Douczki z Matematyki Dyskretnej 2023

Dzień pierwszy

Zajęcia prowadzone są w ramach wolontariatu przez członka KPM, który jest studentem. Miej na uwadze to, że może nie być w stanie on odpowiedzieć na wszystkie zadane przez Was pytania.

1. Podziały liczb

Zadanie 1.

Udowodnij, że liczba podziałów n na składniki dające resztę 1 lub 5 z dzielenia przez 6 jest równa liczbie podziałów n na różne składniki niepodzielne przez 3.

Rozwiązanie:

Wyznaczmy najpierw enumerator podziału liczby n na składniki dające resztę 1 lub 5 przy dzieleniu przez 6. Liczby spełniające ten warunek są postaci $6k+1$ oraz $6k+5$. Zatem

$$A(x) = (1 + x + x^2 + x^3 + \ldots) \cdot (1 + x^5 + x^{10} + x^{15} + \ldots) \cdot (1 + x^7 + x^{14} + x^{21} + \ldots) \cdot$$
$$\cdot \ldots \cdot (1 + x^{6k+1} + x^{2(6k+1)} + \ldots) \cdot (1 + x^{6k+5} + x^{2(6k+5)} + \ldots) \cdot \ldots =$$
$$= \frac{1}{(1-x)(1-x^5)(1-x^7)\ldots(1-x^{6k+1})(1-x^{6k+5})\ldots}$$

Wyznaczmy enumerator podziałów liczby n na różne składniki, które są niepodzielne przez 3. Liczby spełniające ten warunek są postaci $3k+1$ oraz $3k+2$. Zatem

$$B(x) = (1+x) \cdot (1+x^2) \cdot (1+x^4) \cdot \ldots \cdot (1+x^{3k+1}) \cdot (1+x^{3k+2}) \cdot \ldots$$

Chcemy udowodnić, że $A(x) = B(x)$. Pomnóżmy więc każdy z enumeratorów przez enumerator

$$E(x) = (1-x) \cdot (1-x^2) \cdot (1-x^4) \cdot (1-x^5) \cdot \ldots$$

Mamy

$$A(x) \cdot E(x) = \frac{(1-x) \cdot (1-x^2) \cdot (1-x^4) \cdot \ldots}{(1-x)(1-x^5)(1-x^7) \cdot \ldots}$$

Zauważmy, że w liczniku mamy składniki w postaci $(1-x^{3k+1})$ oraz $(1-x^{3k+2})$, czyli wyrażenia postaci $(1-x^{6k+1})$, $(1-x^{6k+2})$, $(1-x^{6k+4})$ oraz $(1-x^{6k+5})$. W mianowniku mamy wyrażenia postaci $(1-x^{6k+1})$ oraz $(1-x^{6k+5})$, zatem po skróceniu, wyrażenia w iloczynie $A(x) \cdot E(x)$ będą postaci $(1-x^{6k+2})$ oraz $(1-x^{6k+4})$.

Mamy

$$B(x) \cdot E(x) = (1-x^2) \cdot (1-x^4) \cdot (1-x^8) \cdot (1-x^{10}) \cdot \ldots$$

czyli mamy wyrażenia postaci $(1-x^{6k+2})$ oraz $(1-x^{6k+4})$.

Ponieważ otrzymaliśmy to samo, stąd $A(x) = B(x)$, czyli liczba podziałów n na składniki dające resztę 1 lub 5 z dzielenia przez 6 jest równa liczbie podziałów n na różne składniki niepodzielne przez 3.

Zadanie 2.

Udowodnij, że liczba $\frac{(kn)!}{k!(n!)^k}$ jest całkowita dla dowolnych naturalnych n i k.

Zadanie 3.
Udowodnij, że liczba podziałów liczby n na cztery części jest taka sama jak liczba podziałów liczby $3n$ na cztery części o rozmiarze co najwyżej $n-1$.

Rozwiązanie:
Aby udowodnić to stwierdzenie, pokażemy bijekcję między zbiorami podziałów.
Weźmy dowolny podział n na liczby $\{a_1, a_2, a_3, a_4\}$. Ma to postać:

$$\sum_{i=1}^{4} a_i = n$$

Teraz rozważmy podział $\{n-a_1, n-a_2, n-a_3, n-a_4\}$. Mamy:

$$(n-a_1)+(n-a_2)+(n-a_3)+(n-a_4) = 4n - \sum_{i=1}^{4} a_i = 3n$$

Dodatkowo, dla każdego i, $1 \leq a_i \leq n-1$, więc dla każdego i, $1 \leq n-a_i \leq n-1$. Oznacza to, że wszystkie warunki są spełnione.

Zadanie 4.
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

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

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

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

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

2. Zadania z grafów

Zadanie 1.
Niech $G = (V, E)$ będzie grafem, takim że $E = E_1 \cup E_2$, gdzie graf $G_1 = (V, E)$ jest planarny zaś $G_2 = (V, E_2)$ jest lasem. Udowodnij, że $\chi(G) < 9$.

