Sveučilište u Rijeci • University of Rijeka
Trg braće Mažuranića 10 • 51 000 Rijeka • Croatia
T: (051) 406-500 • F: (051) 216-671; 216-091
W: www.uniri.hr • E: ured@uniri.hr

Opće informacije		
Nositelj predmeta	doc. dr. sc. Ana Jurasić	
Naziv predmeta	Teorija brojeva	
Studijski program	Diplomski studij Fizika i matematika	
Status predmeta	Obvezatan	
Godina	2.	
Bodovna vrijednost i način izvođenja nastave	ECTS koeficijent opterećenja studenata	6
	Broj sati (P+V+S)	30 + 30 + 0

OPIS PREDMETA
Ciljevi predmeta
Teorija brojeva je područje matematike koje je svojim jednostavno iskazanim, ali vrlo teškim problemima (od kojih su neki rješavani ili se rješavaju stoljećima) oduvijek bilo motivacija i pokretač čitave matematike. U rješavanju tih problema primjenjuju se najnovija saznanja iz algebre, analize i geometrije. Osnovni cilj kolegija jest upoznati studente s načinima razmišljanja i dokazivanja tvrdnji u teoriji brojeva, a posebno upoznati algebarske i analitičke metode u teoriji brojeva. U tu je svrhu u okviru kolegija potrebno: analizirati osnovna svojstva cijelih brojeva: djeljivost, proste brojeve, rastav broja na proste faktore, Euklidov algoritam, kongruencije, opisati rješenja kvadratne kongruencije koristeći Legendreov simbol te usporediti takve kongruencije kroz kvadratni zakon reciprociteta, analizirati kvadratne forme i prikazivost cijelih brojeva kvadratnim formama, a posebno usporediti prikazivost cijelih brojeva kao sume određenog broja potpunih kvadrata, definirati aritmetičke funkcije i usporediti osnovne primjere, razlikovati osnovne tipove diofantskih jednadžbi i opisati načine njihova rješavanja, definirati eliptičke krivulje, analizirati njihova svojstva i primjene u teoriji brojeva, primijeniti teoriju brojeva u kriptografiji javnog ključa, ukratko opisati algebarske metode teorije brojeva te njihovu primjenu, ukratko opisati analitičke metode teorije brojeva te njihovu primjenu.
Uvjeti za upis predmeta
Očekivani ishodi učenja za predmet
Nakon odslušanog predmeta i položenog ispita studenti će: analizirati osnovna svojstva cijelih brojeva te argumentirano primijeniti ta svojstva na jednostavne probleme u teoriji brojeva vezane uz djeljivost i algoritme djeljivosti (A6, B7, D6, E6, F6), računati koristeći modularnu aritmetiku, rješavati kongruencijske jednadžbe te sustave kongruencija (A7, B7, D6, E6, F6), argumentirano primijeniti kvadratni zakon reciprociteta i formule za računanje Legendreovog simbola na rješavanje kvadratnih kongruencija (A6, B7, D6, E6, F6), opisati prikazivost cijelih brojeva kvadratnim formama u jednostavnijim slučajevima te argumentirano usporediti i klasificirati različite kvadratne forme (A6, B7, D6, E6, F6), prikazati i analizirati osnovne multiplikativne funkcije i njihova svojstva te argumentirano provjeriti i prezentirati veze među njima (A6, B6, D6, E6, F6), definirati osnovne tipove diofantskih jednadžbi i argumentirano opisati načine njihova rješavanja (A6, B7, D6, E6, F6), definirati eliptičke krivulje, analizirati njihova osnovna svojstva te opisati važne otvorene probleme (A6, B6, D6, E6, F6), argumentirano primijeniti metode teorijie brojeva u analizi kriptosustava s javnim ljučem (A7, B7, D6, E6, F6), opisati i analizirati algebarske i analitičke metode u teoriji brojeva te ih argumentirano primijeniti na važne probleme teorije brojeva (A6, B6, D6, E6, F6).
Sadržaj predmeta

