M049	Obavezni 4. semestar	**Uvod u teoriju brojeva**	P+V+S 2+2+0	ECTS 6

Cilj predmeta. Teorija brojeva predstavlja najstariju i najrašireniju granu teorijske matematike, s brojnim primjenama. Cilj ovog predmeta je upoznati studente s osnovnim pojmovima, idejama i metodama elementarne teorije brojeva. Na predavanjima će se uvesti i obraditi osnovni pojmovi te pokazati njihova svojstva, uz brojne primjere i ilustrativne primjene, poput utjecaja teorije brojeva u kriptografiji. Na vježbama će studenti svladavati tehnike rješavanja računskih i problemskih zadataka te se osposobiti za rješavanje konkretnih problema.

Potrebna predznanja. Elementarna matematika I i II.

Sadržaj predmeta.

1. Djeljivost. Djeljivost cijelih brojeva i osnovna svojstva djeljivosti. Najveći zajednički djelitelj i Euklidov algoritam. Prosti brojevi. Broj i suma djelitelja cijelog broja. Fermatovi brojevi. Primjena djeljivosti na rješavanje diofantskih jednadžbi.
2. Kongruencije. Osnovna svojstva i rješavanje osnovnih kongruencija. Eulerov, mali Fermatov i Wilsonov teorem. Kineski teorem o ostatcima.
3. Primjena kongruencija. Linearne diofantske jednadžbe. Kriptosustavi. Transpozicijske šifre. RSA kriptosustav.
4. Kvadratni ostatci. Definicija i svojstva Legendreova simbola. Gaussov kvadratni zakon reciprociteta. Jacobijev simbol. Primjena na rješavanje diofantskih jednadžbi.
5. Gaussovi cijeli brojevi. Norma i djeljivost Gaussovih cijelih brojeva. Prikaz prirodnog broja u obliku sume dvaju kvadrata. Primjena Gaussovih cijelih brojeva u određivanju primitivnih Pitagorinih trojki.
6. Pellove i pellovske jednadžbe. Pojam Pellove jednadžbe i egzistencija rješenja. Dirichletov teorem o aproksimaciji. Generiranje rješenja Pellove jednadžbe i veza s verižnim razlomcima. Kriteriji rješivosti nekih pellovskih jednadžbi i algoritmi za njihovo rješavanje.

Očekivani ishodi učenja.

Očekuje se da nakon položenog kolegija studenti:

- klasificiraju diofantske jednadžbe te znaju riješiti jednostavnije tipove istih;
- ispituju temeljna svojstva djeljivosti cijelih brojeva;
- razlikuju kriptosustave i razumiju važnost teorije brojeva u kriptosustavima;
- prepoznaju svojstva Gaussovih cijelih brojeva;
- određuju rješenje Pellovih jednadžbi u danom intervalu.

Izvođenje nastave i vrednovanje znanja. Predavanja i vježbe su obavezne. Tijekom semestra putem kolokvija se provjerava znanje studenata. Uspješno položeni kolokviji zamjenjuju pismeni dio ispita. Nakon odslušanih predavanja i obavljenih vježbi polaže se ispit, koji se sastoji od pismenog i usmenog dijela. Studenti tijekom semestra mogu izraditi seminarski rad. Kvalitetno izrađen seminarski rad utječe na konačnu ocjenu predmeta.

Može li se predmet izvoditi na engleskom jeziku: Da

Osnovna literatura:

1. J. Stilwell, Elements of number theory, Springer, 2003
2. A. Dujella, Uvod u teoriju brojeva, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2002.

Dopunska literatura:

1. T. Andreescu, D. Andrica, An Introduction to Diophantine Equations, GIL Publishing House, 2002

2. A. Dujella, Diofantske jednadžbe, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2007.
3. N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, 1994
4. G. A. Jones, J.M. Jones, Elementary Number Theory, Springer, 2003
5. L. N. Childs, A Concrete Introduction to Higher Algebra, Springer Verlag, 1995