Rozwiązanie:
Każdemu wierzchołkowi v z grafu G przypisujemy krotkę (a, b), gdzie a to kolor wierzchołka v w grafie G_1, zaś b to kolor wierzchołka v w grafie G_2. Różnych krotek w grafie G możemy mieć maksymalnie $4 \cdot 2 = 8$, więc jeśli krotki oznaczają kolory w grafie to $\chi(G) < 9$.

Zadanie 2.
Niech G będzie grafem o liczbie chromatycznej $\chi(G) \leq 8$. Udowodnij, że G jest sumą trzech rozłącznych krawędziowo grafów dwudzielnych.

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.
Niech $G_1, ..., G_{10}$ będą grafami planarnymi o tym samym zbiorze wierzchołkó V i zbiorach krawędzi, odpowiednio, $E_1, ..., E_{10}$. Rozważmy stanowiący ich sumę graf $G = \langle V, E \rangle$ gdzie $E = \bigcup_{i=1}^{10} E_i$. Udowodnij, że $\chi(G) \leq 60$.

Rozwiązanie:
Z tego że grafy są planarne, można wywnioskować, że

$$m_1 \leq 3n - 6$$

$$m_2 \leq 3n - 6$$

$$\vdots$$

$$m_{10} \leq 3n - 6$$

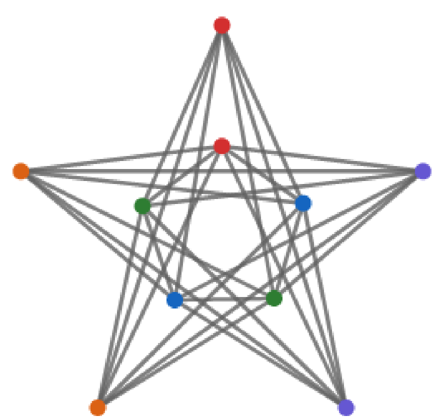
Zatem

$$m_1 + m_2 + ... + m_{10} \leq 30n - 60$$

Zauważmy, że teza jest oczywista dla $n \leq 60$. Rozważmy graf o $60 + x$ wierzchołkach. Mamy $30 \cdot (60 + x) - 60 = 1800 + 30x - 60$, zatem wynika z tego, że suma krawędzi grafów planarnych ma co najwyżej $1740 + 30x$ krawędzi. Grafu nie będzie się dało pokolorować 60 kolorami, gdy każdy wierzchołek będzie stopnia większego niż 60. Ale taki graf ma co najmniej $\frac{(60+x)\cdot 60}{2} = 1800 + 30x$ krawędzi, czyli nie może być sumą grafów planarnych. Gdy będzie miał stopień mniejszy niż 60 to można pokolorować, bo wystarczy zastosować indukcję taką jaką robiliśmy dowodząc, że graf planarny da się pokolorować 6 kolorami.

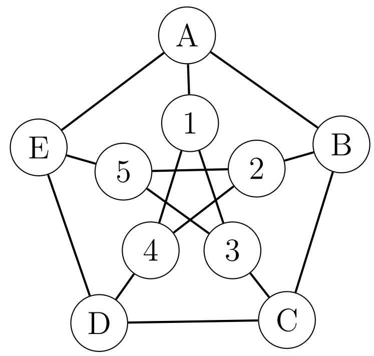
Zadanie 5.
Niech G będzie dopełnieniem grafu Petersena. Znajdź $\chi(G)$.

Rozwiązanie:
Graf można pokolorować 5 kolorami, bo dowodzi to poniższy rysunek.

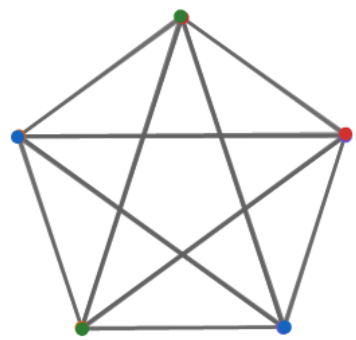


Pokażemy teraz że nie można pokolorować grafu mniej niż 5 kolorami.

Jeśli w grafie Petersena wierzchołki były poetykietowane tak:



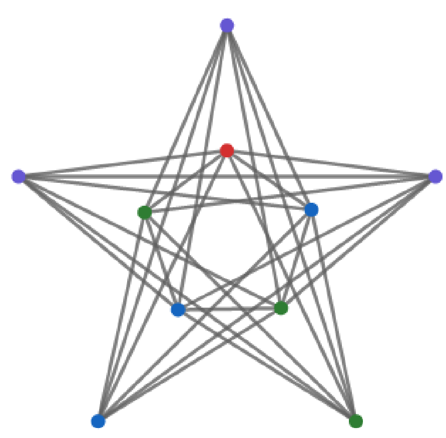
to po ściągnięciu krawędzi w dopełnieniu łączących wierzchołki 1 i B oraz 2 i C oraz 3 i D oraz krawędzi łączącej 4 i E oraz 5 i A, otrzymujemy graf



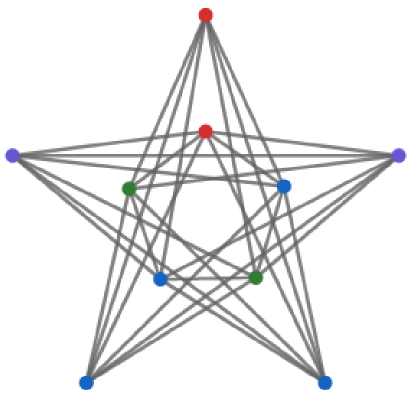
czyli z twierdzenia Wagnera, dopełnienie grafu nie jest planarne.

