UČNI NAČRT PREDMETA / COURSE SYLLABUS			
Predmet:	Elementarna teorija števil		
Course title:	Elementary number theory		

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Univerzitetni študijski program Matematika	ni smeri	3	prvi
First cycle academic study programme Mathematics	none	3	first

Vrsta predmeta / Course type	izbirni

Univerzitetna koda predmeta / University course code:	M0265

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ.** **work**	**ECTS**
45		30			105	6

Nosilec predmeta / Lecturer:	prof. Sašo Strle

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

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Opravljen predmet Algebra 2.	Completed course Algebra 2.

Vsebina:	**Content (Syllabus outline):**

Naravna in cela števila, osnovni izrek aritmetike, multiplikativne funkcije, Moebiusova inverzna formula. Osnovne lastnosti in porazdelitev praštevil.	Natural numbers and integers, fundamental theorem of arithmetic, multiplicative functions, Moebious inversion. Basic properties and distribution of primes.
Največji skupni delitelj, razširjeni Evklidov algoritem. Končni in neskončni verižni ulomki, izrek o najboljši aproksimaciji, periodični verižni ulomki.	Greatest common divisor, extended Euclidean algorithm. Finite and infinite continued fractions, best approximations, periodic continued fractions.
Kongruence, Eulerjeva funkcija, Eulerjev izrek, Wilsonov izrek. Šifriranje. Polinomske kongruence, kvadratni ostanki, Legendreov simbol, izrek o kvadratni recipročnosti.	Congruences, Euler's function, Euler's theorem, Wilson's theorem. Encryption. Polynomial congruences, quadratic residues, Legendre symbol, quadratic reciprocity.
Diofantske enačbe: linearne, kvadratne (Pitagorejske trojice, Pellova enačba). Racionalne točke na stožnicah.	Diophantine equations: linear, quadratic (Pythagorean triples, Pell's equation). rational points on conics.
Predstavitev števil z vsotami kvadratov (vsote dveh, treh in štirih kvadratov), Lagrangeev izrek. Celoštevilske kvadratne forme dveh spremenljivk: kanonična oblika, avtomorfizmi, predstavitve števil.	Sums of squares (sums of two, three or four squares). Lagrange's theorem. Integer binary quadratic forms: reduced forms, automorphisms, representations of numbers.

Temeljni literatura in viri / Readings:

J. Grasselli: Elementarna teorija števil, DMFA 2009.

H. Dörrie: 100 Great Problems of Elementary Mathematics : Their History and Solution, Dover Publications, New York, 1982.

K. H. Rosen: Elementary Number Theory and Its Applications, Addison-Wesley, Reading, London, Amsterdam, 2000.

J. J. Tattersall: Elementary Number Theory in Nine Chapters, 2nd edition, Cambridge Univ. Press, Cambridge, 2005.

Cilji in kompetence:

Študent spozna osnove elementarne teorije števil. Ob reševanju elementarnih matematičnih problemov z elementarnimi sredstvi se uči matematičnega načina razmišljanja. Predmet po tematiki in načinu razmišljanja poglablja temeljna matematična znanja, ki jih potrebuje učitelj matematike.

Objectives and competences:

Students acquire the basic knowledge and skills in elementary number theory. Solving the elementary problems, students enhance their mathematical thinking and comprehension. The course by its content and methods of teaching deepens a prospective teacher's essential mathematical knowledge and skills.

Predvideni študijski rezultati:

Znanje in razumevanje:
Poznavanje in razumevanje osnovnih pojmov in definicij iz elementarne teorije števil ter uporaba konceptov pri reševanju elementarnih matematičnih problemov.

Intended learning outcomes:

Knowledge and understanding:
Knowledge and comprehension of essential concepts and definitions of elementary number theory and acquired ability to use these methods in elementary mathematical problems.

Metode poučevanja in učenja:

Predavanja, vaje, konzultacije

Learning and teaching methods:

Lectures, tutorial sessions, individual consultations

Načini ocenjevanja:	Delež (v %) / Weight (in %)	Assessment:
Izpit se oceni z ločenima ocenama iz vaj in iz teorije.		Course grade consists of two grades.
Izpit iz vaj.		Exercise-based exam.
Izpit iz teorije.		Theoretical knowledge exam.
Ocene: 6-10 (pozitivno), 5 (negativno) (po Statutu UL).		Grades: 6-10 (pass), 5 (fail) (according to the Statute of UL).
	100 %	

Reference nosilca / Lecturer's references:

STRLE, Sašo. Bounds on genus and geometric intersections from cylindrical end moduli spaces. Journal of differential geometry, ISSN 0022-040X, 2003, vol. 65, no. 3, str. 469-511. [COBISS.SI-ID 13135193]

OWENS, Brendan, STRLE, Sašo. A characterization of the Z [sup] n [oplus] Z([delta]) lattice and definite nonunimodular intersection forms. American journal of mathematics, ISSN 0002-9327, 2012, vol. 134, no. 4, str. 891-913. [COBISS.SI-ID 16408153]

PREZELJ, Katja. Binarne kvadratne forme in cela števila : magistrsko delo. Ljubljana: [K. Prezelj], 2016. VI, 106 str., ilustr. [COBISS.SI-ID 17851481]