SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

Sveučilište u Rijeci •Odjel za matematiku
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
http://www.math.uniri.hr• e-adresa: math@math.uniri.hr

DETALJNI IZVEDBENI NASTAVNI PLAN PREDMETA

Opće informacije		
Naziv predmeta	**Teorija brojeva**	
Studijski program	Diplomski studij Diskretna matematika i primjene	
Godina	2.	
Status predmeta	Obvezatan	
Web stranica predmeta	Merlin	
Mogućnost izvođenja nastave na engleskom jeziku	Prema potrebi	
Bodovna vrijednost i način izvođenja nastave	***ECTS koeficijent opterećenja studenata***	**6**
	Broj sati (P+V+S)	30+30+0
Nositelj predmeta	***Ime i prezime***	**dr. sc. Ana Jurasić, docent**
	Ured	O-304
	Vrijeme za konzultacije	Prema potrebi i dogovoru e-mailom
	Telefon	584-662
	e-adresa	ajurasic@math.uniri.hr
Suradnici na predmetu	***Ime i prezime***	**-**
	Ured	
	Vrijeme za konzultacije	
	Telefon	
	e-adresa	

1. OPIS PREDMETA

1.1. 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, prosti brojevi, 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 te analizirati 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.

1.2. Korelativnost i korespondentnost predmeta

Nema uvjeta za upis predmeta. Predmet je u korelaciji s kolegijima Elementarna matematika 2 i Teorija kodiranja i kriptografija.

1.3. Očekivani ishodi učenja za predmet

Očekuje se da će nakon odslušanog kolegija i položenog ispita studenti razviti sljedeće:

- opće kompetencije:
  - sposobnost analiziranja osnovnih svojstava cijelih brojeva te argumentirane primjene tih svojstva na jednostavne probleme u teoriji brojeva vezane uz djeljivost i kongruencije,
  - sposobnost analiziranja osnovnih aritmetičkih funkcija i njihovih svojstva te argumentirane provjere veza među njima,
  - znanje o osnovnim tipovima diofantskih jednadžbi i sposobnost argumentiranog opisivanja načina njihova rješavanja,
- specifične kompetencije:
  - sposobnost rješavanja kongruencijskih jednadžbi te sustava kongruencija,
  - sposobnost argumentirane primjene kvadratnog zakona reciprociteta i formule za računanje Legendreovog simbola na rješavanje kvadratnih kongruencija,
  - mogućnost opisivanja prikazivosti cijelih brojeva kvadratnim formama u jednostavnijim slučajevima te argumentiranog uspoređivanja različitih kvadratnih formi,
  - znanje o eliptičkim krivuljama, sposobnost analiziranja njihovih osnovnih svojstva te poznavanje važnih otvorenih problema,
  - sposobnost argumentirane primjene metoda teorije brojeva u analizi kriptosustava s javnim ključem,
  - znanje i sposobnost analiziranja algebarskih metoda u teoriji brojeva te sposobnost njihove argumentirane primjene na važne probleme teorije brojeva,
  - znanje i sposobnost analiziranja analitičkih metoda u teoriji brojeva te sposobnost njihove argumentirane primjene na važne probleme teorije brojeva.

1.4. Okvirni 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.
Kriptografija. Primjena teorije brojeva u kriptografiji javnog ključa.

1.5. Vrste izvođenja nastave	☒predavanja ☐seminari i radionice ☒vježbe ☒e-učenje ☐ terenska nastava ☐ praktična nastava ☐ praktikumska nastava	☒samostalni zadaci ☒ multimedija i mreža ☐ laboratorijski rad ☐ projektna nastava ☐ mentorski rad ☒konzultativna nastava ☐ ostalo _____
1.6. Komentari	-	

1.7. Oblici praćenja studenata i način vrednovanja rada studenata tijekom nastave

Tijekom semestra prate se i boduju nazočnost na nastavi, kvaliteta aktivnog sudjelovanja u nastavi, domaće zadaće, kolokviji i programski zadaci. Na završnom ispitu se pismeno ili usmeno (ovisi o broju studenata) provjerava poznavanje i razumijevanje sadržaja obrađenog na predavanjima.

