KARTA PRZEDMIOTU

Kod przedmiotu	**11.1-2MAT-F03.2-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 / studia niestacjonarne*
1.3. Poziom studiów	*studia drugiego stopnia*
1.4. Profil studiów	*ogólnoakademicki*
1.5. Specjalność	*nauczanie matematyki, zastosowania matematyki*
1.6. Jednostka prowadząca przedmiot	*WM, Instytut Matematyki*
1.7. Osoba przygotowująca kartę przedmiotu	*dr Elżbieta Zając*
1.8. Osoba odpowiedzialna za przedmiot	*dr hab. Egmont Porten*
1.9. Kontakt	*Egmont.Porten@miun.se*

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Przynależność do modułu	*F*
2.2. Status przedmiotu	*fakultatywny*
2.3. Język wykładowy	*polski*
2.4. Semestry, na których realizowany jest przedmiot	*4*
2.5. Wymagania wstępne	*Algebra z teorią liczb*

3. FORMY, SPOSOBY I METODY PROWADZENIA ZAJĘĆ

3.1. Formy zajęć		*wykład, ćwiczenia laboratoryjne*
3.2. Sposób realizacji zajęć		*zajęcia w pomieszczeniu dydaktycznym UJK*
3.3. Sposób 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** **uzupełniająca**	1. *A. Chrzęszczyk, Algorytmy teorii liczb i kryptografii w przykładach, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2010* 2. *N. Koblitz. Algebraiczne aspekty kryptografii, WNT, Warszawa 2000* 3. *J. von zur Gathen and J. Gerhard. Modern Computer Algebra. Cambridge University Press, second edition, 2003* 4. *V. Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press 2008* 5. *D. Cox, J. Little and D O'Shea, Ideals, Varieties, and Algorithms, Third Edition, Springer, New York, 2007.*

4. CELE, TREŚCI I EFEKTY KSZTAŁCENIA

4.1. Cele przedmiotu

Wiedza

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

Umiejętności

C2 – Kształtowanie umiejętności samodzielnej implementacji algorytmów algebry obliczeniowej z zastosowaniem zdobytej wiedzy i wykorzystaniem pakietów obliczeniowych

Kompetencje społeczne

C3 – Kształtowanie umiejętności rozwiązywania problemów z wykorzystaniem dostępnych źródeł wiedzy i we współpracy z zespołem

4.2. Treści programowe

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 (mała, średnia, duża liczba efektów)

kod	Student, który zaliczył przedmiot	***Stopień nasycenia efektu kierunkowego***	Odniesienie do efektów kształcenia	
w zakresie **WIEDZY:**			**dla kierunku**	**dla obszaru**
W01	zna algorytmy algebraiczne służące do faktoryzacji wielomianów oraz rozwiązywania układów równań, przedstawia wybrane efektywne metody algebry i podaje przykłady ich zastosowań	++	MAT2A_W02	X2A_W02
W02	podaje przykłady zastosowania poznanych metod w kryptografii,	++	MAT2A_W04	X2A_W02
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_W07	X2A_W04 X2A_W05
W zakresie UMIEJĘTNOŚCI:				
U01	Realizuje zadania z zakresu algebry liniowej w oparciu o reprezentację macierzową	++	MAT2A_U15	X2A_U02 X2A_U04 X2A_U06
U02	Stosuje algorytm Euklidesa i jego rozszerzenia w celu wyznaczania największych wspólnych dzielników w pierścieniach euklidesowych	++	MAT2A_U15	X2A_U02 X2A_U04 X2A_U06
U03	testuje nierozkładalność wielomianów i konstruuje ciała skończone jako pierścienie ilorazowe,	++	MAT2A_U15	X2A_U02 X2A_U04 X2A_U06
U04	rozpoznaje problemy, w tym zagadnienia praktyczne, które można sprowadzić do rozwiązywania układów równań wielomianowych,	++	MAT2A_U15	X2A_U04
U05	stosuje w praktyce poznaną wiedzę z zakresu algebry obliczeniowej do zagadnień z zakresu kryptografii (szyfrowanie wiadomości, podpis cyfrowy, dzielenie sekretu),	++	MAT2A_U02	X2A_U03 X2A_U05

U06	implementuje poznane algorytmy i metody wykorzystując pakiety do obliczeń symbolicznych	++	MAT2A_U04	X2A_U03
U07	implementuje wybrane algorytmy w języku programowania (np. Python) i ocenia ich efektywność	++	MAT2A_U18	X2A_U04
w zakresie **KOMPETENCJI SPOŁECZNYCH:**				
K01	pracuje w grupie, współpracuje z jej członkami w celu pozyskania niezbędnej wiedzy oraz opracowania złożonych algorytmów.	++	MAT2A_K03	X2A_K02

4.4. Kryteria oceny osiągniętych efektów kształcenia				
na ocenę 3	**na ocenę 3,5**	**na ocenę 4**	**na ocenę 4,5**	**na ocenę 5**
Zaliczenie konwersatorium: osiąga 50-60% liczby punktów możliwych do uzyskania z kolokwiów, projektu i aktywności na zajęciach. Zaliczenie wykładu: osiąga 50-60% liczby punktów z kolokwium	*Zaliczenie konwersatorium: osiąga 61-70% liczby punktów możliwych do uzyskania z kolokwiów, projektu i aktywności na zajęciach. Zaliczenie wykładu: osiąga 61-70% liczby punktów z kolokwium*	*Zaliczenie konwersatorium: osiąga 71-80% liczby punktów możliwych do uzyskania z kolokwiów, projektu i aktywności na zajęciach. Zaliczenie wykładu: osiąga 71-80% liczby punktów z kolokwium*	*Zaliczenie konwersatorium: osiąga 81-90% liczby punktów możliwych do uzyskania z kolokwiów, projektu i aktywności na zajęciach. Zaliczenie wykładu: osiąga 81-90% liczby punktów z kolokwium*	*Zaliczenie konwersatorium: osiąga 91-100% liczby punktów możliwych do uzyskania z kolokwiów, projektu i aktywności na zajęciach. Zaliczenie wykładu: osiąga 91-100% liczby punktów z kolokwium*

4.5. Metody oceny							
Egzamin ustny	**Egzamin pisemny**	**Projekt**	**Kolokwium**	**Zadania domowe**	**Referat Sprawozdania**	**Dyskusje**	**Inne**
			+(w)	+(k)	+(k)	+(w, k)	

5. BILANS PUNKTÓW ECTS – NAKŁAD PRACY STUDENTA

Kategoria	**Obciążenie studenta**	
	Studia stacjonarne	**Studia niestacjonarne**
LICZBA GODZIN REALIZOWANYCH PRZY BEZPOŚREDNIM UDZIALE NAUCZYCIELA /GODZINY KONTAKTOWE/	**60**	**30**
Udział w wykładach	**30**	**10**
Udział w ćwiczeniach, konwersatoriach, laboratoriach... itd.	**30**	**15**
Udział w konsultacjach		**5**
Udział w egzaminie/kolokwium zaliczeniowym itp.		
Inne		
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	**65**	**95**
Przygotowanie do wykładu	**15**	**20**
Przygotowanie do ćwiczeń, konwersatorium, laboratorium itp.	**20**	**30**
Przygotowanie do egzaminu/kolokwium	**15**	**25**
Zebranie materiałów do projektu, kwerenda internetowa		
Opracowanie prezentacji multimedialnej	**15**	**20**
Przygotowanie hasła do wikipedii		
Inne		
ŁĄCZNA LICZBA GODZIN	**125**	**125**
PUNKTY ECTS za przedmiot	**5**	**5**

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

.....