**Nazwa przedmiotu:**

Teoria liczb

**Koordynator przedmiotu:**

dr Barbara Roszkowska-Lech

**Status przedmiotu:**

Fakultatywny ograniczonego wyboru

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Informatyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

**Semestr nominalny:**

1 / rok ak. 2011/2012

**Liczba punktów ECTS:**

4

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

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

**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:**

Algebra liniowa z geometrią

**Limit liczby studentów:**

**Cel przedmiotu:**

do uzupełnienia

**Treści kształcenia:**

W trakcie wykładu omówione zostaną elementarne zagadnienia z teorii liczb ze szczególnym uwzględnieniem tematów, w których istotną role odgrywają algorytmy.
Program wykładu obejmować będzie następujące zagadnienia: podstawowe własności liczb naturalnych; liczby pierwsze, twierdzenia o liczbach pierwszych; podzielność, algorytm Euklidesa; liniowe równania diofantyczne; kongruencje i arytmetyka modularna; Chińskie Twierdzenie o resztach; potęgowanie modulo n; twierdzenia Fermata, Eulera i Wilsona; reszty i niereszty kwadratowe, symbole Legrendre’a i Jacobiego; obliczanie pierwiastków; logarytm dyskretny i jego obliczanie; testy pierwszości i algorytmy rozkładu; zastosowanie teorii liczb w kryptografii, szyfry z kluczem publicznym.
W trakcie towarzyszących wykładowi ćwiczeniom będą podjęte próby zaprogramowania wybranych algorytmów.

**Metody oceny:**

Zaliczenie przedmiotu na podstawie kolokwium zaliczeniowego i pracy na ćwiczeniach. Łączną ocenę punktową przelicza się na stopnie według poniższych zasad:
a) 3.0 jeżeli uzyskali od 51 do 60 pkt.
b) 3.5 jeżeli uzyskali od 61 do 70 pkt.
c) 4.0 jeżeli uzyskali od 71 do 80 pkt.
d) 4.5 jeżeli uzyskali od 81 do 90 pkt.
e) 5.0 jeżeli uzyskali powyżej 90 pkt.

**Egzamin:**

**Literatura:**

1. Song Y. Yan, Teoria liczb w informatyce PWN, Warszawa 2006
2. Wacław Marzantowicz, Piotr Zarzycki, Elementarna teoria liczb, PWN, Warszawa 2006
3. N. Koblitz, Wykład z teorii liczb i kryptogafii, WNT, Warszawa 1995
4. P. Ribenboim, Mała księga wielkich liczb pierwszych, WNT, Warszawa, 1996

**Witryna www przedmiotu:**

**Uwagi:**

## Efekty przedmiotowe