UNIWERSYTET WARMIŃSKO-MAZURSKI W OLSZTYNIE

Wydział Matematyki i Informatyki

Sylabus przedmiotu/modułu - część A

11020-13-C ARYTMETYKA MODULARNA I KOMPUTEROWA

ECTS: 5 MODULAR AND COMPUTER ARITHEMETIC.

Przedmiot/moduł:
ARYTMETYKA MODULARNA I KOMPUTEROWA
Obszar kształcenia: nauki ścisłe
Status przedmiotu: Obligatoryjny
Grupa przedmiotów: C-przedmiot specjalnościowy
Kod ECTS: 11020-13-C
Kierunek studiów: Matematyka
Specjalność: Matematyka stosowana
Profil kształcenia: Ogólnoakademicki
Forma studiów: Stacjonarne
Poziom studiów/Forma kształcenia: Studia pierwszego stopnia
Rok/semestr: 1/II

Rodzaje zajęć: wykłady, ćwiczenia
Liczba godzin w semestrze/tygodniu:
wykłady: 30/2
ćwiczenia: 30/2
Formy i metody dydaktyczne
wykłady: metoda podająca z prezentacją multimedialną
ćwiczenia: metoda tablicowa, prezentacja obliczeń komputerowych
Forma i warunki zaliczenia: Egzamin/Zaliczenie ćwiczeń na podstawie aktywności studenta oraz kolokwium zawierającego zadania otwarte. Egzamin w pisemny i ustny
Liczba punktów ECTS: 5
Język wykładowy: polski
Przedmioty wprowadzające: Matematyka elementarna
Wymagania wstępne: Znajomość pojęć matematyki i informatyki na poziomie maturalnym

Nazwa jednostki organizacyjnej realizującej przedmiot:
Katedra Algebry i Geometrii
adres: ul. Słoneczna 54, , 10-710 Olsztyn
tel. 524 60 48
Osoba odpowiedzialna za realizację przedmiotu:
dr Bogdan Staruch

TREŚCI WYKŁADÓW

Aksjomatyka Peano liczb naturalnych i definicje rekurencyjne. Zasada indukcji, zasada minimum. Poprawność algorytmu. Rekurencja i iteracja. Relacja podzielności, dzielenie z resztą. Algorytm Euklidesa.Zagadnienie złożoności algorytmu. Problem P=NP? Systemy pozycyjne. Prezentacja liczb w komputerze. Operacje na bitach. Koszt kodowania binarnego. Liczby pierwsze, twierdzenie o rozkładzie na czynniki pierwsze. Złożoność faktoryzacji. Rachunek reszt modulo n. Zastosowanie arytmetyki modularnej do budowy funkcji szyfrującej i deszyfrującej w symetrycznych systemach kryptograficznych. Małe Twierdzenie Fermata. Funkcja Eulera i Twierdzenie Eulera. Chińskie twierdzenie o resztach. Rozwiązywanie kongruencji. Logarytm dyskretny. Systemy kryptograficzne z kluczem publicznym. System RSA. System ElGamal.

TREŚCI ĆWICZEŃ

Treści ćwiczeń są ściśle powiązane z treścią wykładów. Zawarte sa następujące treści: Indukcja, rekurencja. Algorytmy rekurencyjne i iteracyjne. Algorytm dzielenia z resztą i algorytm Euklidesa. Poprawność algorytmu. oszacowanie złożoności algorytmu. Równania diofantyczne. Prawa podzielności w różnych systemach pozycyjnych. Rozwiązywanie kongruencji i układów kongruencji.

CEL KSZTAŁCENIA

Wprowadzenie w sposób ścisły i uporządkowany pojęć teorii liczb (w szczególności rachunku reszt) z naciskiem na zastosowania w informatyce.

OPIS EFEKTÓW KSZTAŁCENIA PRZEDMIOTU W ODNIESIENIU DO OBSZAROWYCH I KIERUNKOWYCH EFEKTÓW KSZTAŁCENIA

Symbole efektów obszarowych X1A_W01, X1A_W02, X1A_W03, X1A_W04, X1A_W05, X1A_U01, X1A_U06, X1A_U07, X1A_U08, X1A_U09, X1A_K01, X1A_K02, X1A_K03, X1A_K04, X1A_K05
Symbole efektów kierunkowych K_W01, K_W02, K_W03, K_W04, K_W08, K_U01, K_U03, K_U36 K_K01, K_K02, K_K04, K_K05

EFEKTY KSZTAŁCENIA

Wiedza

K_W01 Student zna własności liczb oraz ich zastosowania w informatyce-reprezentacja liczb w komputerze, funkcja skrótu (X1A_W01). K_W02 rozumie rolę i znaczenie dowodu (X1A_W03). K_W03 Zna metody indukcyjne i definicje rekurencyjne.Rozumie istotę systemów kryptograficznych (X1A_W02,X1A_W03). K_W04 Zna podstawowe twierdzenia teorii liczb (X1A_W01, X1A_W03). K_W08 Student zna pojęcie złożoności algorytmu oraz sformułowanie problemu P=NP. Zna niektóre algorytmy kryptograficzne (X1A_W04,X1A_W05).