KOLOKVIJI

- Tijekom semestra biti će zadana dva pismena kolokvija sa zadacima iz teorije brojeva.
- Svaki kolokvij traje 120 minuta i održava se u unaprijed dogovorenom terminu.
- Ukupan **maksimalni broj bodova iz kolokvija je 40** (20+20).

DOMAćE ZADAćE

- Tijekom semestra zadaju se svakom studentu po dvije domaće zadaće sa zadacima iz teorije brojeva.
- Domaće zadaće se objavljuju i na web stranicama kolegija.
- Studenti su dužni riješiti domaće zadaće i na vrijeme ih predati nastavniku. Vrijeme predviđeno za rješavanje domaće zadaće je tjedan dana.
- Ukupan **maksimalan broj bodova iz domaćih zadaća je 10** (5+5).

PROGRAMSKI ZADACI

- Dva puta tijekom semestra se zadaju programski zadaci koje studenti rješavaju ukoliko žele.
- Programski zadaci se objavljuju i na web stranicama kolegija.
- Svaka skupina programskih zadataka se sastoji od dva zadatka i boduje se s po maksimalno 5 bodova.
- Studenti rješavaju zadane programske zadatke u dogovorenom programskom jeziku unutar tjedan dana i, ukoliko predaju rad, u mogućnosti su ostvariti bodove.
- Rješavanjem programskih zadataka moguće je ostvariti **maksimalno 10 bodova**.

AKTIVNO SUDJELOVANJE U NASTAVI

- Student je dužan redovno i aktivno sudjelovati u nastavi.
- Aktivno sudjelovanje na predavanjima uključuje pažljivo praćenje nastave i uključivanje u razgovor o pojedininim temama.
- Tijekom semestra na predavanjima će biti dana dva kratka testa znanja u svrhu provjere praćenja i razumijevanja gradiva obrađenog na predavanjima.
- Testovi će se sastojati od kraćih teorijskih pitanja i pitanja vezanih uz jednostavniju primjenu.
- Testovima znanja moguće je ostvariti **maksimalno 10 bodova** (5+5).

Na vježbama će studenti aktivno stjecati znanje svojim sudjelovanjem u rješavanju zadataka.

2. SUSTAV OCJENJIVANJA

2.1. Ocjenjivanje i vrednovanje rada studenata tijekom nastave te način polaganja ispita

Rad studenta na predmetu će se vrednovati i ocjenjivati tijekom nastave i na završnom ispitu. **Ukupan broj bodova koje student može ostvariti tijekom nastave je 70** (ocjenjuju se opisane aktivnosti studenata). Kroz sve oblike kontinuiranog praćenja i vrednovanja studenata tijekom nastave treba ukupno skupiti barem 50% ocjenskih bodova da bi se moglo pristupiti ispitu. Također, student mora ispuniti minimalne uvjete za pristup ispitu. Na ispitu je moguće ostvariti **maksimalno 30 bodova.** Prag prolaznosti na završnom ispitu je 50% uspješno riješenog ispita. Ispit se polaže kao pisana ili usmena provjera znanja.

SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

Sveučilište u Rijeci •Odjel za matematiku
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
http://www.math.uniri.hr• e-adresa: math@math.uniri.hr

Studenti koji tijekom nastave ostvare od 0% do 49,9% ocjenskih bodova koje je bilo moguće steći kroz oblike kontinuiranog praćenja i vrednovanja studenata ocjenjuju se ocjenom F (neuspješan), ne mogu steći ECTS bodove i moraju ponovno upisati predmet. Isto vrijedi i za studente koji u tri ponuđena ispitna roka ne polože završni ispit.

