

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2014/2015

Wydział Fizyki, Matematyki i Informatyki

Kierunek studiów: Matematyka

Profil: Ogólnoakademicki

Forma studiów: stacjonarne

Kod kierunku: M

Stopień studiów: I

Specjalności: Matematyka w finansach i ekonomii

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Matematyka dyskretna
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	
KOD PRZEDMIOTU	WFMiI M oIS B10 14/15
KATEGORIA PRZEDMIOTU	Przedmioty podstawowe
LICZBA PUNKTÓW ECTS	6.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
3	30	30	0	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Zapoznanie studenta z podstawowymi pojęciami i metodami matematyki dyskretniej.

Cel 2 Umiejętność rozpoznania wśród problemów praktycznych takich, do których można zastosować metody matematyki dyskretniej. Rozwiązywanie niektórych takich problemów.

Cel 3 Rozwijanie umiejętności komunikacji.

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

- 1 Zaliczony przedmiot Wstęp do logiki i teorii mnogości.
- 2 Dobra znajomość metody indukcji matematycznej.
- 3 Znajomość algebry w zakresie podstaw teorii grup i podstaw teorii pierścieni.

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student zna podstawowe definicje i twierdzenia przedstawione na wykładach.

EK2 Wiedza Student umie wypowiedzieć algorytm RSA i uzasadnić jego poprawność na gruncie poznanych twierdzeń z teorii liczb.

EK3 Umiejętności Student umie stosować pozostałe poznane algorytmy: algorytm Euklidesa, algorytmy grafowe, algorytmy szyfrujące: El Gammala, Diffiego-Hellmana, DES.

EK4 Umiejętności Student umie komunikować swoją wiedzę, przedstawić klarownie i ścisłe rozumowania matematyczne, zarówno w formie pisemnej jak i ustnej. Umie jasno sformułować pytanie.

EK5 Kompetencje społeczne Student rozumie potrzebę tłumaczenia matematyki laikom. Odpowiedzialnie traktuje swoje wypowiedzi: odróżnia przypuszczenia od faktów potwierdzonych. Szanuje sądy innych i odnosi się do nich merytorycznie. Jest etyczny: szanuje cudzą własność intelektualną.

6 TREŚCI PROGRAMOWE

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Aksjomaty liczb całkowitych. Podstawy arytmetyki w Z. Podzielność. NWD i NWW. Algorytm Euklidesa. Reprezentacja liczb całkowitych w systemach o różnych podstawach. Liczby pierwsze. Twierdzenie, że liczb pierwszych jest nieskończenie wiele. Sito Eratostenesa. Twierdzenie aproksymujące rozmieszczenie liczb pierwszych, bez dowodu.	2
W2	Przystawanie liczb modulo n jako relacja kongruencji. Struktura ilorazowa. Chińskie twierdzenie o resztach. Rozwiązywanie równań i układów równań kongruencyjnych. Małe twierdzenie Fermata. Informacja o wielkim twierdzeniu Fermata.	2
W3	Kryptografia: Klasyfikacja algorytmów szyfrujących, odp. cyfrowy. Algorytm RSA, El Gammala, Diffiego-Hellmana, DES. Szyfry strumieniowe.	10
W4	Kwadraty Łacińskie i design.	2
W5	Zasady zliczania: wzór włącz-wyłącz, zasada iloczynu, zasada szufladkowa Dirichleta. Wariacje, permutacje, kombinacje, kombinacje z powtórzeniami, permutacje z powtórzeniami. Ilość sposobów rozmieszczenia w k pudełkach n przedmiotów (rozdzielalnych lub nie).	4

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W6	Pojęcie grafu, grafy nieskierowane i skierowane. Podstawowe własności grafów (spójność, reprezentacja). Problem poruszania się po krawędziach grafu (cykl Eulera, cykl Hamiltona, drogi minimalne i maksymalne w digrafach z wagami, algorytm Dijkstry i algorytm Bellmana. Drzewa i lasy (problem minimalnego drzewa spinającego- algorytmy Prima i Kruskala), podstawowe zagadnienia związane z kolorowaniem grafów.	10

