

.....

KARTA INFORMACYJNA PRZEDMIOTU

Nazwa przedmiotu	Elementy teorii liczb		Elements of Number Theory				
Kod przedmiotu	WCYKWSM						
Język wykładowy	polski						
Profil studiów	ogólnoakademicki						
Forma studiów	studia stacjonarne						
Poziom studiów	wojskowe studia jednolite magisterskie						
Rodzaj przedmiotu							
Obowiązuje od naboru	2021/2022						
Forma zajęć, liczba godzin/rygor, razem godz., pkt ECTS	semestr	(x egzamin, + zaliczenie, # projekt)					punkty ECTS
		razem	wykłady	ćwiczenia	laboratoria	projekt	seminarium
	IV	30+	16	14+			2.0
	razem		16	14			2.0
Przedmioty wprowadzające	● Brak przedmiotów kształcenia wprowadzających						
Semestr/kierunek studiów	semestr 4 / Kryptologia i cyberbezpieczeństwo / wszystkie specjalności						
Autor	dr Robert Dryło, dr inż. Jarosław Łazuka						
Jednostka odpowiedzialna za przedmiot	Instytut Matematyki i Kryptologii, Wydział Cybernetyki						
Skrócony opis przedmiotu	● wykład ● ćwiczenia						
Pełny opis przedmiotu (treści programowe)	lp.	Semestr IV temat/tematyka zajęć	wkł.	ćw.	lab.	prj.	sem.
	1	Pierścienie euklidesowe, rozszerzony algorytm Euklidesa, podstawowe twierdzenia arytmetyki, jednoznaczność rozkładu w dziedzinie ideałów głównych, zastosowania nad $\mathbb{Z}$ i w pierścieniu wielomianów $K[x]$ nad ciałem K .	2	2			
	2	Podstawowe własności kongruencji, arytmetyka modularna, chińskie twierdzenie o resztach w dziedzinie ideałów głównych.	3	2			
	3	Własności funkcji Eulera, twierdzenie Eulera, małe twierdzenie Fermata, kryptosystem RSA.	2	2			
	4	Rozszerzenia ciał skończonych, stopień rozszerzenia, elementy algebraiczne, bazy ciała skończonego. ro Wielomiany nad ciałami skończonymi. Generowanie i rozszerzenia ciał skończonych.	2	2			
	5	Reszty kwadratowe, symbole Legendrea i Jacobiego, kryptosystem Rabina.	2	2			
	6	Twierdzenia i hipotezy dotyczące liczbach pierwszych, testy pierwszości Fermata, Solovaya-Strassena, Millera-Rabina.	1				
	7	Ułamki łańcuchowe. Funkcje arytmetyczne.	2	1			
	8	Przykłady równań difantycznych, trójki pitagorejskie, równanie Pella.	2	1			
	9	Praca kontrolna.		2			
		Razem	16	14			
Literatura	podstawowa: ● N. Koblitz Wykłady z teorii liczb i kryptografii. WNT, 2006 ● J. Gawinecki, J. Szmidt, Zastosowanie ciał skończonych i krzywych eliptycznych w kryptografii. WAT, 2002 ● Song Y. Yan, Teoria liczb w informatyce. PWN, 2006 uzupełniająca: ● W. Sierpiński, Teoria liczb, 1950 ● K. H. Rosen, Elementary number theory and its applications, Addison-Wesley, 1993						

Efekty uczenia się	Symbol	Efekty kształcenia	odniesienie do efektów kształcenia dla kierunku	
	W02	zna i rozumie w rozszerzonym zakresie problematykę wybranych działów matematyki, niezbędną do rozumienia i studiowania przedmiotów kierunkowych oraz analizowania, modelowania, konstruowania i eksploatacji systemów informatycznych, w tym: symbole, podstawowe pojęcia, określenia i twierdzenia logiki, teorii mnogości, algebry z geometrią, analizy matematycznej, matematyki dyskretnej, optymalizacji, probabilistyki i matematycznych podstaw kryptologii	K_W02	
	W22	zna i rozumie pojęcia, zasady i metody z zakresu teorii liczb i matematycznych podstaw i koncepcji kryptologii	K_W22	
	U03	umie posługiwać się językiem matematyki wykorzystując właściwe symbole, określenia i twierdzenia oraz umie formułować i rozwiązywać problemy metodami matematycznymi	K_U03	
Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez studenta zakładanych efektów uczenia się)	• Zaliczenie przedmiotu i ćwiczeń na podstawie kolokwium. • Warunkiem zaliczenia przedmiotu jest zaliczenie ćwiczeń			
Bilans ECTS (nakład pracy studenta)	SEMESTR 4			
	Aktywność	Obciążenie studenta		
		Liczba godzin	Liczba ECTS	
	Udział w wykładach	16	1	
	Udział w laboratoriach	0	0	
	Udział w ćwiczeniach	14	1	
	Udział w projektach	0	0	
	Udział w seminariach	0	0	
	Samodzielne studiowanie tematyki wykładów	16		
	Samodzielne przygotowanie do laboratoriów			
	Samodzielne przygotowanie do ćwiczeń	14		
	Samodzielna realizacja projektu			
	Samodzielne przygotowanie do seminariów			
	Udział w konsultacjach			
	Przygotowanie do egzaminu			
	Przygotowanie do zaliczenia	2		
	Udział w egzaminie / kolokwium	2		
	Sumaryczne obciążenie pracą studenta	64	2	
	Zajęcia z udziałem nauczycieli	32	2	
	Zajęcia powiązane z działalnością naukową	60	2	
	Zajęcia o charakterze praktycznym	28		

autorzy

**kierownik jednostki organizacyjnej
odpowiedzialnej za przedmiot**

dr Robert Dryło

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr hab. Koidecki Marek

tytuł, stopień naukowy, imię, NAZWISKO, podpis

dr inż. Jarosław Łazuka

tytuł, stopień naukowy, imię, NAZWISKO, podpis