KARTA PRZEDMIOTU

Kod przedmiotu	0541-2MAT-F57-MOA	
Nazwa przedmiotu w języku	polskim	***Metody obliczeniowe algebry***
	angielskim	***Efficient methods of algebra***

1. USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

1.1. Kierunek studiów	matematyka
1.2. Forma studiów	studia stacjonarne
1.3. Poziom studiów	studia drugiego stopnia
1.4. Profil studiów	ogólnoakademicki
1.5. Specjalność	nauczanie matematyki, analiza danych
1.6. Jednostka prowadząca przedmiot	WM, Instytut Matematyki
1.7. Osoba/zespół przygotowująca/y kartę przedmiotu	dr Elżbieta Zając
1.8. Osoba odpowiedzialna za przedmiot	
1.9. Kontakt	

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Przynależność do modułu	Fakultatywny
2.2. Język wykładowy	polski
2.3. Semestry, na których realizowany jest przedmiot	2 lub 4
2.4. Wymagania wstępne	Algebra z teorią liczb

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć		wykład, ćwiczenia laboratoryjne
3.2. Miejsce realizacji zajęć		zajęcia w po mieszczeniu dydaktycznym UJK
3.3. Forma zaliczenia zajęć		zaliczenie z oceną (wykład, ćwiczenia laboratoryjne)
3.4. Metody dydaktyczne		wykład: wykład problemowy, dyskusja; ćwiczenia laboratoryjne: rozwiązywanie zadań przy pomocy komputera, referat, praca z książką
3.5. Wykaz literatury	**podstawowa**	A. Chrzęszczyk, Algorytmy teorii liczb i kryptografii w przy-kładach, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2010 N. Koblitz. Algebraiczne aspekty kryptografii, WNT, Warszawa 2000 J. von zur Gathen and J. Gerhard. Modern Computer Algebra. Cambridge University Press, second edition, 2003 V. Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press 2008 D. Cox, J. Little and D O'Shea, Ideals, Varieties, and Algorithms, Third Edition, Springer, New York, 2007.
	uzupełniająca	

4. CELE, TREŚCI I EFEKTY KSZTAŁCENIA

4.1. Cele przedmiotu ***(z uwzględnieniem formy zajęć)***

Wykład

C1 – zapoznanie z metodami algebry obliczeniowej, które mają zastosowania w m.in. w kryptografii, informatyce i automatyce

Ćwiczenia laboratoryjne

C1 – kształtowanie umiejętności samodzielnej implementacji algorytmów algebry obliczeniowej z zastosowaniem zdobytej wiedzy i wykorzystaniem pakietów obliczeniowych

C2 – kształtowanie umiejętności rozwiązywania problemów z wykorzystaniem dostępnych źródeł wiedzy i we współpracy z zespołem

4.2. Treści programowe ***(z uwzględnieniem formy zajęć)***

Wykład:

Elementy algebry liniowej, rachunek macierzowy, wykorzystanie macierzy rzadkich w operacjach na macierzach, wyznaczanie wektorów własnych i wartości własnych macierzy. Pierścienie euklidesowe, rozszerzony algorytm Euklidesa, chińskie twierdzenie o resztach i ich zastosowania do arytmetyki w pierścieniach ilorazowych liczb całkowitych i pierścieni wielomianów jednej zmiennej nad ciałem. Testowanie pierwszości. Podstawowe fakty z teorii ciał, rozszerzenia algebraiczne, elementy teorii Galois. Ciała skończone, automorfizm Frobeniusa. Testowanie nierozkładalności wielomianów nad ciałami skończonymi. Konstruowanie ciał skończonych. Faktoryzacja i wyznaczanie pierwiastków wielomianów nad ciałami liczbowymi. Rugownik wielomianów. Podstawowe fakty z teorii baz Groebnera. Rozwiązywanie układów równań wielomianowych. Wykorzystanie pakietów obliczeniowych Mathematica, Matlab, Sage. Definiowanie algorytmów z zakresu algebry obliczeniowej w języku Python.

Ćwiczenia laboratoryjne:

Realizacja zadań obliczeniowych i opracowywanie algorytmów z zakresu zgodnego z tematyką wykładu z wykorzystaniem pakietów Mathematica, Matlab, Sage oraz języka programowania Python. Referaty z zakresu zastosowań metod algebry obliczeniowej.

