

25 II 2023

Informacje dla zdających:

1. Egzamin trwa 90 minut. Nikt nie wychodzi w ciągu ostatnich 10 minut.
 2. Podczas egzaminu wolno korzystać jedynie z kalkulatora, narzędzi do pisania i materiałów otrzymanych od prowadzących egzamin. Wszelkie przedmioty poza wspomnianymi powinny być pozostawione w torbach/plecakach we wskazanym przez egzaminujących miejscu. W szczególności nie wolno mieć przy sobie własnych kartek i żadnych narzędzi umożliwiających kontakt ze światem zewnętrznym.
 3. Wszystkie kartki z rozwiązaniami należy podpisać imieniem i nazwiskiem oraz numerem indeksu.
 4. Definicje i twierdzenia w zadaniu 5 nie muszą być zapisywane formalnie, mogą być podane własnymi słowami.
-

Zadania:

1. (400 punktów) 127 studentów o numerach indeksów od 11230 do 11356 zdawało egzamin z matematyki dyskretnej. Możliwe oceny z tego egzaminu to 2.0, 3.0, 3.5, 4.0, 4.5, 5.0.

a) Wykładowca przygotował dodatkowe pytanie z teorii liczb dla osób o numerach indeksów podzielnych przez 4, z kombinatoryki dla osób o numerach indeksów podzielnych przez 5 i z teorii grafów dla osób o numerach indeksów podzielnych przez 6. Ile osób otrzymało co najmniej jedno dodatkowe pytanie?

b) Zakładając, że co najmniej 3 studentów otrzymało każdą z ocen pozytywnych, a co najmniej 5 studentów otrzymało ocenę 2.0, ile jest możliwych układów ocen z egzaminu, jeśli interesuje nas tylko liczba ocen 2.0, liczba ocen 3.0 itd., a nie, który student jaką ocenę otrzymał?

c) Załóżmy, że 15 studentów otrzymało ocenę 5.0, 20 - ocenę 4.5, 22 - ocenę 4.0, 25 - ocenę 3.5, 30 - ocenę 3.0, a pozostali - ocenę 2.0. Na ile sposobów można przyporządkować te oceny studentom?

d) Żeby dopytać osoby, które były „na pograniczu ocen” wykładowca przygotował pulę pytań: 14 z rekurencji, 20 z kombinatoryki, 26 z teorii liczb i 33 z teorii grafów. Każdy dopytywany student losował najpierw 4 różne pytania z teorii grafów, które musiał rozwiązać po kolei (czyli kolejność ich wylosowania była istotna), a następnie 14 różnych pytań z pozostałych działów matematyki dyskretnej, które mógł rozwiązywać w dowolnej kolejności (a więc kolejność losowania nie ma znaczenia), przy czym musiał wylosować dokładnie 6 pytań z kombinatoryki i co najwyżej 3 pytania z rekurencji. Ile istnieje różnych możliwych układów pytań wylosowanych przez dopytywanego studenta?

2. (400 pkt) Rozwiązać następujące zagadnienie rekurencyjne:

$$s_{n+1} = 13s_n - 40s_{n-1} + 30 \cdot 5^n; s_0 = 3, s_1 = -5.$$

3. a) (200 pkt) Dla klucza publicznego (77, 19) w systemie RSA wyznaczyć klucz prywatny, a następnie obliczyć, jaka jednostka tekstu jawnego zostanie odszyfrowana z jednostki szyfrogramu o numerze 5.

