



Univerza v Mariboru

Fakulteta za naravoslovje  
in matematiko

### UČNI NAČRT PREDMETA / COURSE SYLLABUS

<b>Predmet:</b>	Teorija števil
<b>Course title:</b>	Number Theory

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester
Enovit magistrski študijski program druge stopnje Predmetni učitelj	/	2.	4.
Five-year master's degree program Subject Teacher	/		

**Vrsta predmeta / Course type**

**Univerzitetna koda predmeta / University course code:**

Predavanja Lectures	Seminar Seminar	Sem. vaje Tutorial	Lab. vaje Laboratory work	Teren. vaje Field work	Samost. delo Individ. work	ECTS
45		45			150	8

**Nosilec predmeta / Lecturer:**

**Jeziki / Predavanja / Lectures:**   
**Languages: Vaje / Tutorial:**

**Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:**   
**Prerequisites:**

**Vsebina:**

Deljivost celih števil. Največji skupni delitelj. Evklidov algoritem. Najmanjši skupni večkratnik. Linearne diofantske enačbe.

Praštevil. Osnovni izrek aritmetike.

Kongruence. Kriteriji deljivosti. Linearne kongruence. Kitajski izrek o ostankih. Reševanje polinomskih kongruenc. Wilsonov izrek. Fermatov mali izrek in psevdopraštevil. Eulerjev izrek.

Aritmetične funkcije. Multiplikativne funkcije. Möbiusova formula inverzije.

Red celega števila in primitivni koreni. Kvadratični zakon recipročnosti.

Pitagorejske trojke.

**Content (Syllabus outline):**

Divisibility of integers. Greatest common divisor. Euclidean algorithm. Least common multiple. Linear Diophantine equations.

Primes. Fundamental Theorem of Arithmetic.

Congruences. Special divisibility tests. Linear congruences. Chinese Remainder Theorem. Solving polynomial congruences. Wilson's Theorem. Fermat's Little Theorem and pseudoprimes. Euler's Theorem.

Arithmetic functions. Multiplicative functions. Möbius inversion.

The Order of an Integer and Primitive roots. The law of quadratic reciprocity.

Pythagorean Triples.

**Temeljni literatura in viri / Readings:**

D. M. Burton: Elementary Number Theory. New York [etc.] : McGraw-Hill, 1998.

K. H. Rosen: Elementary number theory and its applications. Boston: Pearson/Addison Wesley, cop. 2005.

J. Grasselli: Elementarna teorija števil. Ljubljana: DMFA, 2009.

J. Grasselli: Diofantske enačbe. Ljubljana: DMFA, 1984.

J. Grasselli: Osnove teorije števil. Ljubljana: DMFA, 1975.

**Cilji in kompetence:**

Proučiti temeljne koncepte in rezultate elementarne teorije števil.

**Objectives and competences:**

To study the fundamental concepts and results of elementary number theory.

**Predvideni študijski rezultati:**

Znanje in razumevanje pojmov in rezultatov elementarne teorije števil.

Prenesljive/ključne spretnosti in drugi atributi:

- Pridobljena znanja se dopolnjujejo z znanji s področja algebre, kombinatorike, kriptografije, teorije kodiranja, analize, računalništva, ...

**Intended learning outcomes:**

Knowledge and understanding of notions and results of elementary number theory.

Transferable/Key Skills and other attributes:

The obtained knowledge supplements with the knowledge of algebra, combinatorics, cryptography, coding theory, analysis, computer science, ...

**Metode poučevanja in učenja:**

- Predavanja
- Seminarske vaje
- Individualno delo

**Learning and teaching methods:**

- Lectures
- Tutorial
- Individual work

**Načini ocenjevanja:**Delež (v %) /  
Weight (in %)**Assessment:**

Izpit:	Delež (v %) / Weight (in %)	Exams:
Pisni izpit – problemi, Ustni izpit – teorija.	50% 50%	Written exam – problems, Oral exam – theory.
Vsaka izmed naštetih obveznosti mora biti opravljena s pozitivno oceno.		Each of the mentioned assessments must be assessed with a passing grade.
Opravljene pisni izpit – problemi je pogoj za pristop k ustnemu izpitu – Teorija.		Passing grade of written exam – problems is required to take the oral exam – theory.
Pisni izpit – problemi se lahko nadomesti z dvema delnima testoma (sprotne obveznosti).		Written exam – problems can be replaced with two mid-term tests.

**Reference nosilca / Lecturer's references:**

1. EREMITA, Daniel. Biderivations on tensor products of algebras. *Communications in algebra*, ISSN 0092-7872, 2018, vol. 46, iss. 4, str. 1722-1726. <http://doi.org/10.1080/00927872.2017.1355375>, doi: [10.1080/00927872.2017.1355375](https://doi.org/10.1080/00927872.2017.1355375).
2. EREMITA, Daniel. Commuting traces of upper triangular matrix rings. *Aequationes mathematicae*, ISSN 0001-9054, June 2017, vol. 91, iss. 3, str. 563-578. <http://doi.org/10.1007/s00010-016-0462-7>, doi: [10.1007/s00010-016-0462-7](https://doi.org/10.1007/s00010-016-0462-7).
3. EREMITA, Daniel. Biderivations of triangular rings revisited. *Bulletin of the Malaysian Mathematical Society*, ISSN 0126-6705, Apr. 2017, vol. 40, iss. 2, str. 505-522. <http://doi.org/10.1007/s40840-017-0451-6>, doi: [10.1007/s40840-017-0451-6](https://doi.org/10.1007/s40840-017-0451-6).
4. EREMITA, Daniel. Functional identities in upper triangular matrix rings. *Linear Algebra and its Applications*, ISSN 0024-3795. [Print ed.], 2016, vol. 493, str. 580-605. <http://dx.doi.org/10.1016/j.laa.2015.12.022>.
5. EREMITA, Daniel. Functional identities of degree 2 in triangular rings revisited. *Linear and Multilinear Algebra*, ISSN 0308-1087, 2015, vol. 63, iss. 3, str. 534-553. <http://dx.doi.org/10.1080/03081087.2013.877012>.