Zastanówmy sie teraz, czy możemy jakoś przemalować wierzchołki z rysunku pierwszego tak, aby użyć czterech kolorów. Jasne jest że wewnętrze trzeba pokolorować tak jak na rysunku, gdyż jest tam cykl długości 5. Z tego samego powodu (w grafie Petersena można zamienień wnętrze z zewnętrzem nie zmieniając kształtu grafu) zewnętrze będzie potrzebować trzech kolorów. Chcemy jednak pokolorować graf 4 kolorami, czyli dwa kolory muszą być takie same jak z wnętrza.

Jasne jest że nie mogą to być te kolory co we wnętrzu były dwa razy, bo wierzchołek A musi mieć inny od nich kolor, czyli wierzchołek D musi mieć taki sam kolor jak wierzchołek 3 oraz wierzchołek C musi mieć taki sam kolor jak wierzchołek 4. Wierzchołki E i B nie mogą mieć kolorów tych dwóch z wewnętrza, ale nie mogą mieć też tego samego koloru.



Rozpatrzmy więc pierwszy kolor który we wewnętrzu jest dwa razy i drugi kolor który we wewnętrzu jest raz. Wierzchołki D i C muszą być tego koloru co jest we wewnętrzu dwa razy. Wierzchołek A musi być koloru tego co we wewnętrzu występuje raz. Wierzchołki B i E muszą być więc pokolorowane innym kolorem niż te które do tej pory użyliśmy, ale nie da się ich pokolorować tak, gdyż sąsiadują ze sobą.

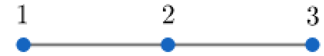


Rozpatrzyliśmy więc wszystkie przypadki i nie udało nam sie znaleźć kolorowania czterema kolorami, zatem dopełnienie grafu Petersena jest 5-kolorowalne, czyli $\chi(G) = 5$.

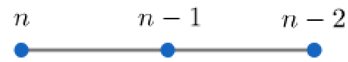
Zadanie 6.
Udowodnij, że jeśli G jest grafem 100-wierzchołkowym, w którym 90 wierzchołków ma stopień nie większy niż 9, to $\chi(G) \leq 10$.

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.

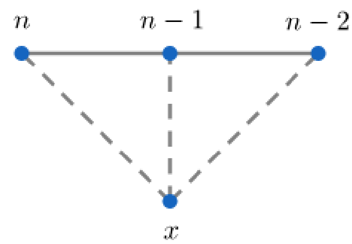
Zadanie 7.
Znajdź liczbę etykietowanych drzew 10-wierzchołkowych, które zawierają drzewo jako podgraf.



Rozwiązanie:
Równie dobrze moglibyśmy rozważać te wierzchołki jako $n, n-1, n-2$ i szukać liczby drzew zawierające takie drzewo jako podgraf.



Jak mamy sobie graf Prufera, to usuwamy po kolei liście o najmniejszym stopniu. W przed ostatnim kroku chcemy, aby wierzchołek $n-2$ był połączony z wierzchołkiem $n-1$ oraz $n-1$ z n, czyli aby ostatnia liczba w kodzie Prufera to była $n-1$. Przyjrzyjmy się przedostatniej liczbie w kodzie Prufera. Będzie to numer wierzchołka z którym będzie połączony 4 od końca liść. Może on być połączony z którymkolwiek z wierzchołków $n, n-1, n-2$, ponieważ ma od nich mniejszy numer.



Zatem przed ostatnia liczba w kodzie Prufera to będzie n, $n-1$ lub $n-2$. Liczba drzew n wierzchołkowych zawierających drzewo z rysunku drugiego jako podgraf wynosić więc będzie $1 \cdot 3 \cdot n^{n-4}$, zatem dla $n = 10$ mamy $3 \cdot 10^6$. Tyle też będzie wynosić liczba drzew zawierających drzewo z rysunku pierwszego jako podgraf, bo wystarczy wziąć numer wierzchołka modulo n a potem dodać 3.

3. Zadania z teorii liczb

Zadanie 1.
Udowodnij, że liczba $n \geq 2$ oraz $n+2$ są jednocześnie pierwsze wtedy i tylko wtedy, gdy

