



Univerza v Mariboru

Fakulteta za naravoslovje
in matematiko

UČNI NAČRT PREDMETA / COURSE SYLLABUS

Predmet:	Teorija števil
Course title:	Number Theory

Študijski program in stopnja Study programme and level	Študijska smer Study field	Letnik Academic year	Semester Semester
Matematika		3.	6.
Mathematics		3.	6.

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			90	6

Nosilec predmeta / Lecturer:

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

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

Vsaka izmed naštetih obveznosti v načinih ocenjevanja mora biti opravljena s pozitivno oceno.

Pozitivna ocena pri pisnem izpitu je pogoj za pristop k ustnemu izpitu.

Vsebina:

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

Praštevila. Osnovni izrek aritmetike.

Prerequisites:

Each of the mentioned assessments must be assessed with a passing grade.

Passing grade of written exam is required to take the oral exam.

Content (Syllabus outline):

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

Primes. Fundamental Theorem of Arithmetic.

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

Aritmetične funkcije. Multiplikativne funkcije. Möbiusova formula inverzije.

Red celega števila in primitivni koreni. Kvadratični zakon recipročnosti.

Pitagorejske trojke.

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.

Dodatna literatura / Additional Readings:

A. Dujella: Number Theory. Zagreb: Školska knjiga, 2021.

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.

Prenosljive/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
- Teoretične vaje

Learning and teaching methods:

- Lectures
- Theoretical exercises

Načini ocenjevanja:

Assessment:

Pisni izpit Ustni izpit	Delež (v %) / Weight (in %) 50% 50%	Written exam Oral exam
----------------------------	--	---------------------------

Opombe:

Pisni izpit se lahko nadomesti s kolokviji v enakem deležu 50%.

Comments:

Written exam can be replaced by written midterm examination in the weight of 50%.

Reference nosilca / Lecturer's references:

1. EREMITA, Daniel. Biderivations and commuting linear maps on current Lie algebras. *Journal of Lie theory*. 2021, vol. 31, no. 1, str. 119-126. ISSN 0949-5932. [COBISS.SI-ID [100444419](#)]
2. BENKOVIČ, Dominik, EREMITA, Daniel. Generalized derivations of current Lie algebras. *Communications in algebra*. 2024, vol. 52, iss. 11, str. 4603-4611. ISSN 0092-7872. [COBISS.SI-ID [200554755](#)]
3. EREMITA, Daniel. Dhara, B. (6-BELDC-M); Ghosh, S. (6-JDVP); Sandhu, G. S. (6-PMNC-M): On Lie ideals satisfying certain differential identities in prime rings. (English summary). - *Extracta Math.* 38 (2023), no. 1, 67–84. *MathSciNet : Mathematical Reviews on the Web*. [Spletna izd.]. 2024, 1 spletni vir (mr4608757). ISSN 2167-5163. [COBISS.SI-ID [200562435](#)]
4. EREMITA, Daniel. Krempa, Jan (PL-WASW-IM): On nil algebras and a problem of Passman concerning nilpotent free algebras. (English summary). - *Algebra and coding theory*, 197-204, *Contemp. Math.*, 785, Amer. Math. Soc., [Providence], RI, [2023], ©2023. *MathSciNet : Mathematical Reviews on the Web*. [Spletna izd.]. 2024, 1 spletni vir (mr4586441). ISSN 2167-5163. [COBISS.SI-ID [215992579](#)]
5. EREMITA, Daniel. Tiwari, S. K. (6-IITPT-DM): Product and commuting generalized derivations in prime rings. (English summary). - *Rend. Circ. Mat. Palermo (2)* 72 (2023), no. 2, 1377–1397. *MathSciNet : Mathematical Reviews on the Web*. [Spletna izd.]. 2024, 1 spletni vir (mr4559105). ISSN 2167-5163. [COBISS.SI-ID [200564227](#)]