4.3. Przedmiotowe efekty kształcenia

Efekt	Student, który zaliczył przedmiot	Odniesienie do kierunkowych efektów kształcenia
w zakresie **WIEDZY:**		
W01	zna algorytmy algebraiczne służące do faktoryzacji wielomianów oraz rozwiązywania układów równań, przedstawia wybrane efektywne metody algebry i podaje przykłady ich zastosowań	MAT2A_W02
W02	podaje przykłady zastosowania poznanych metod w kryptografii,	MAT2A_W04
W03	zna podstawowe zasady realizacji zadań z zakresu algebry obliczeniowej w środowiskach pakietów obliczeniowych Mathematica, Matlab, Sage oraz z wykorzystaniem języka programowania (np. Python)	MAT2A_W06
w zakresie **UMIEJĘTNOŚCI:**		
U01	Realizuje zadania z zakresu algebry liniowej w oparciu o reprezentację macierzową	MAT2A_U014
U02	Stosuje algorytm Euklidesa i jego rozszerzenia w celu wyznaczania największych wspólnych dzielników w pierścieniach euklidesowych	MAT2A_U14
U03	testuje nierozkładalność wielomianów i konstruuje ciała skończone jako pierścienie ilorazowe,	MAT2A_U14
U04	rozpoznaje problemy, w tym zagadnienia praktyczne, które można sprowadzić do rozwiązywania układów równań wielomianowych,	MAT2A_U14
U05	stosuje w praktyce poznaną wiedzę z zakresu algebry obliczeniowej do zagadnień z zakresu kryptografii (szyfrowanie wiadomości, podpis cyfrowy, dzielenie sekretu),	MAT2A_U02
U06	implementuje poznane algorytmy i metody wykorzystując pakiety do obliczeń symbolicznych	MAT2A_U03
U07	implementuje wybrane algorytmy w języku programowania (np. Python) i ocenia ich efektywność	MAT2A_U17
U08	pracuje w grupie, współpracuje z jej członkami w celu pozyskania niezbędnej wiedzy oraz opracowania złożonych algorytmów	MAT2A_U24
w zakresie **KOMPETENCJI SPOŁECZNYCH:**		
K01	precyzyjnie formułuje pytania służące pogłębieniu własnego zrozumienia danego tematy lub odnalezieniu brakujących elementów rozumowania	MAT2A_K02

4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów kształcenia

Efekty przedmiotowe *(symbol)*	Sposób weryfikacji (+/-)					
	Kolokwium		Referat Sprawozdania		Zadania domowe	
	Forma zajęć		*Forma zajęć*		*Forma zajęć*	
	W	*C*	*W*	*C*	*W*	*C*
W01	+					
W02	+					
W03	+					
U01				+		+
U02				+		+
U03				+		+
U04				+		+
U05				+		+
U06				+		+
U07				+		+
U08				+		+
K01				+		+

4.5. Kryteria oceny stopnia osiągnięcia efektów kształcenia

Forma zajęć	Ocena	Kryterium oceny
wykład (*W*)	**3**	co najmniej 50% i nie więcej, niż 60% łącznej liczby punktów możliwych do uzyskania
	3,5	ponad 60% i nie więcej, niż 70% łącznej liczby punktów możliwych do uzyskania
	4	ponad 70% i nie więcej, niż 80% łącznej liczby punktów możliwych do uzyskania
	4,5	ponad 80% i nie więcej, niż 90% łącznej liczby punktów możliwych do uzyskania
	5	ponad 90% liczby punktów możliwych do uzyskania

ćwiczenia laboratoryjne (*C*)	**3**	co najmniej 50% i nie więcej, niż 60% łącznej liczby punktów możliwych do uzyskania
	3,5	ponad 60% i nie więcej, niż 70% łącznej liczby punktów możliwych do uzyskania
	4	ponad 70% i nie więcej, niż 80% łącznej liczby punktów możliwych do uzyskania
	4,5	ponad 80% i nie więcej, niż 90% łącznej liczby punktów możliwych do uzyskania
	5	ponad 90% liczby punktów możliwych do uzyskania

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta**
	Studia stacjonarne
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/	***62***
Udział w wykładach	30
Udział w ćwiczeniach laboratoryjnych	30
Udział w kolokwium zaliczeniowym	2
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	***38***
Przygotowanie do ćwiczeń laboratoryjnych	28
Przygotowanie do kolokwium	10
ŁĄCZNA LICZBA GODZIN	***100***
PUNKTY ECTS za przedmiot	**4**

Przyjmuję do realizacji *(data i podpisy osób prowadzących przedmiot w danym roku akademickim)*

.....