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n(n+2)$$

Rozwiązanie:
$\Rightarrow$ Z twierdzenia Wilsona wiemy, że p jest pierwsze wtedy i tylko wtedy gdy $(p-1)! \equiv -1 \mod p$. Mamy więc

$$(n-1)! \equiv -1 \mod n$$

$$(n+1)! \equiv -1 \mod n+2$$

Wówczas dla pierwszej kongruencji mamy

$$(n-1)! + 1 \equiv 0 \mod n$$

$$4(n-1)! + 4 \equiv 0 \mod n$$

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n$$

Z drugiej kongruencji mamy

$$(n+1)! + 1 \equiv 0 \mod n+2$$

$$2(n+1)! + 2 \equiv 0 \mod n+2$$

$$2(n+1)! - n \equiv 0 \mod n+2$$

$n \perp n+2$ oraz $n+1 \perp n+2$, zatem możemy podzielić przez $n(n+1)$. Mamy

$$2(n-1)! + 1 \equiv 0 \mod n+2$$

$$4(n-1)! + 2 \equiv 0 \mod n+2$$

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n+2$$

Otrzymujemy więc

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n$$

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n+2$$

Z twierdzenia z wykładu mamy więc

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n(n+2)$$

$\Leftarrow$ Jeśli $2 \mid n$, to $n = 2k$ oraz $n+2 = 2k+2$, wówczas

$$4 \cdot (2k-1)! + 4 + 2k \not\equiv 0 \mod 2k(2k+2)$$

ponieważ

$$2 \cdot (2k-1)! + 2 + k \not\equiv 0 \mod 2k(k+1)$$

$$2(2k-1)! + 2 + k \equiv 2 \mod k$$

$$2(2k-1)! + 2 + k \equiv 1 \mod k+1$$

Załózmy więc, że $2 \not\mid n$. Wówczas n oraz $n+2$ są względnie pierwsze, czyli z faktu z wykładu

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n$$

$$4 \cdot (n-1)! + 4 + n \equiv 0 \mod n+2$$

Z pierwszej kongruencji mamy

$$4(n-1)! + 4 \equiv 0 \mod n$$

$$(n-1)! + 1 \equiv 0 \mod n$$

czyli z twierdzenia Wilsona n jest pierwsze. Natomiast z drugiej mamy

$$4(n-1)! + 2 \equiv 0 \mod n+2$$

$$2(n+1)! - n \equiv 0 \mod n+2$$

$$2(n+1)! + 2 \equiv 0 \mod n+2$$

$$(n+1)! + 1 \equiv 0 \mod n+2$$

Zatem również $n+2$ jest pierwsze z twierdzenia Wilsona.

Zadanie 2.
Wykaż, że dla dowolnych liczb całkowitych a i b zachodzi

$$NWW(a,b) \cdot NWD(a,b) = a \cdot b$$

Rozwiązanie:
Niech $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ i $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$, wówczas $NWW(a,b) = p_1^{max(\alpha_1,\beta_1)} \dots p_n^{max(\alpha_n,\beta_n)}$ oraz $NWD(a,b) = p_1^{min(\alpha_1,\beta_1)} \dots p_n^{min(\alpha_n,\beta_n)}$, więc

$$NWD(a,b) \cdot NWW(a,b) = p_1^{min(\alpha_1,\beta_1)} p_2^{min(\alpha_2,\beta_2)} \dots p_n^{min(\alpha_n,\beta_n)} \cdot p_1^{max(\alpha_1,\beta_1)} p_2^{max(\alpha_2,\beta_2)} \dots p_n^{max(\alpha_n,\beta_n)} =$$

$$= p_1^{min(\alpha_1,\beta_1)+max(\alpha_1,\beta_1)} p_2^{min(\alpha_2,\beta_2)+max(\alpha_2,\beta_2)} \dots p_n^{min(\alpha_n,\beta_n)+max(\alpha_n,\beta_n)} = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \dots p_n^{\alpha_n+\beta_n} =$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \cdot p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n} = a \cdot b$$

Zadanie 3.
Udowodnić, że liczba $93^{93} - 33^{33}$ dzieli się przez 10.

Rozwiązanie:
Zauważmy, że zachodzą kongruencje $93 \equiv 3 \mod 10$, $33 \equiv 3 \mod 10$, zatem

$$93^{93} \equiv 3^{93} \mod 10 \qquad 33^{33} \equiv 3^{33} \mod 10$$

Mamy również $3^4 = 81 \equiv 1 \mod 10$, zatem

$$3^{93} = (3^4)^{23} \cdot 3 \equiv 3 \mod 10 \qquad 3^{33} = (3^4)^8 \cdot 3 \equiv 3 \mod 10$$

Skąd $93^{93} \equiv 33^{33} \mod 10$.

Zadanie 4.
Wyznacz wszystkie liczby całkowite dodatnie n, dla których liczba $2^n - 1$ jest podzielna przez 7.

Rozwiązanie:
Szukamy takich n, że $2^n \equiv 1 \mod 7$. Zauważmy, że $2^3 = 8 \equiv 1 \mod 7$, zatem

$$2^{3k} = (2^3)^k \equiv 1 \mod 7$$

$$2^{3k+1} = (2^3)^k \cdot 2 \equiv 2 \mod 7$$

$$2^{3k+2} = (2^3)^k \cdot 2^2 \equiv 4 \mod 7$$

Zatem $2^n - 1$ dzieli się przez 7 dla $3 \mid n$.

Zadanie 5.
Wyznacz ostatnie dwie cyfry liczby 2012^{2012}.

