

KARTA PRZEDMIOTU

Kod przedmiotu	0541.6.MAT2.D.OTL	
Nazwa przedmiotu w języku	polskim	Obliczeniowa teoria liczb Computational number theory
	angielskim	

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. Osoba przygotowująca kartę przedmiotu	dr hab. Olena Karlova
1.6. Kontakt	okarlova@ujk.edu.pl

2. OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

2.1. Język wykładowy	Polski
2.2. Wymagania wstępne*	Algebra abstrakcyjna 1, Algebra abstrakcyjna 2

3. SZCZEGÓŁOWA CHARAKTERYSTYKA PRZEDMIOTU

3.1. Forma zajęć	wykład specjalnościowy, ćwiczenia laboratoryjne	
3.2. Miejsce realizacji zajęć	zajęcia w pomieszczeniu dydaktycznym UJK	
3.3. Forma zaliczenia zajęć	Zal. z oceną (wykład), zal. z oceną (ćwiczenia laboratoryjne)	
3.4. Metody dydaktyczne	wykład specjalnościowy - wykład problemowy ćwiczenia laboratoryjne - metoda laboratoryjna (przy komputerze)	
3.5. Wykaz literatury	podstawowa	Chrzęszczuk A., Algorytmy teorii liczb i kryptografii. BTC. Legionowo 2010 Koblitz N., Wykład z teorii liczb i kryptografii. WNT. 2006.
	uzupełniająca	Yan S.Y., Teoria liczb w informatyce. PWN. Warszawa 2000

4. CELE, TREŚCI I EFEKTY UCZENIA SIĘ

4.1. Cele przedmiotu (z uwzględnieniem formy zajęć)
Wykład specjalnościowy C1 – zapoznanie studentów z obliczeniowymi aspektami teorii liczb
Ćwiczenia laboratoryjne C1 – wdrożenie studentów do wykorzystywania komputera do wspomagania badań matematycznych C2 – kształtowanie postawy samodzielności w poszukiwaniu informacji, gotowości do pracy grupowej
4.2. Treści programowe (z uwzględnieniem formy zajęć)
Wykład specjalnościowy: Obliczeniowe aspekty badania pierwszości liczb: test Eulera, test Millera-Rabina. Liczby Fermata i Mersenne’a. Efektywne metody rozkładu liczb całkowitych na czynniki: metody dzieleni próbnych, Fermata, bazy rozkładu, metoda ułamków łańcuchowych. Zagadnienie logarytmu dyskretnego. Podstawowe zagadnienia multiplikatywnej teorii liczb.
Ćwiczenia laboratoryjne: Rzędy i pierwiastki pierwotne. Obliczeniowe aspekty badania pierwszości liczb. Probabilistyczne testy pierwszości. Generowanie liczb pierwszych. Metody rozkładu liczb całkowitych na czynniki: metody dzieleni próbnych, Fermata. Kongruencja Legendre’a. Metoda ułamków łańcuchowych. Zagadnienie logarytmu dyskretnego.

4.3. Przedmiotowe efekty uczenia się

Efekt	Student, który zaliczył przedmiot	Odniesienie do kierunkowych efektów uczenia się
w zakresie WIEDZY zna i rozumie:		
W01	definicje i twierdzenia z zakresu teorii liczb	MAT2A_W02
W02	aktualne kierunki rozwoju obliczeniowej teorii liczb	MAT2A_W03

W03	w pogłębionym stopniu co najmniej jeden pakiet oprogramowania służący do obliczeń symbolicznych	MAT2A_W05
w zakresie UMIEJĘTNOŚCI potrafi:		
U01	stosować metody algebraiczne w rozwiązywaniu problemów i zadań praktycznych z zakresu teorii liczb	MAT2A_U10
U02	wykorzystywać wybrany program komputerowy do analizy danych	MAT2A_U15
U03	samodzielnie wyszukiwać informacje, także w językach obcych	MAT2A_U13
w zakresie KOMPETENCJI SPOŁECZNYCH jest gotów do:		
K01	planowania swoją pracę i krytycznej oceny stopnia jej zaawansowania	MAT1A_K01

4.4. Sposoby weryfikacji osiągnięcia przedmiotowych efektów uczenia się						
Efekty przedmiotowe (symbol)	Sposób weryfikacji (+/-)					
	Zaliczenie pisemne		Kolokwium		Zadania domowe	
	Forma zajęć		Forma zajęć		Forma zajęć	
	W	C	W	C	W	C
W01	+					
W02	+					
W03	+					
U01				+		+
U02				+		+
U03						+
K01						+

4.5. Kryteria oceny stopnia osiągnięcia efektów uczenia się		
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/	45
Udział w wykładach	15
Udział w ćwiczeniach laboratoryjnych	30
SAMODZIELNA PRACA STUDENTA /GODZINY NIEKONTAKTOWE/	55
Przygotowanie do wykładu	10
Przygotowanie do ćwiczeń laboratoryjnych	30
Przygotowanie do egzaminu/kolokwium	15
ŁĄCZNA LICZBA GODZIN	100
PUNKTY ECTS za przedmiot	4

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

.....