Study programme(s): Teaching Informatics (IC)

Level: master

Course title: Number Theory (IA012)

Lecturer: Igor V. Dolinka

Status: elective

ECTS: 5

Requirements: none

Learning objectives

To introduce students to the basic concepts of number theory and to emphasise their importance within the system of mathematical disciplines, giving close attention to applications of number theory in computer science and applications of computer science in number theory.

Learning outcomes

Minimal: Understanding the basic principles of number theory and the ability to solve more simple arithmetical problems.

Optimal: The ability to creatively solve problems from elementary number theory and a comprehensive understanding of the underlying theory.

Syllabus

Theoretical instruction:

Divisibility, prime and composite numbers. Euclidean algorithm. The floor function. The fundamental theorem of arithmetic. Finding prime numbers, the sieve of Eratosthenes. The function $\pi(x)$. Congruences, systems of linear congruences, the Chinese remainder theorem. Fermat’s little theorem, Euler’s theorem and Wilson’s theorem. Properties of congruences modulo prime numbers, primitive root. Applications in cryptography. Recognizing prime numbers, pseudo-primes, strong pseudo-primes. Primality certificates. Integer factorization. Evaluating the function $\pi(x)$. Perfect numbers, Mersenne primes. Some classes of Diophantine equations. The role of computers in some contemporary problems in number theory.

Practical instruction:

Applications of the presented theoretical concepts.

Literature

1. В. Мићић, З. Каделбург, Д. Ђукић, *Увод у теорију бројева*, Друштво математичара Србије, Београд, 2004.
2. Р. Тошић, В. Вукослављевић, *Елементи теорије бројева*, Алеф, Нови Сад, 1995.
3. S. Y. Yan, *Number Theory for Computing*, Springer, Berlin, 2002.

Weekly teaching load				Other: 0
Lectures: 2	Exercises: 2	Other forms of teaching: 0	Student research: 0	

Teaching methodology

Classical methodology is used in theoretical instruction. At the practical instruction, the presented principles are practised and typical problems and their solutions are analyzed. Students’ knowledge is tested in two colloquia, which test both the degree of acknowledged theoretical concepts as well as the skill of their applications through problem-solving. At the final oral exam, comprehensive understanding of the presented material is tested.

Grading method (maximum number of points 100)

Pre-exam obligations	**points**	**Final exam**	**points**
Colloquia	50	Oral exam	50