FSF3741 Beräkningstalteori 7,5 hp

Computational Number Theory

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

Fastställande

Kursplan för FSF3741 gäller från och med VT19

Betygsskala

P, F

Utbildningsnivå

Forskarnivå

Särskild behörighet

Civilingenjörs- eller Masterexamen med minst 30 hp inom matematik.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Bred översikt över modern beräkningstalteori. Fördjupad kunskap om några speciella algoritmer.

Kursinnehåll

- Factoring
- Shanks SQUFOF
- Kvadratisk såll
- Lenstras elliptiska kurvalgoritm
- Talkroppssållet
- Elliptiska kurvor
- Kryptering mha elliptiska kurvor - undvikande av faktorbaserade inbäddningar
- Identitetsbaserade system via Weil-parningen
- Punkträkning med elliptiska kurvor (Shoof, Sato)
- Primtalsbevisning
- PRIMES är i P - AKS-algoritmen plus Pomerance-Lenstra förfiningen.
- Primtalsbevis mha elliptiska kurvor (Schoof, Atkin-Morain)
- Några moderna probabilistiska primtalstest (Frobenius pseudo primesetc) och analoger av Carmichael-nummer.
- Klassgrupper
- Bestämning av storlek / generatorer med och utan antagande av GRH.
- Snabb verifiering via spårformler
- Fundamentalenheter / regulatorer
- Snabb aritmetik
- FFT
- Fuerer
- Z-moduler och gitter
- Idealaritmetik
- LLL-algoritmen
- Korta vektorer och kryptografiska tillämpningar

Kursupplägg

Veckovisa seminarier.

Kurslitteratur

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

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

Examination

- SEM1 - Seminarier, 7,5 hp, betygsskala: P, F

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 enstaka studenter.

Muntlig presentation av valt ämne. Minst 90% seminarienärvaro.

Övriga krav för slutbetyg

Godkänd muntlig presentation av valt ämne. Minst 90% seminarienärvaro

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.