M108	Obavezni 4. semestar	**Teorija brojeva**	P	S	V	ECTS
			2	0	2	6

Cilj predmeta. Cilj ovog predmeta je upoznati studente s osnovnim pojmovima, idejama i metodama elementarne teorije brojeva. Na predavanjima će se uvesti i obraditi osnovni pojmovi i rezultati teorije brojeva. Na primjerima će se pokazati primjene obrađenih rezultata, te će se ukazati na primjenu teorije brojeva u kriptografiji. Na vježbama će studenti svladavati tehnike rješavanja računskih i problemskih zadataka uz primjenu tvrdnji dokazanih na predavanju.

Potrebna predznanja. Elementarna matematika.

Sadržaj predmeta.

1. Djeljivost. Djeljivost cijelih brojeva i osnovna svojstva. Najveći zajednički djelitelj. Teorem o dijeljenju s ostatkom. Euklidov algoritam. Linearne diofantske jednadžbe.
2. Faktorizacija. Prosti brojevi. Osnovni teorem aritmetike. Broj i suma djelitelja prirodnog broja.
3. Kongruencije. Modularna aritmetika. Linearne kongruencije. Kineski teorem o ostatcima. Eulerov teorem. Wilsonov i Lagrangeov teorem. Primitivni korijeni i indeksi. Primjene kongruencija.
4. Kvadratni ostatci. Legendreov simbol. Gaussov zakon reciprociteta. Jacobijev simbol. Primjena Legendreovog i Jacobijevog simbola.
5. Gaussovi cijeli brojevi. Osnovna svojstva Gaussovih cijelih brojeva. Djeljivost i prosti elementi u skupu Gaussovih cijelih brojeva. Prikaz prirodnog broja u obliku sume dva kvadrata. Pitagorine trojke.
6. Verižni razlomci. Konačni i beskonačni razvoji u verižni razlomak. Razvoj kvadratnih iracionalnosti u verižni razlomak. Pellove i pellovske jednadžbe.

ISHODI UČENJA

R.b.	**ISHODI UČENJA**
1.	Koristiti svojstva djeljivosti i kongruencija u rješavanju zadataka.
2.	Prepoznavati osnovne aritmetičke funkcije.
3.	Nabrojati i primjenjivati osnovne teoreme teorije brojeva.
4.	Razumjeti ulogu teorije brojeva u kriptografiji.
5.	Prepoznavati svojstva Gaussovih cijelih brojeva.
6.	Rješavati neke tipove diofantskih jednadžbi.

POVEZIVANJE ISHODA UČENJA, ORGANIZACIJE NASTAVNOG PROCESA I PROCJENA ISHODA UČENJA

ORGANIZACIJA NASTAVNOG PROCESA	ECTS	ISHOD UČENJA **	AKTIVNOST STUDENATA*	METODA PROCJENE	BODOVI	
					Min	max
Pohađanje predavanja	1	1-6	Prisutnost na nastavi, rasprava, timski rad i samostalan rad na zadatcima	Potpisne liste, praćenje aktivnosti na nastavi	0	4
Provjera znanja (kolokvij)	2	1-6	Priprema za pismenu provjeru znanja	Provjera točnih odgovora (ocjenjivanje)	25	48
Završni ispit	3	1-6	Ponavljanje gradiva	Usmeni ispit	25	48
UKUPNO	6				50	100

Izvođenje nastave i vrednovanje znanja. Predavanja i vježbe su obavezne. Ispit se sastoji od pismenog i usmenog dijela, a polaže se nakon odslušanih predavanja i obavljenih vježbi. Prihvatljivi rezultati postignuti na kolokvijima, koje studenti pišu tijekom semestra, zamjenjuju pismeni dio ispita.

Može li se predmet izvoditi na engleskom jeziku: Da

Osnovna literatura:

1. I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, 2015.
2. A. Dujella, *Uvod u teoriju brojeva*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2002, skripta.

Dopunska literatura:

1. T. Andreescu, D. Andrica, *An Introduction to Diophantine Equations*, GIL Publishing House, 2002.
2. J. Stilwell, *Elements of number theory*, Springer, 2003.
3. A. Dujella, *Diofantske jednadžbe*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2007.
4. G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer, 2003.
5. K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, 1993.
6. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, 1994.
7. A. Dujella, M. Maretić, *Kriptografija*, Element, 2007.