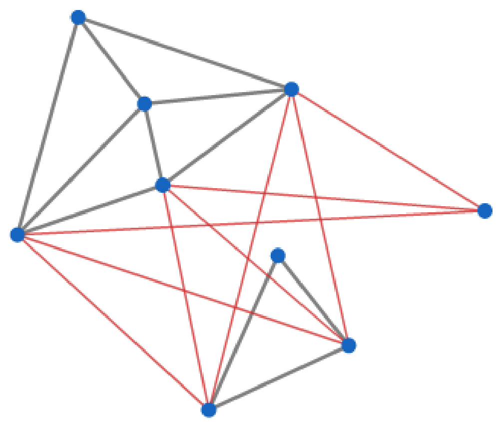
Rozwiązanie:
Jeśli wszystkie trzy wierzchołki o stopniu 4 mają różne kolory, to można pierwszy pokolorować na x sposobów, drugi na $x - 1$, natomiast trzeci na $x - 2$ sposoby. Pozostałe wierzchołki o stopniu 2 można pokolorować na $x - 2$ sposoby. Daje nam to $x(x - 1)(x - 2)^7$ sposobów.
Jeśli wszystkie trzy wierzchołki o stopniu 4 mają jednakowy kolor, to można pokolorować je na x kolorów, a pozostałe wierzchołki o stopniu 2 można pokolorować na $x - 1$ sposobów. Daje nam to $x(x - 1)^6$ sposobów.
Jeśli dwa wierzchołki o stopniu 4 mają ten sam kolor, a trzeci jest innego koloru, to wybieramy sobie na $\binom{3}{1} = 3$ sposobów wierzchołek który ma mieć inny kolor i kolorujemy go na x sposobów. Pozostałe dwa kolorujemy na $x - 1$ sposobów. Wierzchołki między tymi samymi kolorami kolorujemy na $x - 1$ sposobów, natomiast te między różnymi kolorujemy na $t - 2$ sposoby. Daje nam to $3x(x - 1)^3(x - 2)^4$.

Otrzymujemy więc

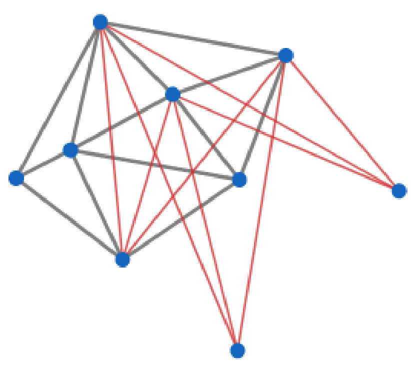
$$f(x) = x(x-1)(x-2)^7 + x(x-1)^6 + 3x(x-1)^3(x-2)^4$$

Zadanie 7.
G jest planarnym grafem 9-wierzchołkowym o 3 spójnych składowych. Udowodnij, że graf G' (dopełnienie grafu G) jest nieplanarny.

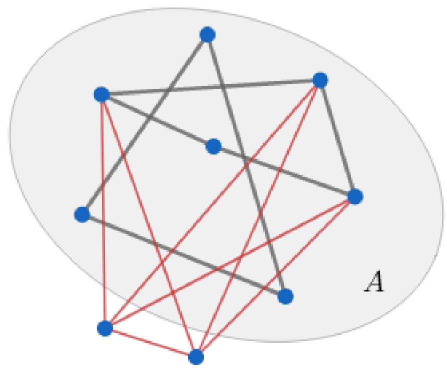
Rozwiązanie:
Rozpatrzmy przypadki. Jeśli dwie mniejsze spójne składowe mają łącznie co najmniej 3 wierzchołki, to dopełnienie grafu zawiera podgraf $K_{3,3}$, zatem nie jest to graf planarny.



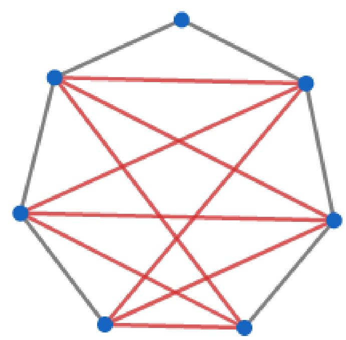
Możemy więc założyć, że jedna składowa ma 7 wierzchołków, a pozostałe mają po 1. Niech składowa z 7 wierzchołkami to A, natomiast pozostałe dwie to B i C. Suma krawędzi w składowej A i w jej dopełnieniu wynosi $\frac{7 \cdot 6}{2} = 21$. Jeśli jakiś wierzchołek w składowej A ma mniej niż trzy krawędzie, to wraz z wierzchołkami z B i z C tworzą podgraf $K_{3,3}$.



