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**
Magistrski študijski program Matematika	ni smeri	1 ali 2	prvi ali drugi
Master's study programme Mathematics	none	1 or 2	first or second

Vrsta predmeta / Course type	izbirni
Univerzitetna koda predmeta / University course code:	M2218

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. Boris Lavrič, prof. Tomaž Košir

Jeziki / Languages:	**Predavanja / Lectures:**	slovenski/Slovene, angleški/English
	Vaje / Tutorial:	slovenski/Slovene, angleški/English

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**
Vsebina:	**Content (Syllabus outline):**

Predavatelj izbere med naslednjimi vsebinami: 1. Algebraična števila: diskriminanta, cela algebraična števila, celostna baza, norma in sled. Kvadratični in ciklotomični obsegi. Nerazcepni elementi. Problem enolične faktorizacije. Praelementi. Evklidski obsegi. Ramanujan-Nagellov izrek. Primarni razcep. 2. Mreže v Rn. Kvocientni torus. Izrek Minkowskega. Razcep celih števil na vsoto kvadratov. Dedekindov izrek. Konstante Minkowskega. 3. Legendrov simbol. Gaussov zakon o kvadratni recipročnosti. Dirichletev izrek o praštevilih v aritmetičnih zaporedjih. Jacobijev simbol. 4. Dirichletev izrek o obrnljivih elementih. 5. Praštevila. Eratostenovo rešeto. Testiranje razcepnosti celih števil. Psevdopraštevila. Fermateva in Mersennova števila. Carmichaelova števila. Razporeditev praštevil. Regularna praštevila. Hevristične metode. Eulerjeva psevdopraštevila. Nelinearne diofantske enačbe. Pitagorejske trojke. Pellova enačba. Kummerjeva teorija za regularna praštevila in Fermatev problem. 6. Lucasova zaporedja. Eulerjev polinom za iracionalna števila. Generiranje praštevil. Transcendentnost znanih števil. 7. Relativna sled in norma. Diskriminanta in diferenta. Primarni razcep v Galoisevih razširitvah. Izrek Kroneckerja in Webra. Teorija razredov. 8. p-adična števila. Formalne potenčne vrste.	The lecturer selects from the following list of contents: 1. Algebraic numbers: discriminant, algebraic integers, integral basis, norm and trace. Quadratic and cyclotomic fields. Irreducible elements. The problem of unique factorization. Prime elements. Euclidean fields. The Ramanujan-Nagell theorem. Prime factorization. 2. Lattices in Rn . The quotient torus. Minkowski's theorem. Sums of squares. The Dedekind's theorem. Minkowski's constants. 3. The Legendre symbol. Gauss' quadratic reciprocity law. Dirichlet's theorem on primes in arithmetic progression. The Jacobi symbol. 4. Dirichlet's unit theorem. 5. Prime numbers. The sieve of Erathostenes. Testing of factorizability of integers. Pseudoprime numbers. Fermat and Mersenne numbers. Carmichael numbers. The distribution of prime numbers. Regular primes. Heuristic methods. Euler pseudoprimes. Nonlinear diophantine equations. Pythagorean triples. Pell's equation. Kummer's theory of regular primes and Fermat's problem. 6. Lucas sequences. Euler polynomial for irrational numbers. Generating prime numbers. Transcendency of renown numbers. 7. Relative trace and norm. Discriminant and different. Factoring of prime ideals in Galois extensions. The theorem of Kronecker and Weber. The class-field theory. 8. p-adic numbers. Formal power series.

Temeljni literatura in viri / Readings:

I. Stewart, D. Tall: Algebraic Number Theory and Fermat's Last Theorem, AK Peters, Natick, ZDA. 3. izdaja, 2002.

P. Ribenboim: Classical Theory of Algebraic Numbers, Universitext. Springer-Verlag, New York, etc. 2001.

P. Ribenboim: The Little Book of Bigger Primes, Springer-Verlag, New York, etc. 2. izdaja, 2004.

K. H. Rosen: Elementary Number Theory and its Applications, Person, Boston, ZDA. 5. izdaja, 2005.

P. Ribenboim: My Numbers, my Friends, Popular Lectures on Number Theory. Springer-Verlag, New York, etc. 2000.

A. A. Gioia: The Theory of Numbers. An Introduction, Dover Publ. 2001.

S. Alaca, K. S. Williams: Introductory Algebraic Number Theory, Cambridge Univ. Press. 2004.

Cilji in kompetence:

Študent se seznani z osnovami teorije števil in njihovo uporabo. Poudarek je na algebraični teoriji števil.

