M049	Obligatory - Semester 4	**Number Theory**	L+P+S 2+2+0	ECTS 6

Course objective. Number theory is the oldest and most widespread branch of theoretical mathematics, with numerous applications. The objective of this course is to familiarize students with basic concepts, ideas and methods of elementary number theory. In lectures, we will introduce and analyze the basic concepts and demonstrate their properties, along with numerous examples and illustrative applications, such as the impact of number theory on cryptography. In exercises, students will learn about computational techniques and problem-solving tasks and will be trained to solve specific problems.

Course prerequisites. Elementary Mathematics I and II.

Syllabus.

1. Divisibility and its basic properties. Greatest common divisor and Euclid algorithm. Prime numbers. Number of divisors and sum of divisors. Fermat numbers. Application of divisibility in solving Diophantine equations.
2. Congruences. Basic properties and solving some basic congruences. Euler, little Fermat and Wilson theorems. Chinese remainder theorem.
3. Application of congruences. Linear Diophantine equations. Cryptosystems. Transpose ciphers. RSA cryptosystem.
4. Quadratic residues. Definition and basic properties of Legendre symbol. Gaussian quadratic reciprocity law. Jacobian symbol. Application on solving Diophantine equations.
5. Gaussian integers. Norm and divisibility of Gaussian integers. Sums of two squares. Application of Gaussian integers to determining primitive Pythagorean triples.
6. Pell and Pellian equations. Pell equation and the existence of solution. Dirichlet aproximation theorem. Structure od the set of solutions of Pell equation and connections with continued fractions. Criterion of solvability of certain Pellian equations and algorithms for determining the solutions of such equations.

Expected learning outcomes.

After completing the course, students are expected to know how to:

- classify Diophantine equations and solve simpler types of the same;
- examine the basic properties of divisibility of integers;
- classify cryptosystems and understand the importance of number theory in cryptosystems;
- identify properties of Gaussian integers;
- determine the solutions of Pell equations in a given interval.

Teaching methods and student assessment. Attendance at lectures and exercises is required. The exam consists of a written and an oral part, and it can be taken after the completion of lectures and exercises. Acceptable mid-term exam scores replace the written examination. Students are encouraged to write seminar papers during the semester and that could influence the final result of the exam.

Can the course be taught in English? Yes.

Basic literature:

1. J. Stilwell, Elements of number theory, Springer, 2003.
2. A. Dujella, Uvod u teoriju brojeva, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2002.

Recommended literature:

1. T. Andreescu, D. Andrica, An Introduction to Diophantine Equations, GIL Publishing House, 2002.
2. A. Dujella, Diofantske jednadžbe, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2007.
3. N. Koblitz, A Course in Number Theory and Cryptography, Springer Verlag, 1994.

4. G.A. Jones, J.M. Jones, Elementary Number Theory, Springer, 2003.
5. L.N. Childs, A Concrete Introduction to Higher Algebra, Springer Verlag, 1995.