Djeljivost. Najveći zajednički djelitelj. Euklidov algoritam. Prosti brojevi. Kongruencije. Eulerov teorem. Kineski teorem o ostacima. Primitivni korijeni i indeksi. Kvadratni ostaci. Legendreov simbol. Kvadratni zakon reciprociteta. Svojstva djeljivosti Fibonaccijevih brojeva. Kvadratne forme. Redukcija binarnih kvadratnih formi. Sume dva i četiri kvadrata. Aritmetičke funkcije. Eulerova i Möbiusova funkcija. Distribucija prostih brojeva. Diofantske jednadžbe. Linearne diofantske jednadžbe. Pitagorine trojke. Pellova jednadžba. Eliptičke krivulje. Primjena teorije brojeva u kriptografiji javnog ključa.		
Vrste izvođenja nastave	☒predavanja ☐seminari i radionice ☒vježbe ☒obrazovanje na daljinu ☐terenska nastava	☒samostalni zadaci ☒multimedija i mreža ☐laboratorij ☐mentorski rad ☐ostalo
Komentari		

Obveze studenata

Studenti su obavezni prisustvovati nastavi, aktivno sudjelovati u svim oblicima nastave, ostvariti određen broj bodova kroz semestar te položiti završni ispit (detalji će biti prikazani u izvedbenom planu predmeta).

Praćenje[18] rada studenata

Pohađanje nastave i aktivnost u nastavi			2.1	Seminarski rad		Eksperimentalni rad	
Pismeni ispit	1	Usmeni ispit	1	Esej		Istraživanje	
Projekt		Kontinuirana provjera znanja	1.9	Referat		Praktični rad	
Portfolio							

Ocjenjivanje i vrednovanje rada studenata tijekom nastave i završnom radu

Rad studenta na predmetu će se vrednovati i ocjenjivati tijekom nastave (npr. kolokviji, provjere, seminari, online testovi, domaće zadaće itd.) i na završnom ispitu.
Ukupan broj bodova koje student može ostvariti tijekom nastave je 70. Završni ispit se boduje s maksimalno 30 bodova.
Detaljna razrada načina praćenja i ocjenjivanja rada studenata bit će prikazana u izvedbenom planu predmeta.

Obvezna literatura (u trenutku prijave prijedloga studijskog programa)

Baker: A Concise Introduction to the Theory of Numbers, Cambridge University Press, Cambridge, 1994.
Dujella A., Maretić M.: Kriptografija, Element, Zagreb, 2007.
Niven, H. S. Zuckerman, H. L. Montgomery: An Introduction to the Theory Numbers, Wiley, New York, 1991.

Dopunska literatura (u trenutku prijave prijedloga studijskog programa)

K. H. Rosen: Elementary Number Theory and Its Applications, Addison-Wesley, Reading, 1993.
K. Chandrasekharan: Introduction to Analytic Number Theory, Springer-Verlag, Berlin, 1968.
H. E. Rose: A Course in Number Theory, Oxford University Press, 1995.
W. M. Schmidt: Diophantine Approximation, Springer-Verlag, Berlin, 1996.
B. Pavković, D. Veljan: Elementarna matematika 2, Školska knjiga, Zagreb, 1995.

Broj primjeraka obvezne literature u odnosu na broj studenata koji trenutno pohađaju nastavu na predmetu

Naslov	Broj primjeraka	Broj studenata

Načini praćenja kvalitete koji osiguravaju stjecanje izlaznih znanja, vještina i kompetencija

U zadnjem tjednu nastave provodit će se anonimna anketa u kojoj će studenti evaluirati kvalitetu održane nastave. Na kraju semestra provest će se analiza uspješnosti studenata na održanim ispitima u tom semestru.

[18] VAŽNO: Uz svaki od načina praćenja rada studenata unijeti odgovarajući udio u ECTS bodovima pojedinih aktivnosti tako da ukupni broj ECTS bodova odgovara bodovnoj vrijednosti predmeta. Prazna polja upotrijebiti za dodatne aktivnosti.