SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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 KOLEGIJA

Opće informacije		
Naziv kolegija	**Teorija brojeva**	
Studijski program	Sveučilišni diplomski studij Diskretna matematika i primjene	
Godina	I.	
Status kolegija	Obvezatan	
Web stranica kolegija	https://moodle.srce.hr	
Mogućnost izvođenja nastave na engleskom jeziku	Da, prema potrebi	
Bodovna vrijednost i način izvođenja nastave	***ECTS koeficijent opterećenja studenata***	**6**
	Broj sati (P+V+S)	30+30+0
Nositelj kolegija	***Ime i prezime***	**Ana Jurasić**
	Ured	O-304
	Vrijeme za konzultacije	Prema potrebi i dogovoru e-mailom
	Telefon	584-662
	e-adresa	ajurasic@math.uniri.hr
Suradnici na kolegiju	***Ime i prezime***	-
	Ured	
	Vrijeme za konzultacije	
	Telefon	
	e-adresa	

1. OPIS PREDMETA

1.1. Ciljevi kolegija

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, matematičke 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 njihove 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,

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

- Ukratko opisati analitičke metode teorije brojeva te njihovu primjenu.

1.2. Korelativnost i korespondentnost kolegija

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 kolegij

Očekuje se da će nakon odslušanog kolegija i položenog ispita student moći:

I1. analizirati osnovna svojstava cijelih brojeva te ih argumentirano primijeniti na jednostavne probleme u teoriji brojeva vezane uz djeljivost i algoritme djeljivosti (A6, B7, D6, E6, F6),
I2. računati koristeći modularnu aritmetiku, rješavati kongruencijske jednadžbe te sustave kongruencija (A7, B7, D6, E6, F6),
I3. argumentirano primijeniti kvadratni zakon reciprociteta i formule za računanje Legendreovog simbola na rješavanje kvadratnih kongruencija (A6, B7, D6, E6, F6),
I4. opisati prikazivost cijelih brojeva kvadratnim formama u jednostavnijim slučajevima te argumentirano usporediti i klasificirati različite kvadratne forme (A6, B7, D6, E6, F6),
I5. prikazati i analizirati osnovne multiplikativne funkcije i njihova svojstva te argumentirano provjeriti i prezentirati veze među njima (A6, B6, D6, E6, F6),
I6. definirati osnovne tipove diofantskih jednadžbi i argumentirano opisati načine njihova rješavanja (A6, B7, D6, E6, F6),
I7. definirati eliptičke krivulje, analizirati njihova osnovna svojstva te opisati važne otvorene probleme (A6, B6, D6, E6, F6),
I8. argumentirano primijeniti metode teorije brojeva u analizi kriptosustava s javnim ključem (A7, B7, D6, E6, F6),
I9. opisati i analizirati algebarske i analitičke metode u teoriji brojeva te ih argumentirano primijeniti na važne probleme teorije brojeva (A6, B6, D6, E6, F6).

1.4. Okvirni sadržaj kolegija

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	Na vježbama će se rješavati zadaci, 50% u auditornom obliku, a 50% u računalnoj učionici, uz korištenje raspoložive programske podrške.	

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

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

KOLOKVIJI

- Tijekom semestra bit će zadana dva pismena kolokvija sa zadacima iz teorije brojeva.
- Svaki kolokvij traje 90 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 domaće zadaće sa zadacima iz teorije brojeva za samostalno rješavanje.
- Domaće zadaće se objavljuju i na web stranicama kolegija.
- Rješavanje zadataka iz domaćih zadaća provjerava se na vježbama dva puta u toku semestra. Detaljnije upute bit će dane na nastavi i u okviru online kolegija.
- Ukupan **maksimalan broj bodova iz domaćih zadaća je 10** (5+5).

PROGRAMSKI ZADACI

- Jednom u semestru zadaju se programski zadaci koje studenti rješavaju ukoliko žele.
- Programski zadaci objavljuju se i na web stranicama kolegija.
- Boduju se s **maksimalno 10 bodova**.
- Studenti rješavaju zadane programske zadatke u dogovorenom programskom jeziku i, ukoliko predaju rad u dogovrenom vremenu, u mogućnosti su ostvariti bodove.

