**Nazwa przedmiotu:**

Algorytmiczna teoria liczb

**Koordynator przedmiotu:**

Dr Barbara Roszkowska-Lech

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

1120-MAMNI-NSP-0111

**Semestr nominalny:**

1 / rok ak. 2022/2023

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

1. godziny kontaktowe – 50 h; w tym
 a) obecność na wykładach – 30 h
 b) obecność na ćwiczeniach – 15 h
 c) konsultacje – 5 h
2. praca własna studenta – 45 h; w tym
 a) przygotowanie do ćwiczeń i do testu – 35 h
 b) zapoznanie się z literaturą – 10 h
Razem 95 h, co odpowiada 4 pkt. ECTS

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

a) obecność na wykładach – 30 h
b) obecność na ćwiczeniach – 15 h
c) konsultacje – 5 h
Razem 50 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

.

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 15h |
| Laboratorium:  | 0h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

Przedmioty poprzedzające:
1. Algebra i jej zastosowania I
2. Algebra i jej zastosowania II
3. Algebra liniowa z geometrią
Zalecane: Elementarna teoria liczb (Teoria liczb)
Wymagania wstępne:
1. Znajomość przestrzeni liniowych, ich bazy i wymiaru, przekształceń liniowych, macierzy.
2. Znajomość zagadnień związanych z podstawowymi własnościami pierścienia liczb całkowitych: kongruencje, arytmetyka modularna.

**Limit liczby studentów:**

.

**Cel przedmiotu:**

Główny cel przedmiotu to omówienie metod i algorytmów teorii liczb.

**Treści kształcenia:**

1. Elementy teorii podzielności, NWD, NWW. Algorytm Euklidesa. Obliczenia w pierścieniu Zn
2. Arytmetyka modularna i złożoność działań arytmetycznych. Twierdzenia Eulera i Fermata. Chińskie twierdzenie o resztach. Potęgowanie modularne
3. Złożoność teorio liczbowych algorytmów
4. Wybrane równania diofantyczne i metody ich rozwiazywania (równanie Pella)
5. Pierwiastki pierwotne, logarytmy dyskretne elementy dużego rzędu mod n.
6. Liczby pierwsze i pseudopierwsze. Testy pierwszości. Rozmieszczenie liczb pierwszych
7. Problem faktoryzacji-algorytmy faktoryzacji
8. Logarytm dyskretny i algorytmy obliczania logarytmów dyskretnych
9. Funkcje teorio- liczbowe i ich zachowanie asymptotyczne i metody obliczania
10. Niektóre inne algorytmy teorii liczb (weryfikacja hipotezy Goldbacha, szukanie par liczb zaprzyjaźnionych itp.)

**Metody oceny:**

Aktywność na warsztatach, test zaliczeniowy
Test końcowy 50 punktów
Aktywność na ćwiczeniach 10 punktów

**Egzamin:**

nie

**Literatura:**

1. Neal Koblitz, Wykład z teorii liczb i kryptografii, Wydawnictwo Naukowo-Techniczne, Warszawa 1995.
2. R. Crandall, C. Pomerance, Prime Numbers. A Computational Perspective, Springer Verlag, Berlin 46 Heidelberg, 2000.
3. Song.Y.Yan, Teoria liczb w informatyce, PWN, 2016
4. D. Bressoud, S.Wagon, A Course in Computational Number Theory, Springer Verlag, Berlin Heidelberg 2000.

**Witryna www przedmiotu:**

e.mini.pw.edu.pl

**Uwagi:**

.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka ATL\_W01:**

Zna podstawowe twierdzenia, metody badawcze oraz algorytmy związane z problemami obliczeniowymi w teorii liczb.

Weryfikacja:

Aktywność na zajęciach, kolokwium zaliczeniowe

**Powiązane charakterystyki kierunkowe:** M2\_W03, M2MCB\_W15

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka ATL\_U01:**

Umie rozwiązywać podstawowe problemy obliczeniowej natury w teorii liczb.

Weryfikacja:

Kolokwium, aktywność na zajęciach

**Powiązane charakterystyki kierunkowe:** M2MCB\_U02, M2MCB\_U04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka ATL\_K01:**

Rozumie przydatność nabytej wiedzy i umiejętności obliczeniowych do stawiania hipotez oraz z ich weryfikacji w możliwych zastosowaniach w kryptografii.

Weryfikacja:

Kolokwium, aktywność na zajęciach

**Powiązane charakterystyki kierunkowe:** M2MCB\_K02

**Powiązane charakterystyki obszarowe:**