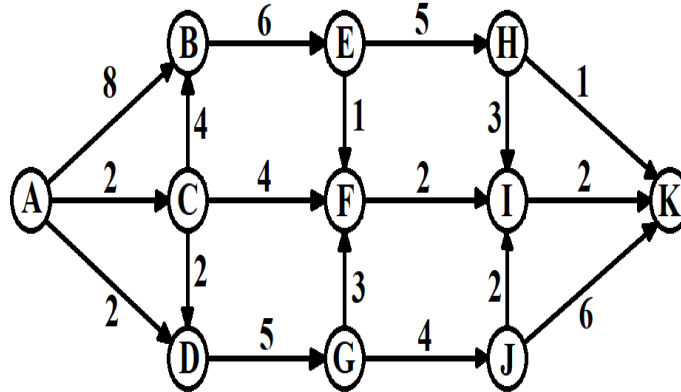
b) (100 pkt) Za pomocą twierdzenia Eulera obliczyć $37^{73849} \pmod{50}$.

c) (100 pkt) Obliczyć $\varphi(8208)$.

4. (400 punktów)

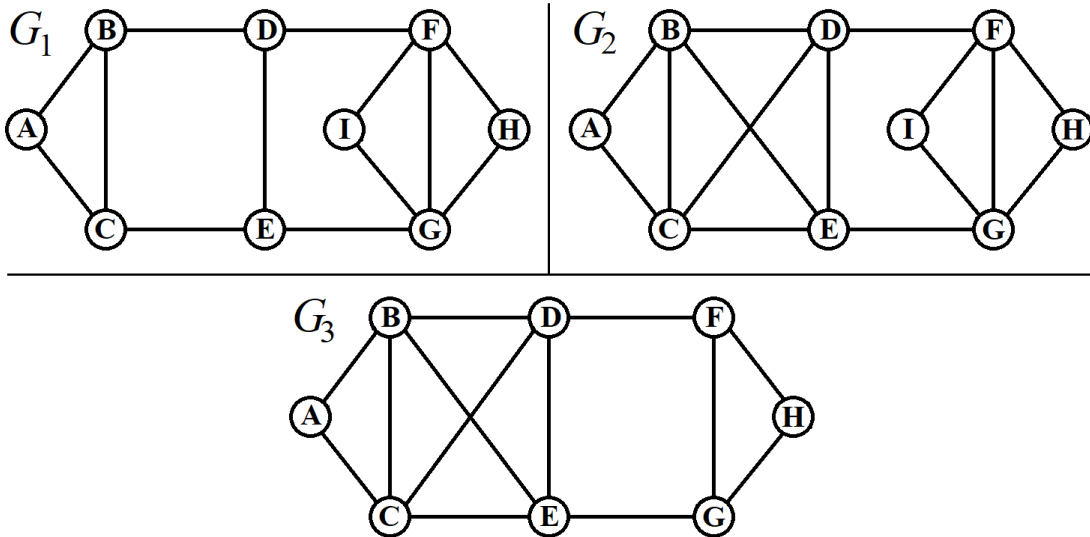
- a) Za pomocą algorytmu Edmondsa-Karpa znaleźć maksymalny przepływ pomiędzy wierzchołkami A oraz K w poniższym grafie skierowanym. Uzupełnić odpowiednią tabelę przebiegu algorytmu i narysować graf z oznaczonym maksymalnym przepływem.

Nr etapu	Ścieżka powiększająca	Przepustowość	Alternatywy
----------	-----------------------	---------------	-------------



- b) Dla każdego z grafów G_1, G_2, G_3 sprawdzić, czy występuje w nim cykl lub droga Eulera. Odpowiedź uzasadnić powołując się na odpowiednie twierdzenie. Jeśli dla któregoś z grafów będzie istnieć droga Eulera, ale nie cykl Eulera, wykorzystać algorytm Fleury'ego do znalezienia jednej z tych dróg zapisując przebieg algorytmu w tabeli o nagłówkach jak poniżej. Zapisać odpowiedź w postaci ciągu kolejnych wierzchołków na tej drodze.

Nr etapu	Wybrany wierzchołek	Alternatywy
----------	---------------------	-------------



5. (400 punktów) a) Wyjaśnić, z czego się składa definicja rekurencyjna i podać przykład takiej definicji.

b) Podać wypowiedź twierdzenia Vizinga, definiując wszystkie oznaczenia, które w nim się pojawiają (tj. wyjaśniając wszystkie definicje, które są konieczne do jego zrozumienia).