2.2. Minimalni uvjeti za pristup ispitu

AKTIVNOST KOJA SE BODUJE	MINIMALNI BROJ BODOVA
kolokviji	20
UKUPNO:	35 (tijekom nastave potrebno je skupiti 50% od mogućeg broja bodova te ostvariti minimalni uvjet na broj bodova iz kolokvija)
OSTALI UVJETI:	-

2.3. Formiranje konačne ocjene

Na temelju ukupnog zbroja ocjenskih bodova stečenih tijekom nastave i na završnom ispitu određuje se konačna ocjena prema sljedećoj raspodjeli:

OCJENA	BODOVI
5 (A)	od 90 do 100 ocjenskih bodova
4 (B)	od 75 do 89,9 ocjenskih bodova
3 (C)	od 60 do 74,9 ocjenskih bodova
2 (D)	od 50 do 59,9 ocjenskih bodova
1 (F)	od 0 do 49,9 ocjenskih bodova

3. LITERATURA

3.1. Obvezna literatura

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

3.2. Dodatna literatura

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

4. DODATNE INFORMACIJE O PREDMETU

4.1. Pohađanje nastave

Studenti smiju izostati s najviše 30% predavanja i s najviše 30% vježbi te su dužni informirati se o nastavi s koje su izostali. Ne tolerira se nikakakav oblik remećenja nastave te korištenje mobitela za vrijeme nastave.

4.2. Način informiranja studenata

Svi relevantni podaci i obavijesti o kolegiju bit će objavljeni u okviru online kolegija. Osobna odgovornost studenta je biti redovito informiran.

4.3. Ostale relevantene informacije

Od studenata se očekuje visok stupanj samostalnosti i odgovornosti u radu. Tijekom rada na kolegiju poticat će se aktivni pristup učenju.

Prilikom izrade zadataka predviđenih planom i programom kolegija studenti se ne smiju služiti tuđim tekstom

kao svojim. Svako neovlašteno preuzimanje tuđega teksta bez navođenja izvora smatra se intelektualnom krađom i podložno je sankcijama predviđenim važećim aktima! Uratke koje studenti budu slali putem sutava Merlin trebaju pripremiti prema uputi koju će dobiti na nastavi.
4.4. Način praćenja kvalitete i uspješnosti izvedbe predmeta
Kvaliteta održane nastave prati se u skladu s aktima Odjela za matematiku i Sveučilišta u Rijeci. Krajem semestra provodit će se anonimna anketa u kojoj će studenti evaluirati kvalitetu održane nastave iz ovog predmeta. Nakon završetka semestra provest će se analiza uspješnosti studenata iz ovog predmeta.
4.5. Ispitni rokovi

Zimski	• 3.2.2020. u 11:00 sati • 17.2.2020. u 11:00 sati
Proljetni izvanredni	9.3.2020. u 14:00 sati