TESTOVI NA PREDAVANJIMA

- Tijekom semestra na predavanjima će biti dana dva kratka testa znanja u svrhu provjere praćenja i razumijevanja gradiva obrađenog na predavanjima. Detaljnije upute bit će dane na nastavi i u okviru online kolegija.
- Testovi će se sastojati od kraćih teorijskih pitanja i pitanja vezanih uz jednostavniju primjenu.
- Testovima znanja moguće je ostvariti **maksimalno 10 bodova** (5+5).

U zadnjem tjednu nastave bit će organizirane **popravne aktivnosti** na kojima će studenti moći pisati jedan propušteni/lošije bodovani kolokvij. Na taj način stečeni bodovi zamjenjuju prethodno stečene bodove iz iste komponenete, bez obzira na ishod. S detaljima vezanim uz popravne aktivnosti studenti će biti upoznati na nastavi te kroz obavijesti na web stranicama kolegija.

1.8. Konstruktivno povezivanje

ISHODI UČENJA	SADRŽAJ	NASTAVNE AKTIVNOSTI	METODE VREDNOVANJA
I1	Djeljivost. Kongruencije. Kvadratni ostatci.	Kroz predavanja, auditorne vježbe, vježbe na računalima i samostalni rad, primjenjivat će se sljedeće metode učenja i poučavanja: metoda usmenog izlaganja, metoda demonstracija, metoda razgovora, metoda čitanja i rada na tekstu.	pisane provjere znanja, provjere znanja na računalu, usmena provjera znanja
I2	Kongruencije. Kvadratni ostatci. Kriptografija.		
I3	Kvadratni ostatci		
I4	Kvadratne forme		
I5	Aritmetičke funkcije		
I6	Diofantske jednadžbe		
I7	Eliptičke krivulje		
I8	Kriptografija		
I9	Cjelokupni sadržaj kolegija		

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

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% mogućih 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.

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/prolaznu ocjenu

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. Dujella: *Teorija brojeva*, Školska knjiga, Zagreb, 2019.
2. Baker: *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, Cambridge, 1994.
3. Dujella A., Maretić M.: *Kriptografija,* Element, Zagreb, 2007.

3.2. Dodatna literatura

1. I. Niven, H. S. Zuckerman, H. L. Montgomery: *An Introduction to the Theory of Numbers,* Wiley, New York, 1991.
2. K. H. Rosen: *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, 1993.
3. K. Chandrasekharan: *Introduction to Analytic Number Theory*, Springer-Verlag, Berlin, 1968.
4. H. E. Rose: *A Course in Number Theory*, Oxford University Press, Oxford, 1995.
5. W. M. Schmidt: *Diophantine Approximation,* Springer-Verlag, Berlin, 1996.
6. B. Pavković, D. Veljan: *Elementarna matematika 2*, Školska knjiga, Zagreb, 1995.

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

4. DODATNE INFORMACIJE O KOLEGIJU

4.1. Pohađanje nastave

Studenti 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 predmetu 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 rad ana predmetu, poticat će se aktivni pristup učenju.

Prilikom izrade zadataka predviđenih planom i programom predmeta 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 kolegija

Kvaliteta održane nastave prati se u skladu s aktima Fakulteta za matematiku i Sveučilišta u Rijeci. Krajem semestra provodit će se anonimna anketa u kojoj će studenti evaluirati kvalitetu održane nastave iz ovog kolegija. Nakon završetka semestra provest će se analiza uspješnosti studenata iz ovog kolegija.

4.5. Ispitni rokovi

Zimski	3.2.2025. u 9:00 17.2.2025. u 9:00
Izvanredni	10.3.2025. u 14:00
Jesenski	28.8.2025.