Umiejętności

K_U01 Rozwiązuje liniowe równania diofantyczne i układy równań liniowych. Rozwiązuje liniowe równania diofantyczne, rozwiązuje kongruencje nieliniowe i układy kongruencji (X1A_U01, X1A_U06). K_U03 Stosuje zasadę indukcji w dowodach, definiuje rekurencyjnie (X1A_U01). K_U36 Potrafi wyprowadzić i udowodnić cechy podzielności w systemach pozycyjnych.Potrafi zaszyfrować i odszyfrowac wiadomość w symetrycznych algorytmach szyfrowania (X1A_U06, X1A_U09).

Kompetencje społeczne

K_K01 rozumie, że pojawiają się wciąż nowe zastosowania arytmetyki w informatyce(X1A_K01,X1A_U07). K_K02 docenia poprawność wnioskowania i konieczność uzasadniania tez na przykładzie własności arytmetycznych (X1A_K01, X1A_K02, X1A_U09). K_K04 ceni własność intelektualną innych osób i wie jak korzystać z niej w sposób uczciwy (X1A_K03,X1A_K04). K_K05 Potrafi posługiwać się formalnym językiem w sposób prosty i zrozumiały dla laików (X1A_K05, X1A_U08).

LITERATURA PODSTAWOWA

1) R. L. Graham, D. E. Knuth, O. Patashnik, 2002r., "Matematyka konkretna", wyd. PWN, 2) W. Narkiewicz, 2003r., "Teoria liczb", wyd. PWN, 3) K. Ross, C. Wright,, 2002r., "Matematyka dyskretna", wyd. PWN, 4) D. R. Stinson, 2005r., "Kryptografia. W teorii i w praktyce", wyd. WNT, 5) J. Gancarzewicz, 2002r., "Arytmetyka", wyd. wyd UJ, 6) T.H.Cormen, Ch.E. Leiserson, R.L. Rivest, C.Stein, 2007r., "Wprowadzenie do algorytmów", wyd. WNT, 7) Bogdan Staruch, Bożena Staruch, 2012r., "wykład autorski w formie prazentacji".

LITERATURA UZUPEŁNIAJĄCA

1) Harel D., Feldman Y., 2002r., "Rzecz o istocie informatyki. Algorytmika.", wyd. WNT, 2) H. Rasiowa, 1970r., "Wstęp do matematyki współczesnej", wyd. PWN, 3) W. Sierpiński, 1964r., "Teoria liczb", wyd. PWN.

Kod ECTS: AAABB-CD-E_F AAA – Kod dziedziny w systemie ECTS, BB – numer kierunku, C – 1 studia pierwszego stopnia (inżynierskie lub licencjackie), 2 – studia drugiego stopnia, 3 – studia jednolite magisterskie, 4 – studia trzeciego stopnia, 5 – studia podyplomowe, D – numer specjalności, E – grupa przedmiotów, F – kolejny numer przedmiotu w podzbiorze.

Szczegółowy opis przyznanej punktacji ECTS - część B

ARYTMETYKA MODULARNA I KOMPUTEROWA

ECTS: 5 **MODULAR AND COMPUTER ARITHEMETIC.**

Na przyznaną liczbę punktów ECTS składają się :

1. Godziny kontaktowe z nauczycielem akademickim:

- wykład	30,0 godz.
- ćwiczenia	30,0 godz.
- konsultacje	5,0 godz.
	65,0 godz.

2. Samodzielna praca studenta:

- przygotowanie do ćwiczeń	20,0 godz.
- przygotowanie do kolokwium	20,0 godz.
- przygotowanie do egzaminu	20,0 godz.
	60,0 godz.
godziny kontaktowe + samodzielna praca studenta OGÓŁEM:	125,0 godz.

1 punkt ECTS = 25,00 godz. pracy przeciętnego studenta,

liczba punktów ECTS = 125,00 godz.: 25,00 godz./ECTS = **5,00 ECTS**

w zaokrągleniu: **5 ECTS**

- w tym liczba punktów ECTS za godziny kontaktowe z bezpośrednim udziałem nauczyciela akademickiego - **2,60** punktów ECTS,
- w tym liczba punktów ECTS za godziny realizowane w formie samodzielnej pracy studenta - **2,40** punktów ECTS.

Kod ECTS: AAABB-CD-E_F AAA – Kod dziedziny w systemie ECTS, BB – numer kierunku, C – 1 studia pierwszego stopnia (inżynierskie lub licencjackie), 2 – studia drugiego stopnia, 3 – studia jednolite magisterskie, 4 – studia trzeciego stopnia, 5 – studia podyplomowe, D – numer specjalności, E – grupa przedmiotów, F – kolejny numer przedmiotu w podzbiorze.