Rozwiązanie:
Wystarczy zbadać, jaką resztę daje podana liczba przy dzieleniu przez 100. Zauważmy, iż $2012 \equiv 12 \mod 100$ oraz $144 \equiv 44 \mod 100$, skąd

$$2012^{2012} \equiv 12^{2012} = (12^2)^{1006} = 144^{1006} \equiv 44^{1006} \mod 100$$

Dalej

$$44^2 = 1936 \equiv 36 \mod 100 \qquad \text{oraz} \qquad 36^2 = 1296 \equiv -4 \mod 100$$

skąd wynika, że

$$44^4 \equiv -4 \mod 100$$

Zatem

$$2012^{2012} \equiv 44^2 \cdot (44^4)^{251} \equiv 36 \cdot (-4)^{251} = -9 \cdot 4^{252} \mod 100$$

Wteszcie $4^4 = 256 = -44 \mod 100$, skąd

$$2012^{2012} \equiv -9 \cdot (4^4)^{63} \equiv 9 \cdot 44^{63} = 9 \cdot 44 \cdot 44^2 \cdot (44^4)^{15} \equiv$$

$$\equiv -9 \cdot 44 \cdot 36 \cdot 4^{15} = -11 \cdot 36 \cdot 4^{15} \equiv 11 \cdot 4^{16} \equiv 11 \cdot 44^4 \equiv 11 \cdot (-4) \equiv 56 \mod 100$$

Zadanie 6.
Wyznaczyć wszystkie liczby pierwsze p, dla których liczba $3^p + 4^p$ jest podzielna przez 181.

Rozwiązanie:
Mamy

$$3^5 + 4^5 = 243 + 1024 = 1267 = 181 \cdot 7$$

Podstawmy więc $p = 5k + l$ dla $l = 0, 1, 2, 3, 4$. Mamy

$$3^5 \equiv -4^5 \mod 181 \Leftrightarrow 3^{5k} \equiv (-1)^k \cdot 4^{5k} \mod 181$$

skąd

$$3^p + 4^p = 3^{5k+l} + 4^{5k+l} = 3^{5k} \cdot 3^l + 4^{5k} \cdot 4^l \equiv (-1)^k \cdot 4^{5k} \cdot 3^l + 4^{5k} \cdot 4^l = 4^{5k} \cdot [(-1)^k \cdot 3^l + 4^l] \mod 181$$

Skoro 181 jest pierwsze, to $3^p + 4^p$ dzieli się przez 181, gdy $(-1)^k \cdot 3^l + 4^l$ dzieli się przez 181, czyli

$$(-1)^k \cdot 3^l + 4^l \equiv 0 \mod 181$$

Dla k nieparzystego i $l = 0$ warunek ten jest oczywiście spełniony,zaś dla pozostałych k, l nie zachodzi. Sprawdzamy bowiem, że $3^0 + 4^0 = 2 \not\equiv 0 \mod 181$

$$1 \leq (-1)^k \cdot 3^l + 4^l \leq 180 \text{ dla } l = 1, 2, 3$$

oraz

$$\pm 3^4 + 4^4 = \pm 81 + 256 \not\equiv 0 \mod 181$$

Wykazaliśmy zatem, że liczba $3^p + 4^p$ dzieli się przez 181 wtedy i tylko wtedy,gdy p jest postaci $5k$ dla pewnej dodatniej liczby nieparzystej k. Ponieważ p ma być liczbą pierwszą, rozwiązanie $p = 5$, odgadnięte na wstępie, jest jedynym rozwiązaniem zadania.

Zadanie 7.
Dane są liczby całkowite dodatnie a, b, c, d, f takie, że

$$a + b = c + d = e + f = 101$$

Udowodnić, że liczby $\frac{ace}{bdf}$ nie można zapisać w postaci ułamka $\frac{m}{n}$, gdzie m, n są liczbami całkowitymi dodatnimi o sumie mniejszej niż 101.

Rozwiązanie:
Zapiszmy liczbę $\frac{ace}{bdf}$ w postaci ułamka nieskracalnego $\frac{m}{n}$. Istnieje zatem taka liczba całkowita dodatnia k, że $ace = k \cdot m$ oraz $bdf = k \cdot n$. Dalej mamy

$$a \equiv -b \mod 101$$

$$c \equiv -d \mod 101$$
$$e \equiv -f \mod 101$$

skąd

$$ace \equiv -bdf \mod 101$$

czyli $ace + bdf = k \cdot (m + n)$ dzieli się przez 101. Z drugiej strony 101 jest liczbą pierwszą i każda z liczb a, b, c, d, e, f jest mniejsza od 101, czyli ace oraz bdf nie dzielą się przez 101, a zatem k także nie dzieli się przez 101. Stąd $101 \mid m + n$, czyli $m + n \geq 101$.

Zadanie 8.
W pewnej klasie jest mniej niż 40 osób. Gdy uczniowie chcieli podzielić się na grupy 5-osobowe, 4 osoby zostały bez grupy. Gdy natomiast chcieli podzielić się na grupy 6-osobowe, 5 osób zostało bez grupy. Ilu uczniów jest w tej klasie?

Rozwiązanie:
Dołączmy do klasy jeszcze jednego ucznia; wtedy będzie można uczniów podzielić na grupy pięcioosobowe, a także na grupy sześcioosobowe, więc liczba uczniów będzie podzielna przez 30. Wobec tego liczba uczniów wyniesie dokładnie 30. Początkowo jest więc 29 uczniów.

