

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2022/2023

Wydział Informatyki i Telekomunikacji

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	Teoria liczb
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Number theory
KOD PRZEDMIOTU	WiT M oIS C17 22/23
KATEGORIA PRZEDMIOTU	Przedmioty kierunkowe
LICZBA PUNKTÓW ECTS	5.00
SEMESTRY	5

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
5	30	20	0	0	0	10

3 CELE PRZEDMIOTU

Cel 1 Zapoznanie z podstawami arytmetyki, arytmetyki modularnej i teorii liczb.

Cel 2 Przygotowanie do rozwiązywania problemów kryptograficznych.

Cel 3 Podniesienie umiejętności myślenia matematycznego i analitycznego.

4 WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1 Podstawy analizy matematycznej i teorii mnogości.

5 EFEKTY KSZTAŁCENIA

EK1 Wiedza Student zna i rozumie podstawowe pojęcia z algebry abstrakcyjnej i elementarnej teorii liczb.

EK2 Wiedza Student zna podstawowe protokoły kryptograficzne i twierdzenia teorio-liczbowe na których się opierają.

EK3 Umiejętności Student potrafi rozwiązać podstawowe zadania, wyszukać informacje w literaturze, sformułować opinie na temat podstawowych pojęć algebry, teorii liczb i ich zastosowań.

EK4 Kompetencje społeczne Student regularnie uczestniczy w zajęciach. Student korzysta z materiałów uzupełniających i dodatkowych umieszczonych na platformie e-learningowej. Student widzi zastosowania i rozumie potrzebę teorii liczb w społeczeństwie informatycznym.

6 TREŚCI PROGRAMOWE

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W1	Podstawy teoriomnościowe i arytmetyczne. Indukcja matematyczna i zasada minimum.	2
W2	Funkcje: typy, rodzaje własności; relacje: definicja, rodzaje, własności przykłady.	1
W3	Elementy teorii grup: grupa, podgrupa, podgrupa normalna, homomorfizmy grup, grupa ilorazowa, grupy cykliczne, suma prosta. Podstawowe struktury algebraiczne: pierścienie, ciała, przykłady.	3
W4	Arytmetyka liczb całkowitych: podzielność, dzielenie z resztą, algorytm Euklidesa, wsteczny algorytm Euklidesa, proste liniowe równania diofantyczne, największy wspólny dzielnik, najmniejsza wspólna wielokrotność.	4
W5	Kongruencje liniowe, układy kongruencji liniowych. Chińskie twierdzenie o resztach.	2
W6	Liczby pierwsze, własności, sito Eratostenesa, twierdzenia o rozmieszczeniu liczb pierwszych, zastosowanie liczb pierwszych. Liczby pierwsze Sophie Germain. Liczby pierwsze ich rozmieszczenie w postępach arytmetycznych. Twierdzenia: Dirichleta, Siegela-Walfisza oraz Bombieriego-Vinogradova o liczbach pierwszych w postępach arytmetycznych.	3
W7	Zasadnicze twierdzenie arytmetyki, rozkład kanoniczny. Systemy liczbowe.	2
W8	Arytmetyka modularna: relacja przystawania modulo n . Pierścienie $\mathbb{Z}_n$. Twierdzenia Eulera i Fermata. Liczby pseudopierwsze. Liczby Carmichaela. Testy pierwszości. Rząd elementu modulo n . Logarytmy dyskretne, podstawowe własności, algorytmy Shanksa, Pohliga-Hellmana.	3

WYKŁAD		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
W9	Reszty i niereszty kwadratowe.	2
W10	Funkcje arytmetyczne, funkcje multiplikatywne, splot Dirichleta. Sumy funkcji arytmetycznych.	1
W11	Ułamki łańcuchowe i ich zastosowania (przybliżanie liczb niewymiernych, teoria węzłów), równania diofantyczne.	3
W12	Kryptografia, symetryczna i asymetryczna, RSA, podpis cyfrowy, protokół Diffiego-Hellmana, algorytm ElGamala.	4

ĆWICZENIA		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
C1	Zadania z podstaw teorii mnogościowych i arytmetycznych. Zadania na dowodzenie przy pomocy indukcji matematycznej i zasady minimum.	1
C2	Zadania z teorii grup, pogłębienie rozumienia struktur algebraicznych.	1
C3	Wykorzystanie algorytmu Euklidesa, wstecznego algorytmu Euklidesa. Rozwiązywanie prostych liniowych równań diofantycznych.	2
C4	Różne systemy liczbowe.	1
C5	Zadania o liczbach pierwszych.	1
C6	Kongruencje i ich zastosowania. Twierdzenia Eulera i Fermata. Obliczanie logarytmu dyskretnego, podstawowe własności.	2
C7	Kongruencje liniowe, układy kongruencji liniowych i ich rozwiązywanie. Chińskie twierdzenie o resztach zastosowanie.	2
C8	Reszty i niereszty kwadratowe, zadania	2
C9	Funkcje arytmetyczne i multiplikatywne własności.	2
C10	Ułamki łańcuchowe zadania. Teoria splotów wymiernych jako praktyczne zastosowanie.	2
C11	Kryptografia, symetryczna i asymetryczna, RSA, podpis cyfrowy, protokół Diffiego-Hellmana, algorytm ElGamala, zadania.	4