Zatem wszystkie wierzchołki w składowej A mają stopień co najmniej 4. Z nierówności $m \leq 3n - 6$ otrzymujemy, że składowa A ma maksymalnie 15 krawędzi. Wówczas jej dopełnienie ma co najmniej 6 krawędzi. Gdyby dopełnienie miało 7 krawędzi, to istniałby cykl i wraz z wierzchołkami z B i C powstałby podgraf homeomorficzny z K_5.



Dopełnienie grafu nie może mieć więc 7 krawędzi, czyli musi mieć 6 krawędzi. Krawędzie te muszą tworzyć drzewo. Jednak jako że w składowej A wszystkie wierzchołki miały stopień co najmniej 4, toteż w dopełnieniu wierzchołki będą miały stopień co najwyżej 2. Zatem krawędzie w dopełnieniu będą tworzyły ścieżkę składającą się z 6 krawędzi.



Jednak w takiej sytuacji łatwo znaleźć w składowej A podgraf $K_{3,3}$. Wyczerpaliśmy więc wszystkie możliwości, czyli dopełnienie 9-wierzchołkowego grafu planarnego o 3 składowych musi być nie planarne.

Zadanie 8.
Niech $p > 2$ będzie liczbą pierwszą. Udowodnij, że ułamek nieskracalny reprezentujący liczbę H_{p-1} ma licznik podzielny przez p.

Rozwiązanie:
Po sprowadzeniu ułamka do wspólnego mianownika, teza jest równoważna temu, że

$$p \mid \frac{(p-1)!}{1} + \frac{(p-1)!}{2} + \frac{(p-1)!}{3} + ... + \frac{(p-1)!}{(p-1)}$$

Nawet jeśli ten licznik jest skracalny z mianownikiem równym $(p-1)!$, to nie skracają się przez p. Zauważmy, że mamy parzyście wiele składników zatem możemy dobrać te liczby w pary. Dla dowolnego $x < p$ mamy $x(p-x) \mid (p-1)!$, zatem

$$p \mid \frac{(p-1)!}{x} + \frac{(p-1)!}{p-x} \Leftrightarrow p \mid \frac{(p-1)!p}{x(x-p)}$$

x oraz $p-x$ są to różne mniejsze od p liczby naturalne, zatem dobierając w pary składnik x-ty oraz $p-x$-ty otrzymujemy liczbę podzielną przez p, skąd i cała suma dzieli się przez p.

Zadanie 9.
Udowodnij następującą cechę podzielności: liczba n jest podzielna przez 73 wtedy i tylko wtedy, gdy różnica liczby złożonej z czterech ostatnich cyfr zapisu dziesiętnego n i liczby złożonej z pozostałych cyfr jest podzielna przez 73 (np. liczba 12345687 jest podzielna przez 73, ponieważ różnica $5687 - 1234 = 4453 = 73 \cdot 61$ jest podzielna przez 73).

Rozwiązanie:
Niech $m = n \mod 10^4$. Teza zadania jest równoważna temu, że

$$n \equiv 0 \mod 73 \Leftrightarrow m - \frac{n-m}{10^4} \equiv 0 \mod 73$$

Mamy $10^4 \equiv x \mod 73$, zatem wymnażając kongruencje stronami mamy

$$(10^4 + 1) \cdot m - n \equiv 0 \mod 73$$

$10^4 + 1 \equiv 0 \mod 73$, zatem teza jest prawdziwa.

