



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Elementarna teoria liczb [S1MNT1>F-ETL]

Przedmiot

Kierunek studiów

Matematyka nowoczesnych technologii

Rok/Semestr

3/5

Studia w zakresie (specjalność)

–

Profil studiów

ogólnoakademicki

Poziom studiów

pierwszego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

stacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

30

Laboratorium

0

Inne

0

Ćwiczenia

15

Projekty/seminaria

0

Liczba punktów ECTS

3,00

Koordynatorzy

dr Anna Iwaszkiewicz-Rudoszańska

anna.iwaszkiewicz-rudoszanska@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student powinien mieć podstawową wiedzę z zakresu, algebry abstrakcyjnej i matematyki dyskretnej. Powinien także przeprowadzać poprawne wnioskowania logiczne i rozumieć konieczność poszerzania swoich kompetencji.

Cel przedmiotu

Celem przedmiotu jest przedstawienie podstawowych pojęć i metod stosowanych elementarnej teorii liczb oraz jej zastosowań.

Przedmiotowe efekty uczenia się

Wiedza:

- Ma pogłębioną wiedzę z zakresu elementarnej teorii liczb [K_W01(P6S_WG)];
- Zna podstawowe definicje i twierdzenia z elementarnej teorii liczb [K_W01(P6S_WG)].

Umiejętności:

- Posługuje się kongruencjami, zna ich podstawowe własności i zastosowania, m.in. w kryptografii [K_U01(P6S_UW)];

- Potrafi rozwiązywać podstawowe typy równań diofantycznych [K_U01(P6S_UW)];
- Umie przeprowadzić rozumowanie matematyczne: udowodnić twierdzenie lub podać odpowiedni kontrprzykład [K_U01(P6S_UW)].

Kompetencje społeczne:

- Zna ograniczenia własnej wiedzy i rozumie potrzebę dalszego kształcenia [K_K01(P6S_KK),K_K02(P6S_KK)].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykłady: ocena wiedzy i umiejętności wykazanych na zaliczeniu pisemnym, składającym się z pięciu równo punktowanych pytań; zagadnienia udostępnione studentom co najmniej dwa tygodnie przed zaliczeniem;

próg zaliczeniowy 50%, każde 10% więcej to pół oceny w górę.

Ćwiczenia: umiejętności weryfikowane na podstawie trzech krótkich, równo punktowanych sprawdzianów; do zaliczenia potrzeba w sumie 50% możliwych do zdobycia punktów; każde 10% punktów więcej to pół oceny w górę; możliwe dodatkowe punkty za rozwiązanie zadań domowych.

Treści programowe

Podzielność w zbiorze liczb całkowitych. Kongruencje. System kryptograficzny RSA. Kongruencje kwadratowe. System kryptograficzny Rabina. Wybrane równania diofantyczne. Przedstawienie liczb naturalnych w postaci sumy kwadratów liczb naturalnych. Funkcje arytmetyczne. Testy pierwszości i algorytmy faktoryzacji.

Tematyka zajęć

Aktualizacja: 31.05.2024r.

Wykłady:

- podzielność w zbiorze liczb całkowitych (definicja, własności, algorytm Euklidesa, liczby pierwsze, twierdzenie Dirichleta o liczbach pierwszych w postępach arytmetycznych z dowodami szczególnych przypadków);
- kongruencje (definicja, własności, cechy podzielności, chińskie twierdzenie o resztach, funkcja Eulera i twierdzenie Eulera, Wilsona i Lagrange'a);
- system kryptograficzny RSA jako zastosowanie twierdzenia Eulera;
- kongruencje kwadratowe (reszty i niereszty kwadratowe, symbol Legendre'a i Jacobiego, prawo wzajemności reszt kwadratowych Gaussa);
- system kryptograficzny Rabina;
- wybrane równania diofantyczne;
- przedstawienie liczb naturalnych w postaci sumy kwadratów liczb naturalnych;
- funkcje arytmetyczne (definicja i przykłady, funkcje addytywne i multiplikatywne, splot Dirichleta);
- testy pierwszości i algorytmy faktoryzacji (test Fermata, Solovaya-Strassena, Millera-Rabina, faktoryzacja liczb Mersenne'a i Fermata, metoda Fermata, Dixona i p-1 Pollarda).

Ćwiczenia:

- podzielność w zbiorze liczb całkowitych;
- kongruencje (kongruencje liniowe, chińskie twierdzenie o resztach, małe twierdzenie Fermata i twierdzenie Eulera);
- system kryptograficzny RSA;
- kongruencje kwadratowe, symbol Legendre'a i Jacobiego, prawo wzajemności reszt kwadratowych Gaussa;
- system kryptograficzny Rabina;
- wybrane równania diofantyczne.

Metody dydaktyczne

Wykłady: prezentacja (zawartość prezentacji przekazywana studentom przed wykładem) uzupełniana dowodami i przykładami przedstawianymi na tablicy, z pytaniami kierowanymi do studentów; teoria przedstawiana w powiązaniu z aktualną wiedzą studentów.

Ćwiczenia: rozwiązywanie przykładowych zadań na tablicy, samodzielne rozwiązywanie zadań przez studentów, inicjowanie dyskusji nad rozwiązaniami, szczegółowe recenzowanie rozwiązań przez

prowadzącego
ćwiczenia.

Literatura

Podstawowa:

- W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN, Warszawa 2006;
- W. Narkiewicz, Teoria liczb, PWN, Warszawa 2003;
- M. Zakrzewski, Teoria liczb, GiS, Wrocław 2017;
- J. Rutkowski, Teoria liczb w zadaniach, PWN, Warszawa 2019.

Uzupełniająca:

- N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995;
- W. Sierpiński, 250 zadań z elementarnej teorii liczb, WSiP, 1987.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	75	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	45	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	30	1,00