



FSF3741 Beräkningstalteori 7,5 hp

Computational Number Theory

Fastställande

Kursplan för FSF3741 gäller från och med HT09

Betygsskala

G

Utbildningsnivå

Forskarnivå

Särskild behörighet

M.Sci in Mathematics (at least 30 points)

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

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

Kursinnehåll

- 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
- Furer
- Z-modules and lattices
- Ideal arithmetic
- The LLL algorithm
- Short vectors and cryptographic applications

Kursupplägg

Weekly seminar

Kurslitteratur

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

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

Examination

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enskilda studenter.

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

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

Övriga krav för slutbetyg

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

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.