FSF3741 Computational Number Theory 7.5 credits

Beräkningstalteori

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

Course syllabus for FSF3741 valid from Spring 2019

Grading scale

P, F

Education cycle

Third cycle

Specific prerequisites

Masters degree in mathematics, or in computational mathematics or in computer science/engineering with at least 30 cr in mathematics.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

Broad overview of modern computational number theory. In depth knowledge of specialized

Course contents

- Factoring
- Shank's SQUFOF
- Quadratic sieve
- Lenstra's elliptic curve algorithm
- Number field sieve
- Elliptic curves
- Elliptic curve cryptography - avoiding factor base embeddings
- Identity based schemes via the Weil pairing
- Point counting on elliptic curves (Shoof, Sato)
- Primality proving
- PRIMES is in P - the AKS algorithm, plus the Pomerance-Lenstra refinement.
- Elliptic curve primality proving (Schoof, Atkin-Morain)
- Some modern probabilistic primality test (Frobenius pseudo primes etc) and analogues of Carmichael numbers.
- Class groups
- Determining the size/generators with and without assuming GRH.
- Fast verification via trace formulae
- Fundamental units/regulators
- Fast arithmetic
- FFT
- Fuerer
- Z-modules and lattices
- Ideal arithmetic
- The LLL algorithm
- Short vectors and cryptographic applications

Disposition

Weekly seminar.

Course literature

Prime numbers: a computational perspective by Richard Crandall, Carl Pomerance

F- A course in computational algebraic number theory by Henri Cohen

Examination

- SEM1 - Seminars, 7.5 credits, grading scale: P, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Oral presentation of selected topic. At least 90% seminar attendence

Other requirements for final grade

Approved oral presentation of selected topic. At least 90% seminar attendence.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.