PROJEKT		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
P1	Twierdzenia o rozmieszczeniu liczb pierwszych. Twierdzenie Bertranda-Czebyszewa. Liczby pierwsze ich rozmieszczenie w postępach arytmetycznych. Twierdzenia: Dirichleta, Siegela-Walfisza oraz Bombieriego-Vinogradova o liczbach pierwszych w postępach arytmetycznych, wnioski z tych twierdzeń. Liczby pierwsze a Hipoteza Riemana.	4
P2	Funkcje arytmetyczne i funkcje multiplikatywne, splot Dirichleta. Sumy funkcji arytmetycznych i ich asymptotyka.	3
P3	Kryptografia symetryczna przykłady. Kryptografia asymetryczna, RSA, podpis cyfrowy, protokół Diffiego-Hellmana, algorytm ElGamala.	3

7 NARZĘDZIA DYDAKTYCZNE

N1 Zadania tablicowe

N2 Praca w grupach

N3 Prezentacje multimedialne

N4 Dyskusja

N5 Konsultacje

N6 E-Learning (platforma Moodle), w przypadku potrzeby zajęć zdalnych MS-TEAMS

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	15
Egzaminy i zaliczenia w sesji	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	30
Opracowanie wyników	30
Przygotowanie raportu, projektu, prezentacji, dyskusji	15
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	150
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	5.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Kolokwium 1

F2 Kolokwium 2

F3 Kolokwium 3 kryptografia

F4 Aktywność na ćwiczeniach i praca na platformie e-learningowej

OCENA PODSUMOWUJĄCA

P1 Średnia ważona ocen z kolokwiów, zadań domowych, aktywności.

WARUNKI ZALICZENIA PRZEDMIOTU

W1 50% możliwych do zdobycia punktów.

OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

B1 Zadania domowe, testy na e-kursie

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1

NA OCENĘ 2.0	Student nie wykazał wiedzy, o której mowa w kryterium na ocenę 3.
NA OCENĘ 3.0	Student umie wykorzystać w dostatecznym stopniu poznane wzory i twierdzenia do rozwiązywania wskazanych zadań obejmujących tematykę przedmiotu i uzyskał przy tym więcej niż połowę maksymalnej sumarycznej liczby punktów.
NA OCENĘ 3.5	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 3. Student rozumie w ponad dostatecznym stopniu poznane wzory i twierdzenia, co jest wyrażone przez to, że uzyskał więcej niż 60% maksymalnej sumarycznej liczby punktów.
NA OCENĘ 4.0	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 3.5. Student rozumie w dobrym stopniu poznane wzory i twierdzenia, co jest wyrażone przez to, że uzyskał więcej niż 70% maksymalnej sumarycznej liczby punktów.
NA OCENĘ 4.5	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 4. Student rozumie w ponad dobrym stopniu poznane wzory i twierdzenia ponadto rozumie zależności między poznanymi faktami, co jest wyrażone przez to, że uzyskał więcej niż 80% maksymalnej sumarycznej liczby punktów.
NA OCENĘ 5.0	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 4.5. Student rozumie w bardzo dobrym stopniu poznane wzory i twierdzenia ponadto potrafi odpowiedzieć na dodatkowe pytania, co jest wyrażone przez to, że uzyskał więcej niż 90% maksymalnej sumarycznej liczby punktów.
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie wykazał wiedzy, o której mowa w kryterium na ocenę 3.
NA OCENĘ 3.0	Student zna w dostatecznym stopniu podstawowe protokoły kryptograficzne i twierdzenia teorio liczbowe na których się opierają, co zostało potwierdzone przez to, że uzyskał więcej niż połowę maksymalnej liczby punktów z kolokwium dotyczącego kryptografii, patrz ocena formująca F3.
NA OCENĘ 3.5	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 3. Student rozumie w ponad dostatecznym stopniu podstawowe protokoły kryptograficzne, co zostało potwierdzone przez to, że uzyskał więcej niż 60% maksymalnej liczby punktów z kolokwium dotyczącego kryptografii, patrz ocena formująca F3.
NA OCENĘ 4.0	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 3.5. Student rozumie w dobrym stopniu podstawowe protokoły kryptograficzne, co zostało potwierdzone przez to, że uzyskał więcej niż 70% maksymalnej liczby punktów z kolokwium dotyczącego kryptografii, patrz ocena formująca F3.
NA OCENĘ 4.5	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 4. Student rozumie w ponad dobrym stopniu podstawowe protokoły kryptograficzne, co zostało potwierdzone przez to, że uzyskał więcej niż 80% maksymalnej liczby punktów z kolokwium dotyczącego kryptografii, patrz ocena formująca F3.
NA OCENĘ 5.0	Student wykazał się wiedzą, o której mowa w kryterium na ocenę 5. Student rozumie w bardzo dobrym stopniu podstawowe protokoły kryptograficzne ponadto potrafi odpowiedzieć na dodatkowe pytania, co zostało potwierdzone przez to, że uzyskał więcej niż 90% maksymalnej liczby punktów z kolokwium dotyczącego kryptografii, patrz ocena formująca F3.

