

(1.) Course Title: INFPHD198 Algorithms in algebraic number theory	Credits: 6
Course Classification: Optional	
Theoretical or Practical Nature of the Course, 'training character' ¹³ : 90% theory(credit%)	
Type of Class: lecture + consultation and number of hours: 2/week in the given semester, (If the course is not (only) taught in Hungarian, then the language: English) Additional (specific) methods and characteristics² used in delivering the knowledge (if any): -	
Assessment Method (Exam / Midterm Grade / Other³): midterm report Additional (specific) methods⁴ applied in knowledge assessment (if any): topic elaborations	
Course Placement in Curriculum (Semester Number): -	
Prerequisites (if any): Discrete Mathematics I – II.	
Course Description: A concise yet informative description of the knowledge to be acquired.	
The goal is the deep investigation of such areas of modern algebra that are appropriate to improve methods applying in computational number theory. Short description: 1. Quadratic fields. 1.1. Number systems in quadratic fields. 1.1.1. Digit sets. 1.1.2. Periodic elements. 1.1.3. The elements of the boundary set of the “basic set” ($B\gamma$). 1.1.4. The approximation of the dimension of $B\gamma$. 1.2. Fundamental discriminants. 1.3. Binary quadratic forms. 1.4. Class number for fundamental discriminants. 1.5. Algebraic integers. 1.6. Quadratic fields and prime numbers. 2. Elliptic curves. 2.1. Elliptic curve primality proving. 2.2. Elliptic curve factorization. 2.3. Elliptic curve cryptography. 3. Prime algorithms 3.1. Prime test. 3.2. Sieving algorithms. 3.3. Prime records. The course is recommended for: The course is primarily recommended for computer science students who are interested in mathematics and would like to perfect the software they design or develop through theoretical study. It is not recommended for mathematicians.	

2-5 Most Important Required and Recommended Literature

List of required and recommended literature (notes, textbooks) with bibliographic data (author, title, publication details, (possibly pages), ISBN).

Imre Káta: Generalized Number System and Fractal Geometry
Lawrence C. Washington: Elliptic Curves
Saban Alaca – Kenneth S. Williams: Introductory Algebraic Number Theory
Henri Cohen: A Course in Computational Algebraic Number Theory

List of Prescribed Professional Competencies and Competency Elements

(knowledge, skills, etc., KKK Section 8) that the course significantly contributes to developing (highlight the most important ones).

a) Knowledge

- Has a research-level understanding of the general and specific characteristics, major directions, and precisely developed boundaries of the subject area within the discipline, as well as the agreed and debated interrelations.
- Creatively comprehends the interrelations, theories, and conceptual frameworks and terminologies of the given field of study.¹
- Possesses research methodology knowledge necessary for independent research in the given discipline/field.

b) Skills

- Capable of creative analysis of the field, synthesizing comprehensive and specific interrelations with a new perspective, and conducting appropriate evaluative and critical activities.
- Able to apply and further develop the specialized learning and problem-solving methods of the field.
- Can creatively elaborate on the novel, previously unknown practical implications of theoretical issues.
- Capable of planning and executing new projects, conducting research in the field, and developing new techniques and approaches.
- Able to identify unforeseen professional problems and uncover the detailed theoretical and practical background necessary for their resolution at a research level.
- Can construct and communicate new relations relevant to the field, as well as comprehensive interrelations significant for personal and communal existence.

c) Attitudes

- Represents and further develops the relations that contribute to the process of human self-creation based on the field's characteristics.

¹**Section 108**, Article 37 of the National Curriculum Act (Nftv.) 37. lesson: a session (lecture, seminar, exercise, consultation) requiring the personal involvement of the instructor to fulfil the academic requirements specified in the curriculum, the duration of which is at least forty-five minutes and not more than sixty minutes.

² e.g. case studies, role play, thematic presentations, etc.

³ e.g. continuous debriefing, mid-year report

⁴ e.g. request for case studies, thematic papers, essays, business, organisational plans, etc.

- Possesses an interest and learning ability that enable identifying and solving currently unpredictable research problems in the field.
- Demonstrates a firm professional commitment, a continuous dedication to exploring new approaches, and an acceptance of the necessity for persistent effort.

d) Autonomy and Responsibility

- Builds and initiates new knowledge areas with creative independence and proposes new practical solutions.
- Participates in formulating theoretical and practical questions with a leadership role and high-level cooperation.
- Engages as an equal discussion partner with professionals in the field.
- Takes responsibility for raising and addressing new ethical questions concerning theoretical and practical aspects of the profession.

Course responsible (name, position, academic degree): **Dr. Gábor Farkas, Habil. Associate Professor, PhD**

Instructor(s) involved in teaching the course (if any) (name, position, academic degree):
-