Zadanie 9.
Wyznacz wszystkie liczby pierwsze p, dla których liczba $p^2 + 2$ jest pierwsza.

Rozwiązanie:
Zauważmy, że liczba 3 spełnia warunki zadania. Dowolna liczba pierwsza p może dawać resztę 1 lub 2 przy dzieleniu przez 3. Dla $p = 3k + 1$ mamy

$$p^2 + 2 = (3k + 1)^2 + 2 = 9k^2 + 6k + 3 = 3(3k^2 + 2k + 1)$$

zatem nie jest to liczba pierwsza. Dla $p = 3k + 2$ mamy

$$p^2 + 2 = (3k + 2)^2 + 2 = 9k^2 + 12k + 6 = 3(3k^2 + 4k + 2)$$

zatem to nie jest liczba pierwsza. Stąd jedyną liczbą spełniającą warunki zadania jest 3.

Zadanie 10.
Liczbę naturalną n pomnożono przez 3, otrzymując w wyniku liczbę 999^{1000}. Wyznacz cyfrę jedności liczby n.

Rozwiązanie:
Zauważmy, że liczba 999^2 jest zakończona cyfrą 1, wobec czego liczba $3n = (999^2)^{500}$ jest także zakończona cyfrą 1. Stąd wniosek, że liczba $21n = 7 \cdot 3n$ jest zakończona cyfrą 7. Jednak liczby $21n$ i n mają tę samą cyfrę jedności, gdyż ich różnica $21n - n = 20n$ jest zakończona cyfrą 0.

4. Zadania z grup

Zadanie 1.
Udowodnij, że w dowolnej grupie element neutralny oraz element odwrotny są wyznaczone jednoznacznie.

Rozwiązanie:
Niech e_1, e_2 to element neutralny wówczas $e_1 = e_1 \cdot e_2 = e_2 \cdot e_1 = e_2$. Czyli element neutralny jest wyznaczony jednoznacznie. Niech a' i a'' to elementy odwrotne elementu $a \in G$, wówczas $a' = e \cdot a' = (a'' \cdot a) \cdot a' = a'' \cdot (a \cdot a') = a'' \cdot e = a''$. $\square$

Zadanie 2.
Znajdź wszystkie podgrupy grupy $\mathbb{Z}_{12}$ oraz rzędy wszystkich jej elementów, gdzie $\mathbb{Z}_{12}$ jest cykliczną grupą rzędu 12.

Rozwiązanie:
Podgrupami będą $\langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle$. Mamy również

k	0	1	2	3	4	5	6	7	8	9	10	11
$o(k)$	1	12	6	4	3	12	2	12	3	4	6	12

Zadanie 3.
Sześcioelementowa grupa dihedralna D_6 to grupa izometrii trójkąta równobocznego.

a) Wykaż, że jest generowana przez dwa elementy: obrót - nazwijmy go ρ (zgodnie ze wskazówkami zegara) oraz symetrię osiową - nazwijmy ją σ. Wypisz każdy element jako iloczyn generatorów i napisz jaka to izometria płaszczyzny

b) Policz rząd każdego elementu

Rozwiązanie:

a) Dla trójkąta równobocznego o wierzchołkach A, B, C mamy

$$D_6 = \{id, o_{\frac{2\pi}{3}}, o_{\frac{4\pi}{3}}, S_A, S_B, S_C\}$$

Są to wszystkie izometrie, ponieważ permutacji wierzchołków trójkąta jest $3! = 6$. Działaniem w tej grupie jest składanie izometrii. Niech $o_{\frac{2\pi}{3}} = \rho$ oraz $S_A = \sigma$, wówczas $id = \rho^3 = \sigma^2$, $o_{\frac{4\pi}{3}} = \rho^2$, $S_B = \sigma \cdot \rho^2$, $S_C = \sigma \cdot \rho$. Zatem $\langle \rho, \sigma\rangle = D_6$.

b) Policzmy rząd każdego elementu.

k	id	$o_{\frac{2\pi}{3}}$	$o_{\frac{4\pi}{3}}$	S_A	S_B	S_C
$o(k)$	1	3	3	2	2	2

Mamy

- $\sigma^2 = id$
- $\rho^3 = id$
- $\sigma\rho\sigma = \rho^2$

Te trzy warunki wyznaczają nam działania w grupie.

Ogólnie dla $D_{2n} = \langle \rho, \sigma \rangle$ mamy działania $\sigma^2 = id$, $\rho^n = id$ oraz $\sigma\rho\sigma = \rho^{n-1}$.

Zadanie 4.
Niech $G = \mathbb{Z}_n$. Udowodnij, że wtedy dla dowolnego $r \in \mathbb{Z}_n$ zachodzi $o(r) = \frac{n}{NWD(n,r)}$.

