UNIWERSYTET WARMIŃSKO-MAZURSKI W OLSZTYNIE

Wydział Matematyki i Informatyki

Sylabus przedmiotu/modułu - część A

11017-10-B_F PRZEDMIOT FAKULTATYWNY – TEORIA LICZB W INFORMATYCE

ECTS: 5 FACULTATIVE SUBJECT – NUMBER THEORY IN COMPUTER SCIENCE

TREŚCI WYKŁADÓW

Aksjomatyka Peano liczb naturalnych i definicje rekurencyjne. Zasada indukcji, zasada minimum. Poprawność algorytmu. Rekurencja i iteracja. Relacja podzielności, dzielenie z resztą. Równania diofantyczne. Zliczanie. Zagadnienie złożoności algorytmu. Problem P=NP? Systemy pozycyjne. Koszt kodowania binarnego. Operacje na bitach. Liczby pierwsze, twierdzenie o rozkładzie na czynniki pierwsze. Złożoność faktoryzacji. Grupy, pierścienie i ciała. Pierścienie reszt modulo n. Ciała skończone. Tablice z haszowaniem. 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. Szybki algorytm potęgowania. Logarytm dyskretny. Systemy kryptograficzne z kluczem publicznym. System RSA. Ataki na system RSA. System ElGamal. Testy pierwszości. Algorytmy probabilistyczne. Metoda Las Vegas i Monte Carlo.

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. Zastosowanie własności liczb w tablicach z haszowaniem i algorytmach kryptograficznych.

CEL KSZTAŁCENIA

Celem zajęć jest ukazanie zastosowania teorii liczb w informatyce, w szczególności w algorytmice i kryptografii. Jednym z celów jest również uświadomienie studentom istnienia formalnego aparatu kryjącego się za większością stosowanych algorytmów.

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

Symbole efektów obszarowych T1A_W01 T1A_W03 T1A_W04 T1A_W07 InzA_W02 T1A_U01 T1A_U08 T1A_U09 InzA_U02 T1A_K01
Symbole efektów kierunkowych K_W01 K_W15 K_U01 K_U07 K_K01

EFEKTY KSZTAŁCENIA

Wiedza

K_W01 K_W15 Student zna własności liczb oraz ich zastosowania w algorytmach stosowanych w informatyce, w szczególności w funkcjach skrótu i algorytmach kryptograficznych.(T1A_W01 T1A_W07) K_W15 Student zna pojęcie złożoności algorytmu oraz sformułowanie problemu P=NP i jego zastosowanie w systemach kryptograficznych. (T1A_W03 T1A_W04 InzA_W02)

Umiejętności

K_U01 Student potrafi stosować arytmetyke modularną. Rozwiązuje liniowe równania diofantyczne i układy równań liniowych. Stosuje Małe Tw. Fermata w rozwiązywaniu równań diofantycznych. Potrafi zaszyfrować i odszyfrowac wiadomość w symetrycznych algorytmach szyfrowania oraz dla niewielkich liczb – w algorytmie RSA i ElGamal. Korzysta z literatury i zasobów internetowych. (T1A_U01) K_U07 Student potrafi napisać program implementujący wybrane algorytmy teorioliczbowe. (T1A_U08 T1A_U09 InzA_U02)

Kompetencje społeczne

K_K01 Student rozumie problem bezpieczeństwa danych oraz konieczność ich ochrony. Student zdaje sobie sprawę ze stosowania ugruntowanej teorii matematycznej w problemach informatyki. (T1A_K01)

LITERATURA PODSTAWOWA

1) Bożena Staruch, 2012r., "Teoria liczb w informatyce", wyd. wykład autorski w formie elektronicznej, 2) T.H.Cormen, Ch.E. Leiserson, R.L. Rivest, C.Stein, 2007r., "Wprowadzenie do algorytmów", wyd. WNT, 3) R. L. Graham, D. E. Knuth, O. Patashnik, 2002r., "Matematyka konkretna", wyd. PWN, 4) D.Harel, Y.Feldman , 2008r., "zecz o istocie informatyki. Algorytmika", wyd. WNT, 5) W. Narkiewicz, 2003r., "Teoria liczb", wyd. PWN, 6) K. Ross, C. Wright, 2006r., "Matematyka dyskretna", wyd. PWN, 7) D. R. Stinson, 2005r., "Kryptografia. W teorii i w praktyce", wyd. WNT.

LITERATURA UZUPEŁNIAJĄCA

1) J. Gancarzewicz, 2002r., "Arytmetyka", wyd. UJ, 2) H. Rasiowa, 1970r., "Wstęp do matematyki współczesnej", wyd. PWN, 3) W. Sierpiński, 1950r., "Teoria liczb", wyd. PWN.

Przedmiot/moduł:
PRZEDMIOT FAKULTATYWNY – TEORIA LICZB W INFORMATYCE
Obszar kształcenia: nauki techniczne
Status przedmiotu: Fakultatywny
Grupa przedmiotów: B_F-przedmiot kierunkowy do wyboru
Kod ECTS: 11017-10-B_F
Kierunek studiów: Informatyka
Specjalność: Wszystkie specjalności
Profil kształcenia: Ogólnoakademicki
Forma studiów: Stacjonarne
Poziom studiów/Forma kształcenia: Studia pierwszego stopnia
Rok/semestr: III/6

Rodzaje zajęć: wykład, ćwiczenia audytoryjne, pracownia komputerowa
Liczba godzin w semestrze/tygodniu:
wykłady: 30/2
ćwiczenia: 30/2
Formy i metody dydaktyczne
wykłady: metoda podająca z prezentacją multimedialną
ćwiczenia: metoda ambulatoryjna przy tablicy, praca przy komputerze - testowanie poznanych algorytmów i tworzenie własnych programów.
Forma i warunki zaliczenia: Egzamin/Zaliczenie ćwiczeń na podstawie aktywności studenta, samodzielnej implementacji jednego z algorytmów teorii liczb, kolokwium zawierającego zadania otwarte. Egzamin w postaci testu
Liczba punktów ECTS: 5
Język wykładowy: polski
Przedmioty wprowadzające: Matematyka dyskretna, Algorytmy i struktury danych, Wstęp do programowania
Wymagania wstępne: Podstawowy zakres wiedzy z przedmiotów wprowadzających

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 Bożena Staruch
e-mail: bostar@matman.uwm.edu.pl

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

PRZEDMIOT FAKULTATYWNY – TEORIA LICZB W INFORMATYCE

ECTS: 5 **FACULTATIVE SUBJECT – NUMBER THEORY IN COMPUTER SCIENCE**

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	15,0 godz.
- przygotowanie sprawozdań z ćwiczeń	10,0 godz.
- przygotowanie do egzamniu	20,0 godz.
- przygotowanie do kolokwium	15,0 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.