COURSE DESCRIPTION CARD - SYLLABUS

Course name
Elementary number theory [S1MNT1>F-ETL]

Course

Field of study
Mathematics of Modern Technologies

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
30

Laboratory classes
0

Other
0

Tutorials
15

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr Anna Iwaszkiewicz-Rudoszańska
anna.iwaszkiewicz-rudoszanska@put.poznan.pl

Lecturers

Prerequisites

Basic knowledge of abstract algebra and discrete mathematics. Logical thinking skills. Understanding of the limitations of one’s knowledge and motivation for further education.

Course objective

The aim of the course is to present the basic concepts and methods used in elementary number theory and its applications.

Course-related learning outcomes

Knowledge:
• Sudent has in-depth knowledge of elementary number theory [K_W01(P6S_WG)];
• Student knows the basic definitions and theorems of elementary number theory [K_W01(P6S_WG)].

Skills:
• Student uses congruences, knows their basic properties and applications, including in cryptography [K_U01(P6S_UW)];
• Student is able to solve the basic types of Diophantine equations [K_U01(P6S_UW)];

• Student knows how to prove the theorem or give an appropriate counterexample [K_U01(P6S_UW)].

Social competences:
• Student knows the limitations of her/his knowledge and understands the need for further education [K_K01(P6S_KK), K_K02(P6S_KK)].

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lectures: valuation of knowledge and skills during written test.
Tutorials: three short, evenly scored tests.

Programme content

Divisibility in a set of integers. Congruences. RSA. Quadratic congruences. Selected Diophantine equations. Representation of natural numbers as the sum of squares of natural numbers. Arithmetic functions. Primality tests and factorization algorithms.

Course topics

Update: 31.05.2024r.
Lectures:
• divisibility in a set of integers (definition, properties, Euclidean algorithm, prime numbers, Dirichlet's prime number theorem in arithmetic progress with proofs of special cases);
• congruences (definition, properties, divisibility tests, Chinese remainder theorem, Euler function and Euler, Wilson and Lagrange theorems);
• the RSA cryptographic system as an application of the Euler theorem;
• quadratic congruences (quadratic residues and nonresidues, the symbol of Legendre and Jacobi, quadratic reciprocity theorem);
• Rabin's cryptographic system;
• selected Diophantine equations;
• representation of natural numbers as the sum of squares of natural numbers;
• arithmetic functions (definition and examples, additive and multiplicative functions, Dirichlet convolution);
• primality tests and factorization algorithms (Fermat, Solovay-Strassen, Miller-Rabin tests, factorization of Mersenne and Fermat numbers, Fermat, Dixon and p-1 Pollard methods).
Tutorials:
• divisibility in a set of integers;
• congruences (linear congruences, Chinese remainder theorem, Fermat's little theorem and Euler theorem;
• RSA cryptographic system;
• quadratic congruences, Legendre and Jacobi symbol, quadratic reciprocity theorem;
• Rabin cryptographic system;
• selected diophantine equations.

Teaching methods

Lectures: mulimedia presentation accompanied with examples presented on the blackboard as well as asking questions to students.
Tutorials: solving examples on the blackboard, initiating discussions about solutions, real-time feedback from the teacher.

Bibliography

Basic:
• W. Marzantowicz, P. Zarzycki, Elementarna teoria liczb, PWN, Warszawa 2006;
• W. Narkiewicz, Teoria liczb, PWN, Warszawa 2003;
• M. Zakrzewski, Teoria liczb, GiS, Wrocław 2017;
• J. Rutkowski, Teoria liczb w zadaniach, PWN, Warszawa 2019.

Additional:
• N. Koblitz, Wykład z teorii liczb i kryptografii, WNT, Warszawa 1995;
• W. Sierpiński, 250 zadań z elementarnej teorii liczb, WSiP, 1987.

Breakdown of average student's workload

	Hours	ECTS
Total workload	75	3,00
Classes requiring direct contact with the teacher	45	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00