Rozwiązanie:
Aby $\frac{n}{NWD(n,r)}$ było rzędem elementu r, to

1. liczba $r \cdot \frac{n}{NWD(n,r)}$ musi być podzielna przez n, bo wówczas $\frac{n}{NWD(n,r)} \cdot r$ to 0 w $\mathbb{Z}_n$
2. jeśli istnieje θ takie, że $\theta \cdot r = 0$ w $\mathbb{Z}_n$, to $\theta \geq \frac{n}{NWD(n,r)}$

Liczba $r \cdot \frac{n}{NWD(n,r)}$ jest podzielna przez n, ponieważ $\frac{r}{NWD(n,r)} \in \mathbb{Z}$, bo $NWD(n,r) \mid r$. Wiemy, że $n \mid \theta \cdot r$, gdzie $n = NWD(n,r) \cdot n'$ oraz $r = NWD(n,r) \cdot r'$ przy czym $NWD(n', r') = 1$. Mamy więc $NWD(n,r) \cdot n' \mid \theta \cdot NWD(n,r) \cdot r'$, czyli $n' \mid \theta \cdot r'$. Skoro $NWD(n', r') = 1$, to r' nie dzieli się przez n', czyli θ dzieli się przez n', skąd $\theta \geq n'$. Zatem $\theta \geq \frac{n}{NWD(n,r)}$.

Zadanie 5.
Niech $g \in G$ będzie elementem skończonego rzędu. Udowodnij, że $g^k = 1$ wtedy i tylko wtedy, gdy $o(g) \mid k$.

Rozwiązanie:
$\Rightarrow$ Załóżmy, że $g^k = 1$ oraz $k = o(g) \cdot m + r$ dla pewnego $0 \leq r < o(g)$. Wówczas

$$1 = g^k = g^{o(g) \cdot m + r} = \left(g^{o(g)}\right)^m \cdot g^r = 1 \cdot g^r$$

skąd otrzymujemy, że $r = 0$, zatem $o(g) \mid k$.
$\Leftarrow$ Jeśli $o(g) \mid k$, to wówczas $k = o(g) \cdot m$, czyli $g^k = g^{o(g) \cdot m} = \left(g^{o(g)}\right)^m = 1^m = 1$.

Zadanie 6.
Rozłóż na rozłączne cykle następujące permutacje

a) $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 5 & 1 & 4 & 2 & 6 & 9 & 8 & 10 \end{pmatrix}$

b) $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 1 & 10 & 2 & 4 & 3 & 5 & 8 & 9 & 6 \end{pmatrix}$

A następnie policz $\sigma_1 \cdot \sigma_2$, $\sigma_2 \cdot \sigma_1$ oraz $\sigma_1 \cdot \sigma_2 \cdot \sigma_1^{-1}$.

Rozwiązanie:

a) Mamy $\sigma_1 = (1\ 3\ 5\ 4)(2\ 7\ 6)(8\ 9)(10)$

b) Mamy $\sigma_2 = (1\ 7\ 5\ 4\ 2)(3\ 10\ 6)(8)(9)$

Dalej mamy

$$\sigma_1 \cdot \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 1 & 10 & 2 & 4 & 3 & 5 & 8 & 9 & 6 \\ 6 & 3 & 10 & 7 & 1 & 5 & 4 & 9 & 8 & 2 \end{pmatrix} = (1\ 6\ 5)(2\ 3\ 10)(4\ 7)(8\ 9)$$

$$\sigma_2 \cdot \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 5 & 1 & 4 & 2 & 6 & 9 & 8 & 10 \\ 10 & 5 & 4 & 7 & 2 & 1 & 3 & 9 & 8 & 6 \end{pmatrix} = (1\ 10\ 6)(2\ 5)(3\ 4\ 7)(8\ 9)$$

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 1 & 5 & 3 & 7 & 2 & 9 & 8 & 10 \end{pmatrix}$$

$$\sigma_1 \cdot \sigma_2 \cdot \sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 1 & 5 & 3 & 7 & 2 & 9 & 8 & 10 \\ 2 & 3 & 7 & 4 & 10 & 5 & 1 & 9 & 8 & 6 \\ 7 & 5 & 6 & 1 & 10 & 4 & 3 & 8 & 9 & 2 \end{pmatrix} = (1\ 7\ 3\ 6\ 4)(2\ 5\ 10)(8)(9)$$

Zadanie 7.
Na ile sposobów można pokolorować wierzchołki kwadratu dwoma kolorami, jeśli utożsamiamy kolorowania przez obrót kwadratem.

Rozwiązanie:
Wiemy, że liczba różnych kolorowań to liczba orbit, czyli średnia liczba punktów stałych elementów grupy (u nas obrotów). Mamy cztery elementy: identyczność, obrót o 90°, obrót o 180° oraz obrót o 270°, zatem nasza grupa to $\{id, o_{90^\circ}, o_{270^\circ}\}$. Identyczność ma 4 cykle jedno-elementowe, obrót o 90° oraz obrót o 270° mają jeden cykl cztero-elementowy, zaś obrót o 180° ma dwa cykle dwuelementowe. Stąd jako, że mamy dwa kolory, to liczba punktów stałych wynosi $2^4 + 2 \cdot 2^1 + 2^2 = 24$. Stąd liczba różnych kolorowań to $\frac{24}{4} = 6$.

