Studijski program	Vrsta studija (ciklus)	III ciklus
	Naziv studijskog programa	Matematičke nauke u jugoistočnoj Evropi

PREDMET				
Naziv predmeta	**Algoritamska teorija brojeva**			
Šifra predmeta	Semestar	Status predmeta	ECTS	Kontakt sati
PMAT 605		izborni	10	30
Cilj predmeta	Teoriju brojeva oduvijek odlikuje to da neki izazovni problem čija formulacija je i nematematičarima lahko razumljiva, tokom veoma dugog razoblja odolijevaju intenzivnim naporima usmjerenim na nalaženje njihovog 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. Dio teorije brojeva koji se bavi proučavanjem algoritama kojima se rješavaju problemi teorije brojeva je algoritamska teorija brojeva. Cilj kursa je dati uvid problematiku ove naučne discipline.			

SADRŽAJ PREDMETA

- Algoritmi elementarne teorije brojeva
- Primjene algoritamske linearne algebre u teroiji brojeva
- Osnovni zadaci kompjutacione algebarske teorije brojeva
- Primjene u kriptografiji
- Testovi prostosti i faktorizacija
- Kompjutacioni problemi u teoriji sa nejedinstvenom faktorizacijom i suma-nula teoriji
- Nedavna dostignuća

LITERATURA

[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., Springer Verlag, 2002.

[3] H. Cohen: A Course in Computational Number Theory, Graduate Texts in Mathematics 138, Springer-Verlag, Berlin, 1993.

GRADING

Kriterij		Poeni	Uslov
1.	Zadaće	20	11
2.	Projekt	40	22
3.	Završni ispit	40	22
Ukupno		100	55