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 KOLEGIJA

### *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 kolegija. Kolegij 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<br>☐ seminari i radionice<br>☒ vježbe<br>☐ e-učenje<br>☐ terenska nastava<br>☐ praktična nastava<br>☐ praktikumska nastava | ☒ samostalni zadaci<br>☒ multimedija i mreža<br>☐ laboratorijski rad<br>☐ projektna nastava<br>☐ mentorski rad<br>☐ konzultativna nastava<br>☐ 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*

**KOLOKVIJI**

- Tijekom semestra bit 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 50** (25+25).

**DOMAĆE ZADAĆE**

- Tijekom semestra zadaju se svakom studentu domaće zadaće sa zadacima iz teorije brojeva za samostalno rješavanje.
- Domaće zadaće se objavljuju i na mrežnim stranicama kolegija.
- Rješavanje zadataka iz domaćih zadaća provjerava se na vježbama dva puta tijekom semestra. Detaljnije upute bit će dane na nastavi i u okviru online kolegija.
- Ukupan **maksimalan broj bodova iz domaćih zadaća je 10** (5+5).

**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 komponente, 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 | | |

## 2. SUSTAV OCJENJIVANJA

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

Rad studenta na kolegiju 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 kolegij. 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 | 25 |
| **UKUPNO:** | **35**<br>(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.

## 4. DODATNE INFORMACIJE O KOLEGIJU

### *4.1. Pohađanje nastave*

Studenti su dužni informirati se o nastavi s koje su izostali. Ne tolerira se nikakav 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.

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

### *4.3. Ostale relevantne 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 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*** | **4.2.2026.** u 9:00<br>**18.2.2026.** u 9:00 |
| ***Izvanredni*** | **9.3.2026.** u 14:00 |
| ***Jesenski*** | **31.8.2026.** u 11:00 |

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. SATNICA IZVOĐENJA NASTAVE U AKADEMSKOJ GODINI 2025/2026.

| *DATUM* | *VRIJEME* | *OBLIK NASTAVE* | *NAZIV TEME* | *GRUPA* | *PROSTORIJA* |
|---|---|---|---|---|---|
| 2.10.2025. | 8:15-9:45 | P | Djeljivost. Prosti brojevi. | Svi | O-355 |
| 7.10.2025. | 8:15-9:45 | V | Djeljivost. Prosti brojevi. | Svi | O-355 |
| 9.10.2025. | 8:15-9:45 | P | Kongruencije. Eulerov teorem. Wilsonov teorem. Primitivni korijeni i indeksi. | Svi | O-355 |
| 14.10.2025. | 8:15-9:45 | V | Kongruencije i primjene. Mali Fermatov teorem. Eulerov teorem. Wilsonov teorem. | Svi | O-355 |
| 16.10.2025. | 8:15-9:45 | P | Kvadratni ostaci. Legendreov simbol. Kvadratni zakon reciprociteta. | Svi | O-355 |
| 21.10.2025. | 8:15-9:45 | V | Kvadratni ostaci. Legendreov simbol i primjene. Kvadratni zakon reciprociteta. | Svi | O-355 |
| 23.10.2025. | 8:15-9:45 | P | Jacobijev simbol. | Svi | O-355 |
| 28.10.2025. | 8:15-9:45 | V | Jacobijev simbol i primjene. | Svi | O-355 |
| 30.10.2025. | 8:15-9:45 | P | Kvadratne forme. Redukcija binarnih kvadratnih formi. | Svi | O-355 |
| 4.11.2025. | 8:15-9:45 | V | Kvadratne forme. Redukcija binarnih kvadratnih formi. Ekvivalentne kvadratne forme. | Svi | O-355 |
| 6.11.2025. | 8:15-9:45 | P | Sume dva kvadrata. Sume četiri kvadrata. | Svi | O-355 |
| 11.11.2025. | 8:15-9:45 | V | Sume dva kvadrata. Sume četiri kvadrata. | Svi | O-355 |
| 13.11.2025. | 8:15-9:45 | P | Aritmetičke funkcije. | Svi | O-355 |
| 20.11.2025. | 8:00-10:00 | V | **Prvi kolokvij** | Svi | O-355 |
| 25.11.2025. | 8:15-9:45 | P | Distribucija prostih brojeva. | Svi | O-355 |
| 27.11.2025. | 8:15-9:45 | V | Aritmetičke funkcije i primjena. | Svi | O-363 |
| 2.12.2025. | 8:15-9:45 | P | Linearne diofantske jednadžbe. Pitagorine trojke. | Svi | O-355 |
| 4.12.2025. | 8:15-9:45 | V | Linearne diofantske jednadžbe. Pitagorine trojke | Svi | O-363 |
| 9.12.2025. | 8:15-9:45 | P | Pellove i pellovske jednadžbe | Svi | O-355 |
| 11.12.2025. | 8:15-9:45 | V | Pellove i pellovske jednadžbe | Svi | O-363 |
| 16.12.2025. | 8:15-9:45 | P | Eliptičke krivulje i primjena | Svi | O-355 |
| 18.12.2025. | 8:15-9:45 | V | Eliptičke krivulje i primjena | Svi | O-363 |
| 23.12.2025. | 8:15-9:45 | P | Testovi prostosti i metode faktorizacije | Svi | O-355 |
| 8.1.2026. | 8:15-9:45 | V | Testovi prostosti i metode faktorizacije | Svi | O-363 |
| 13.1.2026. | 8:15-9:45 | P | Ideja kriptosustava s javnim ključem. RSA kriptosustav. | Svi | O-355 |
| 15.1.2026. | 8:00-10:00 | V | **Drugi kolokvij** | Svi | O-363 |
| 20.1.2026. | 8:15-9:45 | P | Ostali kriptoustavi s javnim ključem | Svi | O-355 |
| 22.1.2026. | 8:15-9:45 | V | Ideja kriptosustava s javnim ključem. RSA kriptosustav. | Svi | O-363 |
| 27.1.2026. | 8:00-10:00 | V | **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