Zadanie 8.
Ile jest różnych kolorowań wierzchołków sześcianu trzema kolorami, jeśli utożsamiamy kolorowania przez obrót sześcianem.

Rozwiązanie:
Wiemy, że liczba różnych kolorowań to liczba orbit, czyli średnia liczba punktów stałych elementów grupy (u nas obrotów). Mamy identyczność (osiem cykli długości 1), obrót przez środki ścian (są ich trzy) o 90° (dwa cykle długości 4), 180° (cztery cykle długości 2) i 270° (dwa cykle długości 4), obrót wokół przekątnej sześcianu (są ich cztery) $120°, 240°$ (oba to dwa cykle długości 1 i dwa cykle długości 3) oraz obrót wokół środków krawędzi przeciwległych (są ich sześć) o 180° (cztery cykle długości 2). Liczba punktów stałych wynosi więc

$$3^8 + 3(\cdot 3^2 + 3^4 + 3^2) + 4 \cdot (3^2 \cdot 3^2 + 3^2 \cdot 3^2) + 6 \cdot 3^4) = 7992$$

Stąd liczba różnych kolorowań to $\frac{7992}{24} = 333$.

Zadanie 9.
Na ile różnych sposobów można pokolorować wierzchołki kwadratu, jeśli utożsamiamy kolorowanie przez obrót kwadratu w $\mathbb{R}^3$.

Rozwiązanie:

Zadanie 10.
Kolorujemy wierzchołki czworościanu foremnego trzema różnymi kolorami, a krawędzie dwoma

różnymi kolorami. Oblicz, na ile istotnie różnych sposobów można to zrobić, jeśli utożsamiamy takie kolorowania, że jedno przechodzi na drugie przy pewnym obrocie czworościanu w $\mathbb{R}^3$.

Rozwiązanie:
Grupa obrotów czworościanu foremnego zawiera 12 elementów: identyczność, 2 obroty (w prawo i w lewo) wzdłuż osi przechodzącej przez wybrany wierzchołek i środek podstawy (razem $2 \cdot 4$), oraz 1 obrót wzdłuż osi przechodzącej przez środki przeciwległych krawędzi ($1 \cdot 3$). (Dokładne rodzaje obrotów można zobaczyć w źródłach). Dla każdego obrotu chcemy policzyć liczbę punktów stałych, czyli takich kolorowań wierzchołków i krawędzi, które po obrocie pozostają niezmienione (na przykład krawędź a, która po obrocie przechodzi na miejsce krawędzi b, powinna mieć ten sam kolor jak krawędź b). Dzięki temu, wykorzystując Lemat Burnside'a, będziemy mogli znaleźć liczbę orbit, czyli odpowiedzieć, ile jest unikalnych kolorowań. Każdy czworościan powstały w wyniku obrotu możemy traktować jako pewną permutację $(1, 2, 3, 4) \times (1, 2, 3, 4, 5, 6)$ (pierwsza permutacja określa permutację wierzchołków, druga permutację krawędzi). Obrotowi przyporządkowany jest także rozkład na cykle. Możemy zauważyć, że jeśli mamy cykl, to aby kolorowanie pozostało niezmienione po obrocie, wszystkie elementy tego cyklu muszą mieć ten sam kolor (podobnie jak przykład z dwiema krawędziami). Weźmy na przykład obrót przez oś symetrii przechodzącą przez jeden z wierzchołków (konkretnie obrót o 60 stopni w prawo z osią przechodzącą przez wierzchołek D). W przypadku kolorowania wierzchołków, permutacja składa się z cykli [A,C,B][D]. Oznacza to, że dla tego obrotu mamy 32 punkty stałe - na 3 sposoby dobieramy kolory dla pierwszego cyklu i to samo dla drugiego. Jeśli chodzi o krawędzie, obrotowi odpowiada dwie 3-elementowe cykle - krawędzie wychodzące z wierzchołka D oraz te tworzące trójkąt ABC, co daje nam 22 punkty stałe dla kolorowania krawędziami. W ten sposób liczba punktów stałych kolorowania wierzchołków i krawędzi jest taka sama jak liczba par (unikalne kolorowanie wierzchołków, unikalne kolorowanie krawędzi), czyli 3222.
Ustaliliśmy liczbę punktów stałych dla obrotu wokół osi przechodzącej przez wybrany wierzchołek. Pozostało jeszcze uwzględnić obroty: identyczność (tu liczba cykli dla wierzchołków i krawędzi jest taka sama jak liczba elementów, czyli 4) oraz obroty wokół osi przechodzącej przez środki przeciwnych krawędzi (tu cykle mają odpowiednio 2 i 4 elementy, ze względu na to, że krawędzie same na siebie przechodzą), dając nam kolejno 3426 i 3224 punkty stałe.
Teraz możemy skorzystać z Lematu Burnside'a, by znaleźć liczbę orbit. Wzór dla naszego problemu to:

$$\frac{1}{12}\left(3 \cdot 4 \cdot 2^6 + 8 \cdot 3 \cdot 2^4 + 3 \cdot 3 \cdot 2^4\right) = 492$$

co oznacza, że istnieje 492 unikalne sposoby kolorowania, uwzględniając warunki obrotu.