Studijski program	Vrsta studija (ciklus)	Treći ciklus
	Naziv studijskog programa	Prirodne i matematičke nauke u obrazovanju

PREDMET

Naziv predmeta	**Algoritamska teorija brojeva**

Šifra predmeta	Semestar	Status predmeta	ECTS bodovi	Kontakt sati
	III	Izborni	10	

Obavezni prethodno položeni predmeti	

Nastavnici i saradnici	Nosilac predmeta	Doc.dr. Almasa odžak
	Učesnici u nastavi	

Ciljevi predmeta	Teoriju brojeva oduvijek odlikuje to da neki izazovni problemi čija formulacija je i nematematičarima lako razumljiva, tokom veoma dugog razoblja odolijevaju intenzivnim naporima usmjerenim na nalaženje njhova rješenja. U tom procesu, teorija brojeva je značajno utjecala i utječe na razvoj mnogih matematičkih disciplina. Nekoliko epohalnih dostignuća tokom posljednjih desetljeća, s jedne strane, kao i neslućeno veliko područje primjena s druge, uvišestručili su interes matematičara za istraživanja u ovoj oblasti. Program predmeta je struktuiran tako da doktorantima pruži uvid u neka od aktualnih područja algoritamske teorije brojeva. Izbor naprednih tema za produbljeno razmatranje ovisiće od iskazanog interesa učesnika.

Sadržaj predmeta

#	Nastavna jedinica	Kontakt sati			
		P	V	S	K
	• Teorija brojeva i kompleksnost. • Najveći zajednički djelilac; Euklidov algoritam za NZD; Analiza najkompleksnijih slučajeva; • Binarni NZD algoritam; Neprekidni razlomci; • Modularni račun; Kineski teorem o ostacima; Kvadratni ostaci; Računanje Legendreovog i Jakobievog simbola; • Rješavanje jednačina nad konačnim poljima; Korijeni; Henselova lema; • Algoritmi za određivanje prostih brojeva; Testovi prostosti za brojeve specijalnog oblika; Pseudoprosti i Carmichaelovi brojevi; Vjerovatnosni testovi prostosti; Testovi prostosti pomoću sita; Konstrukcija "slučajnih" prostih brojeva; Algoritmi za faktorizaciju brojeva.	30	30		

OPTEREĆENJE STUDENTA (sati)

Kontakt sati		Laboratorijske vježbe				Priprema ispita	
Literatura – čitanje		Pisani radovi		Ostalo (navesti)		UKUPNO	

LITERATURA	PROVJERA ZNANJA I OCJENJIVANJE			
1. Eric Bach and Jeffrey Shallit: Algorithmic Number Theory, Volume I: Efficient Algorithms, MIT Press, August 1996 2. Yan, Song Y.: Number Theory for Computing, 2nd ed., 2002, Springer Verlag 3. H. Cohen: A Course in Computational Number Theory (Corrected Third Printing), Graduate Texts in Mathematics 138, Springer 1996		Kriterij	Poeni	Uslov
	1.	Testovi tokom kursa	25	13
	2.	Seminarski rad	25	12
	3.	Završni ispit	50	30
	U k u p n o		100	55