Module title			Abbreviation
Algorithmic Number Theory			10-M=VAZTin-211-m01

Module coordinator	Module offered by
Dean of Studies Mathematik (Mathematics)	Institute of Mathematics

ECTS	Method of grading	Only after succ. compl. of module(s)
10	numerical grade	--

Duration	Module level	Other prerequisites
1 semester	graduate	--

Contents

Binary numbers, computation of the greatest common divisor, pseudoprime tests, computation of primitive roots. Primality tests for Fermat and Mersenne numbers, factorisation methods (Pollard-Rho, (p-1)-method, elliptic curve method, quadratic sieve method), discrete logarithm.

Intended learning outcomes

The student knows about the theoretical foundations and the possible applications of several methods in algorithmic number theory.

Courses (type, number of weekly contact hours, language — if other than German)

V (4) + Ü (2)
Module taught in: English

Method of assessment (type, scope, language — if other than German, examination offered — if not every semester, information on whether module is creditable for bonus)

a) written examination (approx. 90 to 120 minutes, usually chosen) or
b) oral examination of one candidate each (approx. 20 minutes) or
c) oral examination in groups (groups of 2, 15 minutes per candidate)
Language of assessment: English
Assessment offered: Only when announced in the semester in which the courses are offered and in the subsequent semester
creditable for bonus

Allocation of places

--

Additional information

--

Workload

300 h

Teaching cycle

--

Referred to in LPO I (examination regulations for teaching-degree programmes)

--

Module appears in

Master's degree (1 major) Mathematics International (2021)
Master's degree (1 major) Mathematics International (2022)