Objectives and competences:

The student learns the basics of the number theory and its applications. The emphasis is on the algebraic theory of numbers.

Predvideni študijski rezultati:

Znanje in razumevanje:
Poznavanje osnovnih pojmov in izrekov teorije števil in njihovo prepoznavanje v drugih vejah matematike.

Uporaba:

V drugih vejah matematike, kriptografiji in teoriji kodiranja. Uporaba v računalništvu in informatiki, zlasti pri računalniški varnosti.

Refleksija:

Razumevanje teorije na podlagi primerov in uporabe.

Prenosljive spretnosti – niso vezane le na en predmet:

Intended learning outcomes:

Knowledge and understanding:
Knowledge of basic concepts and theorems of the number theory of and their recognition in other areas of mathematics.

Application:

In other areas of mathematics, cryptography and coding theory. Application in computer science and informatics, especially in computer safety

Reflection:

Understanding the theory on the basis of examples and applications.

Transferable skills:

Formulacija problemov v primernem jeziku, reševanje in analiza doseženega na primerih, prepoznavanje algebraičnih struktur v teoriji števil.	Formulation of problems in appropriate language, solving and analysis of the result on examples, identifying algebraic structures in theory of numbers.

Metode poučevanja in učenja:	**Learning and teaching methods:**
predavanja, vaje, domače naloge, konzultacije	Lectures, exercises, homeworks, consultations

Načini ocenjevanja:	Delež (v %) / Weight (in %)	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt): izpit iz vaj (2 kolokvija ali pisni izpit) ustni izpit Ocene: 1-5 (negativno), 6-10 (pozitivno) (po Statutu UL)	50% 50%	Type (examination, oral, coursework, project): 2 midterm exams instead of written exam, written exam oral exam Grading: 1-5 (fail), 6-10 (pass) (according to the Statute of UL)

Reference nosilca / Lecturer's references:

Tomaž Košir:

– GRUNENFELDER, Luzius, KOŠIR, Tomaž. Geometric aspect of multiparameter spectral theory. Transactions of the American Mathematical Society, ISSN 0002-9947, 1998, let. 350, št. 6, str. 2525-2546 [COBISS.SI-ID 8449113]

– GRUNENFELDER, Luzius, KOŠIR, Tomaž, OMLADIČ, Matjaž, RADJAVI, Heydar. On groups generated by elements of prime order. Geometriae dedicata, ISSN 0046-5755, 1999, let. 75, št. 3, str. 317-332 [COBISS.SI-ID 8849241]

– KOŠIR, Tomaž, SETHURAMAN, B. A. Determinantal varieties over truncated polynomial rings. Journal of Pure and Applied Algebra, ISSN 0022-4049. [Print ed.], 2005, vol. 195, no. 1, str. 75-95

[COBISS.SI-ID 13266265]

Boris Lavrič:

– LAVRIČ, Boris. Delno urejeni številski kolobarji. Obzornik za matematiko in fiziko, ISSN 0473-7466, 1994, let. 41, št. 3, str. 83-91 [COBISS.SI-ID 5854041]

– LAVRIČ, Boris. Urejeni številski obsegi. Obzornik za matematiko in fiziko, ISSN 0473-7466, 1994, let. 41, št. 2, str. 45-50 [COBISS.SI-ID 5856601]

– LAVRIČ, Boris. Vsote praštevil in vsote njihovih kvadratov. Obzornik za matematiko in fiziko, ISSN 0473-7466, 1996, let. 43, št. 5, str. 161-167 [COBISS.SI-ID 7003737]