5. SATNICA IZVOĐENJA NASTAVE U AKADEMSKOJ GODINI 2024/2025.

DATUM	*VRIJEME*	*OBLIK NASTAVE*	*NAZIV TEME*	*GRUPA*	*PROSTORIJA*
1.10.2024.	10:15-11:45	P	Djeljivost. Najveći zajednički djelitelj. Euklidov algoritam. Prosti brojevi. Jednoznačna faktorizacija.	Svi	O-363
1.10.2024.	12:15-13:45	V	Djeljivost. Najveći zajednički djelitelj. Najmanja zajednička mjera. Euklidov algoritam i prošireni Euklidov algoritam, primjena. Prosti brojevi.	Svi	O-355
2.10.2024.	14:15-15:45	P	Kongruencije. Kineski teorem o ostacima. Eulerov teorem. Wilsonov teorem. Primitivni korijeni i indeksi.	Svi	O-355
4.10.2024.	8:15-9:45	V	Kongruencije i primjene. Mali Fermatov teorem. Eulerov teorem. Wilsonov teorem. Kineski teorem o ostacima.	Svi	O-355
8.10.2024.	10:15-11:45	P	Kvadratni ostaci. Legendreov simbol. Kvadratni zakon reciprociteta.	Svi	O-363
8.10.2024.	12:15-13:45	V	Kvadratni ostaci. Legendreov simbol i primjene. Jacobijev simbol i primjene. Kvadratni zakon reciprociteta.	Svi	O-355
9.10.2024.	14:15-15:45	P	Jacobijev simbol. Svojstva djeljivosti Fibonaccijevih brojeva.	Svi	O-355
11.10.2024.	8:15-9:45	V	Jacobijev simbol. Svojstva djeljivosti Fibonaccijevih brojeva.	Svi	O-355
29.10.2024.	12:15-13:45	P	Kvadratne forme. Redukcija binarnih kvadratnih formi.	Svi	O-355

SVEUČILIŠTE U RIJECI
FAKULTET ZA MATEMATIKU

Sveučilište u Rijeci •Fakultet 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

5.11.2024.	12:15-13:45	V	Kvadratne forme. Redukcija binarnih kvadratnih formi. Ekvivalentne kvadratne forme.	Svi	O-355
8.11.2024.	8:15-9:45	P	Sume dva kvadrata. Sume četiri kvadrata.	Svi	O-355
12.11.2024.	12:15-13:45	V	Sume dva kvadrata. Sume četiri kvadrata.	Svi	O-355
15.11.2024.	8:15-9:45	V	**Prvi kolokvij**	Svi	O-355
19.11.2024.	12:15-13:45	P	Aritmetičke funkcije.	Svi	O-355
22.11.2024.	8:15-9:45	V	Aritmetičke funkcije i primjena.	Svi	O-363
26.11.2024.	12:15-13:45	P	Distribucija prostih brojeva	Svi	O-355
29.11.2024.	8:15-9:45	P	Linearne diofantske jednadžbe. Pitagorine trojke.	Svi	O-363
3.12.2024.	12:15-13:45	P	Pellove i pellovske jednadžbe.	Svi	O-355
6.12.2024.	8:15-9:45	V	Linearne diofantske jednadžbe. Pitagorine trojke	Svi	O-363
10.12.2024.	12:15-13:45	P	Eliptičke krivulje i primjena	Svi	O-355
13.12.2024.	8:15-9:45	V	.Pellove i pellovske jednadžbe	Svi	O-363
17.12.2024.	12:15-13:45	P	Testovi prostosti i metode faktorizacije.	Svi	O-355
20.12.2024.	8:15-9:45	V	Eliptičke krivulje i primjena	Svi	O-363
24.12.2024.	12:15-13:45	P	Eliptičke krivulje i primjena	Svi	O-355
7.1.2025.	12:15-13:45	P	Ideja kriptosustava s javnim ključem. RSA kriptosustav.	Svi	O-355
10.1.2025.	8:15-9:45	V	Testovi prostosti i metode fakrizacije.	Svi	O-363
14.1.2025.	12:15-13:45	V	**Drugi kolokvij**	Svi	O-363
17.1.2025.	8:15-9:45	P	Ostali kriptoustavi s javnim ključem.	Svi	O-355
21.1.2025.	12:15-13:45	V	Ideja kriptosustava s javnim ključem. RSA kriptosustav.	Svi	O-355
24.1.2025.	8:15-9:45	V	Ostali kriptosustavi s javnim ključem.	Svi	O-363
31.1.2025.	8:15-9:45		**Popravne aktivnosti**		O-363

Moguća su manja odstupanja u realizaciji izvedbenog plana.
Do 40% planirane nastave može biti održano online.

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