5. SATNICA IZVOĐENJA NASTAVE I ODRŽAVANJA KOLOKVIJA U AKADEMSKOJ GODINI 2019/2020.

DATUM	*VRIJEME*	*OBLIK NASTAVE*	*NAZIV TEME*	*GRUPA*	*PROSTORIJA*
1.10.2019.	12:15-13:45	P	Djeljivost. Najveći zajednički djelitelj. Euklidov algoritam. Prosti brojevi. Jednoznačna faktorizacija.	Svi	O-335
2.10.2019.	8:15-9:45	AV	Djeljivost. Najveći zajednički djelitelj. Najmanja zajednička mjera. Euklidov algoritam i prošireni Euklidov algoritam, primjena. Prosti brojevi.	Svi	O-335
9.10.2019.	8:15-9:45	P	Kongruencije. Kineski teorem o ostacima. Eulerov teorem. Wilsonov teorem. Primitivni korijeni i indeksi.	Svi	O-335
15.10.2019.	12:15-13:45	AV	Kongruencije i primjene. Mali Fermatov teorem. Eulerov teorem. Wilsonov teorem. Kineski teorem o ostacima.	Svi	O-335
16.10.2018.	8:15-9:45	P	Kvadratni ostaci. Legendreov simbol. Kvadratni zakon reciprociteta.	Svi	O-335
22.10.2019.	12:15-13:45	AV	Kvadratni ostaci. Legendreov simbol i primjene. Jacobijev simbol i primjene. Kvadratni zakon reciprociteta.	Svi	O-335
23.10.2019.	8:15-9:45	P	Jacobijev simbol. Svojstva djeljivosti Fibonaccijevih brojeva.	Svi	O-335
29.10.2019.	12:15-13:45	AV	Jacobijev simbol. Svojstva djeljivosti Fibonaccijevih brojeva.	Svi	O-335
30.10.2019.	8:15-9:45	P	Kvadratne forme. Redukcija binarnih kvadratnih formi.	Svi	O-335
5.11.2019.	12:15-13:45	AV	Kvadratne forme. Redukcija binarnih kvadratnih formi. Ekvivalentne kvadratne forme.	Svi	O-335
6.11.2019.	8:15-9:45	P	Sume dva kvadrata. Sume četiri kvadrata.	Svi	O-335
12.11.2019.	12:15-13:45	AV	Sume dva kvadrata. Sume četiri kvadrata.	Svi	O-335
13.11.2019.	8:15-9:45	P	Diskriminanta kvadratne forme. Reprezentacija cijelog broja kvadratnom formom.	Svi	O-335
19.11.2019.	12:15-13:45	AV	Aritmetičke funkcije i primjena.	Svi	O-335

SVEUČILIŠTE U RIJECI
ODJEL ZA MATEMATIKU

Sveučilište u Rijeci •Odjel za matematiku
Radmile Matejčić 2 • 51 000 Rijeka • Hrvatska
T: (051) 584-650 • F: (051) 584-699
http://www.math.uniri.hr• e-adresa: math@math.uniri.hr

20.11.2019.	8:15-9:45	P	Distribucija prostih brojeva. Aritmetičke funkcije.	Svi	O-335
26.11.2019.	12:00-14:00	AV	**Prvi kolokvij.**	Svi	O-335
27.11.2019.	12:15-13:45	P	Linearne diofantske jednadžbe. Pitagorine trojke.	Svi	O-335
3.12.2019.	12:15-13:45	AV	Linearne diofantske jednadžbe. Pitagorine trojke. Primitivne Pitagorine trojke.	Svi	O-335
4.12.2019.	8:15-9:45	P	Pellove i pellovske jednadžbe.	Svi	O-335
10.12.2019.	12:15-13:45	AV	Pellove i pellovske jednadžbe.	Svi	O-335
11.12.2019.	8:15-9:45	P	Eliptičke krivulje i primjena.	Svi	O-335
17.12.2019.	12:15-13:45	AV	Eliptičke krivulje i primjena.	Svi	O-335
18.12.2019.	8:15-9:45	P	Ideja kriptosustava s javnim ključem. RSA kriptosustav.	Svi	O-335
7.1.2020.	12:15-13:45	AV	Ideja kriptosustava s javnim ključem. RSA kriptosustav.	Svi	O-335
8.1.2020.	8:15-9:45	P	Ostali kriptoustavi s javnim ključem.	Svi	O-335
14.1.2020.	12:15-13:45	AV	Ostali kriptoustavi s javnim ključem.	Svi	O-335
15.1.2020.	8:15-9:45	P	Testovi prostosti.	Svi	O-335
21.1.2020.	12:15-13:45	AV	Testovi prostosti i metode faktorizacije.	Svi	O-335
22.1.2020.	8:15-9:45	P	Metode faktorizacije.	Svi	O-335
28.1.2020.	12:00-14:00	AV	**Drugi kolokvij.**	Svi	O-335
29.1.2020.	8:15-9:45	P	Završno predavanje Popravne aktivnosti.	Svi	O-335

Moguća su manja odstupanja u realizaciji izvedbenog plana.

P – predavanja
AV – auditorne vježbe
VP – vježbe u praktikumu
MV – metodičke vježbe
S – seminari