M108	**Number Theory**	P	S	V	ECTS
		2	0	2	6

The aim of the course. The aim of this course is to introduce students to the basic concepts, ideas and methods of elementary number theory. During the lectures we will introduce and analyze the basic concepts and results of the number theory. Applications of the obtained results will be presented by examples, and we will indicate the application of the number theory in cryptography. By using claims proved during the lectures, through the exercises students should adopt techniques for solving computational and problem-solving tasks.

Prerequisites. Elementary Mathematics.

Course content.

1. *Divisibility*. Divisibility of integers and basic properties of divisibility. The Euclidean algorithm.
2. *Factorization*. Prime numbers. The fundamental theorem of arithmetic. Number and sum of divisors of a positive integer.
3. *Congruences*. Modular arithmetic. Linear congruences. The Chinese remainder theorem. The Euler function. Wilson's and Lagrange's theorem. Primitive roots and indices. Linear Diophantine equations. Applications of congruences.
4. *Quadratic residues*. The Legendre symbol. Quadratic reciprocity law. The Jacoby symbol. Applications of Legendre's and Jacoby's symbol.
5. *The Gaussian integers*. Elementary properties of Gaussian integers. Divisibility and primes in the set of Gausian integers. Sums of two squares. Pythagorean triples.
6. *Continued fractions*. Finite and infinite continued fractions. Quadratic irrationals. Pell's equations.

Learning outcomes

No.	**Learning outcomes**
1.	Use properties of divisibility, factorization and congruences in problem solving.
2.	Recognise basic arithmetic functions.
3.	State and apply basic theorems of number theory.
4.	Understand the role of number theory in cryptography.
5.	Identify properties of Gaussian integers.
6.	Solve some types of Diophantine equations.

CONNECTING LEARNING OUTCOMES, ORGANIZATION OF TEACHING PROCESS AND ASSESSMENT OF STUDENT LEARNING OUTCOMES

Organization of the educational process	ECTS	Learning outcomes **	Student activities*	The method of estimate	Points	
					Min	max
Lecture attendance	1	1-6	Lecture attendance, discussion, team work and independent work on given tasks.	Attendance sheets, tracking activities	0	4
Written exam. (colloquium)	2	1-6	Prepairing for written exam.	Evaluation.	25	48
Final exam.	3	1-6	Reviewing of presented lectures.	Oral exam.	25	48
Total	6				50	100

Teaching and evaluation of knowledge. Attendance at lectures and exercises is required. The exam consists of written and oral part, and can be taken after completion of lectures and exercises. Acceptable results of colloquiums written during the semester can replace the written part of the exam.

Can the course be taught in English: Yes.

Basic literature:

1. I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, 2015.
2. A. Dujella, *Uvod u teoriju brojeva*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2002, script.

Additional literature:

1. T. Andreescu, D. Andrica, *An Introduction to Diophantine Equations*, GIL Publishing House, 2002.
2. A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.
3. A. Dujella, *Diofantske jednadžbe*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2007., script
4. G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer, 2003.
5. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, 1994.
6. K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, 1993.
7. J. Stilwell, *Elements of number theory*, Springer, 2003.