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Stosowanie zasady minimum i zasady indukcji. Ciągi definiowane indukcyjnie. Ciąg Fibonacciego.	2
C2	Dowodzenie prostych faktów arytmetycznych. Algorytm Euklidesa i jego zastosowania. Reprezentacja liczb całkowitych w systemach o różnych podstawach.	4
C3	Przystawanie modulo n , struktury Z_n , równania kongruencyjne. Zastosowania. Układy równań kongruencyjnych. Zastosowania małego twierdzenia Fermata.	4
C4	Stosowanie algorytmów szyfrujących.	6
C5	Kombinatoryka i zliczanie obiektów kombinatorycznych.	4
C6	Ilustracja podstawowych pojęć z teorii grafów. Informacje uzyskiwane z macierzy grafu i jej potęg. Zagadnienia praktyczne modelowane przy pomocy grafów.	2
C7	Rozpoznawanie grafów Eulerowskich i Hamiltonowskich. Stosowanie algorytmów grafowych.	8

7 NARZĘDZIA DYDAKTYCZNE

N1 Dyskusja

N2 Konsultacje

N3 Wykłady

N4 Zadania tablicowe

N5 Praca w grupach

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	60
Konsultacje przedmiotowe	8
Egzaminy i zaliczenia w sesji	7
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	75
Opracowanie wyników	20
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	180
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	6.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Ćwiczenie praktyczne

F2 Kolokwium

F3 Odpowiedź ustna

F4 Zadanie tablicowe

OCENA PODSUMOWUJĄCA

P1 Średnia ważona ocen formujących

P2 Egzamin pisemny

P3 Egzamin ustny

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Aby zaliczyć przedmiot, należy uzyskać pozytywną ocenę z każdego efektu kształcenia.

W2 Wszystkie oceny podsumowujące muszą być pozytywne.

W3 W niektórych przypadkach prowadzący przedmiot zwalnia studenta z egzaminu pisemnego..

W4 Ocena końcowa jest średnią z trzech ocen podsumowujących. W przypadku wyniku pośredniego, zaokrąglany jest on w kierunku oceny P1.

OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA**B1** Ćwiczenie praktyczne**B2** Test**KRYTERIA OCENY**

EFEKT KSZTAŁCENIA 1	
NA OCENĘ 2.0	Student nie spełnia kryteriów na ocenę dostateczną
NA OCENĘ 3.0	Student zna wszystkie spośród definicji następujących pojęć: liczba pierwsza, graf nieskierowany, macierz grafu, trasa, ścieżka, droga, cykl, podzielność, NWD, NWW, przystawanie modulo n , ciąg Fibonacciego. Student umie wypowiedzieć poprawnie każde z następujących twierdzeń: zasada indukcji, zasada minimum, algorytm dzielenia, wzór włącz-wyłącz, zasadę Dirichleta, twierdzenia dotyczące zliczania permutacji i wariacji. Ponadto student potrafi wypowiedzieć niektóre inne definicje i twierdzenia, być może z niewielkimi usterkami. Potrafi przedstawić dowody niektórych nietrudnych twierdzeń.
NA OCENĘ 3.5	Student spełnia wymagania na ocenę dostateczną, przy czym lista definicji i twierdzeń obowiązkowych jest rozszerzona o następujące: reprezentacja liczb naturalnych w systemach o różnych podstawach, lemat uzasadniający poprawność sita Eratostenesa, twierdzenie, że liczb pierwszych jest nieskończenie wiele, małe twierdzenie Fermata, chińskie twierdzenie o resztach, struktura ilorazowa liczb całkowitych przy dzieleniu przez przystawanie modulo n . Student nie myli twierdzenia z twierdzeniem odwrotnym ani tezy z założeniami. W swoich argumentacjach klarownie odróżnia to, co wiadomo, od tego co należy dowieść. Potrafi przedstawić poprawnie dowody większości nietrudnych twierdzeń.
NA OCENĘ 4.0	Student spełnia kryteria na ocenę 3.5, przy czym lista pojęć i twierdzeń obowiązkowych rozszerza się o: równoważność zasady indukcji i zasady minimum, Poprawność niektórych algorytmów. Student umie przedstawić dowody większości poznanych twierdzeń, być może z niewielkimi usterkami.
NA OCENĘ 4.5	Student zna prawie wszystkie pojęcia podane na wykładzie i umie zilustrować je przykładami i kontrprzykładami. Student poprawnie wypowiada wszystkie twierdzenia. Potrafi przedstawić dowody prawie wszystkich poznanych twierdzeń. W przypadku zauważenia usterki, sam potrafi ją skorygować.
NA OCENĘ 5.0	Student zna wszystkie definicje i twierdzenia podane na wykładzie. Wypowiada je bezbłędnie, ilustrując przykładami. Zna dowody wszystkich twierdzeń z kursu. Jego wypowiedzi są płynne, precyzyjne i jasne.
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie spełnia kryteriów na ocenę dostateczną
NA OCENĘ 3.0	Student umie wyjaśnić różnicę między tradycyjnym kodowaniem z użyciem klucza tajnego, a kodowaniem z kluczem publicznym. Wie, do której kategorii zalicza się metoda RSA. Umie przedstawić kolejne etapy kodowania przy użyciu tej metody, być może z niewielkimi usterkami.

