



Kursplan

Fakulteten för teknik

Institutionen för matematik

2MA406 Elementär talteori, 7,5 högskolepoäng

Elementary number theory, 7.5 credits

Huvudområde

Matematik

Ämnesgrupp

Matematik

Nivå

Grundnivå

Fördjupning

G2F

Fastställande

Fastställd 2014-10-03

Senast reviderad 2015-11-03 av Fakulteten för teknik. Revidering av mål, undervisningsform och examination.

Kursplanen gäller från och med vårterminen 2016

Förkunskaper

60 hp i matematik eller matematikdidaktik inkluderande kurserna 1MA403

Vektorgeometri 7,5 hp och 1MA462 Diskret matematik 7,5 hp eller motsvarande.

Mål

Efter genomgången kurs förväntas studenten kunna

- lösa problem, utföra beräkningar och föra resonemang inom den del av matematiken som omfattas av kursen samt skriftligt kunna kommunicera dessa lösningar, beräkningar och resonemang
- redogöra för definitioner samt formulera och bevisa teorem som är centrala i kursen.

Innehåll

Kursen innehåller följande moment:

- Delbarhet, primtal och största gemensamma delare. Aritmetikens fundamentalsats. Euklides algoritm. Representation av heltal i olika baser.
- Aritmetiska funktioner och Möbius inversionsformel.
- Kongruensteori. Linjära kongruenskvationer. Kinesiska restsatsen. Fermats och Eulers satser.
- Substitutionskrypton. Blockkrypton. Kryptosystem med öppna nycklar som till exempel RSA.
- Kvadratiske rester. Legendresymbolen. Gauss reciprocitetssats.

- Primitiva rötter. Index kalkyl. Slumptalsgeneratorer. Kryptosystemet ElGamal.

Undervisningsformer

Föreläsningar och övningar.

Examination

Kursen bedöms med betygen A, B, C, D, E, Fx eller F.

Betyget A utgör det högsta betygssteget, resterande betyg följer i fallande ordning där betyget E utgör det lägsta betygssteget för att vara godkänd. Betyget F innebär att studentens prestationer bedömts som underkända.

Examinationen sker med skriftlig tentamen.

Kursvärdering

Under kursens genomförande eller i nära anslutning till kursen genomförs en kursvärdering. Resultat och analys av kursvärderingen ska återkopplas till de studenter som genomfört kursen och de studenter som deltar vid nästa kurstillfälle.

Kursvärderingen genomförs anonymt. Den sammanställda rapporten arkiveras vid fakulteten.

Överlappning

Kursen kan inte ingå i examen med annan kurs, vars innehåll helt eller delvis överensstämmer med innehållet i denna kurs: 2MA106 Elementär talteori, 7,5 hp

Övrigt

Betygskriterier för A-F-skalan kommuniceras till studenten via särskilt dokument. Studenten informeras om kursens betygskriterier senast i samband med kursstart.

Kurslitteratur och övriga läromedel

Obligatorisk litteratur.

Rosen K H, *Elementary Number Theory and its Applications*, Pearson Addison Wesley, senaste upplagan. 454 (721) sidor.