Zadanie 10.
Oblicz $\underbrace{2^{2^{\cdots^{2}}}}_{2016} \mod 2016$

Rozwiązanie:
Szukamy rozwiązania dla kongruencji

$$\underbrace{2^{2^{\cdots^{2}}}}_{2016} \equiv x \mod 2016$$

Mamy $2016 = 2^5 \cdot 3^2 \cdot 7$, zatem

$$\underbrace{2^{2^{\cdots^{2}}}}_{2016} \equiv x \mod 2^5$$

$$\underbrace{2^{2^{\cdots^{2}}}}_{2016} \equiv x \mod 3^2$$

$$\underbrace{2^{2^{\cdots^{2}}}}_{2016} \equiv x \mod 7$$

Z pierwszej kongruencji od razu dostajemy $x \equiv 0 \mod 32$.
Z twierdzenia Eulera mamy $\phi(9) = 3^2 - 3 = 6$, czyli $2^6 \equiv 1 \mod 9$. Teraz chce policzyć jaka jest reszta z dzielenia $\underbrace{2^{2^{\cdots^{2}}}}_{2015}$ przez 6, czyli znaleźć rozwiązanie dla kongruencji $\underbrace{2^{2^{\cdots^{2}}}}_{2015} \equiv y \mod 6$ lub równoważnie układu kongruencji $\underbrace{2^{2^{\cdots^{2}}}}_{2015} \equiv y \mod 2 \Leftrightarrow y \equiv 0 \mod 2$ oraz $\underbrace{2^{2^{\cdots^{2}}}}_{2015} \equiv y \mod 3$. Drugą kongruencję znowu rozbijamy z twierdzenia Eulera. Mamy $\phi(3) = 3 - 1 = 2$, zatem $2^2 \equiv 1 \mod 3$. Reszta z dzielenia $\underbrace{2^{2^{\cdots^{2}}}}_{2014}$ przez 4 jest równa 0, zatem $y \equiv 1 \mod 3$, skąd również otrzymyjemy, że $y \equiv 4 \mod 6$, zatem $x \equiv 2^4 \mod 9$, czyli $x \equiv 7 \mod 9$.

Mamy $\phi(7) = 7 - 1 = 6$, zatem $2^6 \equiv 1 \mod 7$. Reszta z dzielenia $\underbrace{2^{2^{\cdots^2}}}_{2015}$ przez 6 wynosi 4, zatem $x \equiv 2^4 \mod 7$, czyli $x \equiv 2 \mod 7$.
Daje nam to układ trzech kongruencji

$$\begin{cases} x \equiv 0 \mod 32 \\ x \equiv 7 \mod 9 \\ x \equiv 2 \mod 7 \end{cases}$$

Po rozwiązaniu otrzymujemy

$$x \equiv 1024 \mod 2016$$

Zadanie 11.
Udowodnij, że jeśli $n > 0$ jest parzyste, to $n^2 - 1 \mid 2^{n!} - 1$.

Rozwiązanie:
Skoro n jest parzyste, to $n-1$ oraz $n+1$ są względnie pierwsze, zatem $\phi(n^2-1) = \phi(n-1) \cdot \phi(n+1)$. Mamy $\phi(n-1) \leq n$, czyli $\phi(n-1) \mid n!$. Mamy $\phi(n+1) \leq n$, czyli $\phi(n+1) \mid n!$. Zatem również $\phi(n-1) \cdot \phi(n+1) = \phi(n^2-1) \mid n!$. Mamy więc $n! = k \cdot \phi(n^2-1)$. Z twierdzenia Eulera mamy $2^{\phi(n^2-1)} \equiv 1 \mod (n^2-1)$, zatem również $2^{k \cdot \phi(n^2-1)} \equiv 1 \mod (n^2-1) = 2^{n!} \equiv 1 \mod (n^2-1)$, skąd otrzymujemy $2^{n!} - 1 \equiv 0 \mod (n^2-1) \Leftrightarrow n^2 - 1 \mid 2^{n!} - 1$

Zadanie 12.
Znajdź liczbę rozwiązań kongruencji $x^{118} \equiv 113 (\mod 1001)$ w zbiorze $\{0, ..., 1000\}$ i podaj jedno z nich.

Rozwiązanie:
Oczywiście $1001 = 7 \cdot 11 \cdot 13$, zatem mamy

$$x^{118} \equiv 113 \mod 7 \Leftrightarrow x^{118} \equiv 1 \mod 7$$

$$x^{118} \equiv 113 \mod 11 \Leftrightarrow x^{118} \equiv 3 \mod 11$$

$$x^{118} \equiv 113 \mod 13 \Leftrightarrow x^{118} \equiv 9 \mod 13$$

Skoro 113 jest względnie pierwszy z liczbą $p \in \{7, 11, 13\}$, to x też jest względnie pierwsze z p. Z twierdzenia Eulera mamy

$$x^{\phi(7)} \equiv 1 \mod 7 \Leftrightarrow x^6 \equiv 1 \mod 7$$

$$x^{\phi(11)} \equiv 1 \mod 11 \Leftrightarrow x^{10} \equiv 1 \mod 11$$

$$x^{\phi(13)} \equiv 1 \mod 13 \Leftrightarrow x^{12} \equiv 1 \mod 13$$

Mamy więc

$$x^4 \equiv 1 \mod 7 \Leftrightarrow x \equiv 1 \mod 7 \lor x \equiv 6 \mod 7$$

$$x^8 \equiv 3 \mod 11 \Leftrightarrow x \equiv 2 \mod 11 \lor x \equiv 9 \mod 11$$

$$x^{10} \equiv 9 \mod 13 \Leftrightarrow x \equiv 4 \mod 13 \lor x \equiv 9 \mod 13$$

Daje nam to 8 układów równań, zatem rozwiązań $x^{118} \equiv 113(\mod 1001)$ jest 8. Jednym z układów równań jest

$$\begin{cases} x \equiv 1 \mod 7 \\ x \equiv 2 \mod 11 \\ x \equiv 4 \mod 13 \end{cases}$$

Rozwiązaniem tego układu jest $x \equiv 134 \mod 1001$.