NA OCENĘ 3.5	Student umie zdefiniować kodowanie i rozkodowanie jako funkcje o specjalnych własnościach; umie podać ich dziedziny. Umie przedstawić w pełni poprawnie kolejne kroki algorytmu RSA; wskazując, które z używanych danych są jawne. Na tej podstawie umie wyjaśnić zdanie, że RSA dostarcza metody kodowanie z kluczem publicznym.
NA OCENĘ 4.0	Student spełnia kryteria na ocenę 3.5 i ponadto potrafi poprawnie podać procedurę odkodowującą wiadomość. Pobieźnie uzasadnia jej poprawność, wskazując zastosowanie małego twierdzenia Fermata lub twierdzenia o resztach. Wypowiedź może zawierać niewielkie usterki.
NA OCENĘ 4.5	Student spełnia kryteria na ocenę 4. Potrafi poprawnie uzasadnić wykonalność i poprawność procedury kodowania i odkodowania powołując się na twierdzenia z teorii liczb. Wypowiedź może zawierać drobne usterki, ale gdy zostają one wskazane, student umie je skorygować.
NA OCENĘ 5.0	Student płynnie i bezusterkowo formułuje wypowiedź algorytmu i procedury odwrotnej, uzasadnia ich wykonalność i poprawność. Powołuje się poprawnie na twierdzenia z teorii liczb. Wskazuje elementy jawne i tajne procedury. Wyjaśnia na czym polega "publiczność" klucza w kodowaniu RSA.
EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie spełnia kryteriów na ocenę dostateczną.
NA OCENĘ 3.0	Student umie stosować przynajmniej następujące poznane algorytmy: sito Eratostenesa, schemat rozwiązywania równań i układów równań kongruencyjnych w oparciu o chińskie twierdzenie o resztach, test pierwszości oparty o małe twierdzenie Fermata, algorytmy teorio-grafowe. W wielu wypadkach poprawnie rozpoznaje praktyczne problemy, w których mają one zastosowanie. Ma pojęcie o algorytmach: El Gammala, DES i Diffiego-Hellmana.
NA OCENĘ 3.5	Student spełnia kryteria na ocenę 3 oraz w większości wypadków potrafi wskazać twierdzenia, na których opiera się poprawność tych algorytmów.
NA OCENĘ 4.0	Student spełnia kryteria na ocenę 3.5, potrafi stosować algorytmy szyfrujące wymienione na ocenę 3.0, potrafi wykazać poprawność niektórych algorytmów.
NA OCENĘ 4.5	Student umie stosować wszystkie poznane algorytmy, umie udowodnić poprawność większości z nich i poprawnie rozpoznaje praktyczne problemy, w których mają one zastosowanie.
NA OCENĘ 5.0	Student umie stosować wszystkie poznane algorytmy, umie udowodnić ich poprawność i poprawnie rozpoznaje praktyczne problemy, w których mają one zastosowanie.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie spełnia kryteriów na ocenę dostateczną.
NA OCENĘ 3.0	Student potrafi poprawnie wypowiedzieć większość definicji i niektóre twierdzenia, być może odwołując się do intuicji. Po zwróceniu uwagi, potrafi doprecyzować swoją wypowiedź.