EFEKT KSZTAŁCENIA 3	
NA OCENĘ 2.0	Student nie wykazał umiejętności, o których mowa w kryterium na ocenę 3.
NA OCENĘ 3.0	Student umie wykorzystać poznane wzory i twierdzenia do rozwiązywania wskazanych zadań obejmujących tematykę ćwiczeń i wykładów oraz uzyskał przy tym więcej niż połowę maksymalnej sumarycznej liczby punktów.
NA OCENĘ 3.5	Student umie wykorzystać poznane wzory i twierdzenia do rozwiązywania wskazanych zadań obejmujących tematykę ćwiczeń i wykładów, wykazał się umiejętnością korzystania z literatury oraz uzyskał przy tym więcej niż 60% maksymalnej sumarycznej liczby punktów.
NA OCENĘ 4.0	Student wykazał się umiejętnościami, o których mowa w kryterium na ocenę 3.5. Student umie wykorzystać poznane wzory i twierdzenia do rozwiązywania wskazanych zadań obejmujących tematykę ćwiczeń i wykładów, potrafi formułować wnioski i opinie na temat podstawowych pojęć oraz uzyskał przy tym więcej niż 70% maksymalnej sumarycznej liczby punktów.
NA OCENĘ 4.5	Student wykazał się umiejętnościami, o których mowa w kryterium na ocenę 4. Student umie wykorzystać poznane wzory i twierdzenia do rozwiązywania wskazanych zadań obejmujących tematykę ćwiczeń i wykładów, potrafi podać zastosowania podstawowych pojęć i faktów oraz uzyskał przy tym więcej niż 80% maksymalnej sumarycznej liczby punktów.
NA OCENĘ 5.0	Student wykazał się umiejętnościami, o których mowa w kryterium na ocenę 4,5. Student umie płynnie wykorzystać poznane wzory i twierdzenia do rozwiązywania wskazanych zadań obejmujących tematykę ćwiczeń i wykładów ponadto potrafi rozwiązać zadania o podwyższonym stopniu trudności oraz uzyskał przy tym więcej niż 90% maksymalnej sumarycznej liczby punktów.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie wykazał umiejętności, o których mowa w kryterium na ocenę 3.
NA OCENĘ 3.0	Student rozumie potrzebę regularnej pracy i systematycznie uczęszczał na zajęcia.
NA OCENĘ 4.0	Student wykazał się systematycznością o której mowa w kryterium na ocenę 3. Student mając świadomość ograniczeń własnej wiedzy aktywnie uczestniczy w wykładach i ćwiczeniach, a także systematycznie pracuje na platformie e-learningowej.
NA OCENĘ 5.0	Student spełnia warunki, o których mowa w kryterium na ocenę 4. Ponadto odczuwa potrzebę pogłębienia własnego zrozumienia danego tematu poprzez szukanie zastosowań teorii liczb i kryptografii oraz sięganie po dodatkowe materiały i literaturę.

10 MACIERZ REALIZACJI PRZEDMIOTU

EFEKT KSZTAŁCENIA	ODNIESIENIE DANEGO EFEKTU DO SZCZEGÓŁOWYCH EFEKTÓW ZDEFINIOWANYCH DLA PROGRAMU	CELE PRZEDMIOTU	TREŚCI PROGRAMOWE	NARZĘDZIA DYDAKTYCZNE	SPOSOBY OCENY
EK1	K_W02 K_W04 K_W06	Cel 1 Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 P1 P2 P3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1
EK2	K_W06 K_W08	Cel 3	W8 W9 W10 W11 W12 C8 C9 C10 C11 P3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1
EK3	K_U01 K_U03 K_U16 K_U28	Cel 1 Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1
EK4	K_K03 K_K06	Cel 1 Cel 2 Cel 3	W1 W2 W3 W4 W5 W6 W7 W8 W9 W10 W11 W12 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 P1 P2 P3	N1 N2 N3 N4 N5 N6	F1 F2 F3 F4 P1

11 WYKAZ LITERATURY

LITERATURA PODSTAWOWA

- [1] | Władysław Narkiewicz — *Teoria liczb*, Warszawa, 1977, Biblioteka Matematyczna tom 50, PWN
- [2] | Marek Zakrzewski — *Markowe wykłady z matematyki. Teoria liczb*, Wrocław, 2017, Wydawnictwo GIS
- [3] | Jerzy Rutkowski — *Algebra abstrakcyjna w zadaniach*, Warszawa, 2019, PWN

LITERATURA UZUPEŁNIAJĄCA

- [1] | Wacław Marzantowicz, Piotr Zarzycki — *Elementarna teoria liczb*, Warszawa, 2006, PWN

12 INFORMACJE O NAUCZYCIELACH AKADEMICKICH

OSOBA ODPOWIEDZIALNA ZA KARTĘ

dr Maciej Zakarczemny (kontakt: mzakarczemny@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)