NA OCENĘ 3.5	Student potrafi poprawnie wypowiedzieć prawie wszystkie definicje i większość twierdzeń, a niektóre z nich udowodnić. Po zwróceniu uwagi, potrafi doprecyzować swoją wypowiedź. W rozwiązaniach zadań poprawnie odwołuje się do znanych twierdzeń. Odróżnia hipotezę od udowodnionego faktu. Nie myli twierdzenia z twierdzeniem odwrotnym.
NA OCENĘ 4.0	Student spełnia kryteria na ocenę 3.5. Jasno formułuje pytania. Zna granice swojej wiedzy: nie podaje hipotez za fakty. Jego rozumowania są jasne, poprawne, być może z pewnymi usterkami.
NA OCENĘ 4.5	Student spełnia kryteria na ocenę 4. Przedstawiane przez niego rozumowania są ścisłe, klarowne i na ogół bezusterkowe.
NA OCENĘ 5.0	Student spełnia wymagania na ocenę 4.5. Umie komunikować swoją wiedzę płynnie, jasno i ciekawie. Przedstawiane rozumowania są poprawne. Gdy zostanie zapytany, student potrafi wytłumaczyć wszystkie szczegóły. Potrafi zastosować poznane sposoby rozumowania do innych sytuacji.
EFEKT KSZTAŁCENIA 5	
NA OCENĘ 2.0	Student nie spełnia kryteriów na ocenę dostateczną.
NA OCENĘ 3.0	Student rozumie potrzebę tłumaczenia matematyki laikom i potrafi przystępnie wytłumaczyć niektóre pojęcia matematyki dyskretnej. Szanuje cudzą własność intelektualną.
NA OCENĘ 3.5	Student rozumie potrzebę tłumaczenia matematyki laikom i potrafi przystępnie wytłumaczyć niektóre pojęcia matematyki dyskretnej. Zna praktyczne zastosowania niektórych zagadnień. Szanuje cudzą własność intelektualną.
NA OCENĘ 4.0	Student rozumie potrzebę tłumaczenia matematyki laikom i potrafi przystępnie wytłumaczyć wiele pojęć i faktów z matematyki dyskretnej. Zna praktyczne zastosowania większości zagadnień. Bierze udział w dyskusji, starając się jasno przekazać własne propozycje rozwiązań. Szanuje innych uczestników dyskusji. Szanuje cudzą własność intelektualną.
NA OCENĘ 4.5	Student rozumie potrzebę tłumaczenia matematyki laikom i potrafi przystępnie wytłumaczyć większość pojęć i faktów z matematyki dyskretnej oraz wagę ich precyzyjnego sformułowania. Zna praktyczne zastosowania prawie wszystkich omawianych zagadnień. Bierze udział w dyskusji, starając się jasno przekazać własne propozycje rozwiązań. Szanuje innych uczestników dyskusji. Szanuje cudzą własność intelektualną.
NA OCENĘ 5.0	Student rozumie potrzebę tłumaczenia matematyki laikom i potrafi przystępnie wytłumaczyć pojęcia, fakty i metody matematyki dyskretnej. Potrafi wytłumaczyć znaczenie precyzyjnego sformułowania pojęć i zagadnień dla praktycznych zastosowań matematyki dyskretnej. Chętnie bierze udział w dyskusji, szanując innych jej uczestników. Często proponuje trafne rozwiązania omawianych problemów i stara się je przedstawić jasno i precyzyjnie. Szanuje cudzą własność intelektualną.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1		Cel 1	W1 W2 W3 W4 W6 C1 C2 C3 C5 C6	N1 N2 N3 N4	F1 F2 F3 F4 P1 P2 P3
EK2		Cel 1 Cel 2 Cel 3	W1 W2 W3 C4	N1 N2 N3 N4 N5	F1 F2 F3 F4 P1 P2 P3
EK3		Cel 2	W2 W3 W6 C2 C4 C5 C7	N1 N2 N3 N4 N5	F1 F2 F3 F4 P1 P2 P3
EK4		Cel 3	W1 W2 W3 W4 W5 W6 C1 C2 C3 C4 C5 C6 C7	N1 N2 N3 N4	F2 F3 F4 P1 P2 P3
EK5		Cel 3	W1 W2 W3 W4 W5 W6 C1 C2 C3 C4 C5 C6 C7	N1 N2 N3 N4	F1 F2 F3 F4 P1 P2 P3

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

[1 | Kenneth A. Ross, Charles R.B. Wright — *Matematyka dyskretna*, Warszawa, 2002, PWN

LITERATURA UZUPEŁNIAJĄCA

[1 | R.Wilson — *Wprowadzenie do teorii grafów*, Warszawa, 1999, PWN

[2 | M. Goodaire, M. Parementer — *Discrete Mathematics with Graph Theory*, New York, 2000, Prentice Hall

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr Grzegorz Gancarzewicz (kontakt: gancarz@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

1 dr Grzegorz Gancarzewicz (kontakt: ggancarzewicz@gmail.com)

2 dr Katarzyna Pałasińska (kontakt: kpalasin@pk.edu.pl)

3 dr Szymon Pliś (kontakt: splis@pk.edu.pl)



13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....
.....
.....