



## 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 av Fakulteten för teknik 2014-10-03

Kursplanen gäller från och med höstterminen 2015

### 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:

- definiera grundläggande begrepp inom den elementära talteorin
- redogöra för och härleda elementära egenskaper hos heltalen
- använda de aritmetiska funktionerna för att beskriva talteoretiska samband
- lösa linjära kongruensekvationer och bestämma lösbarheten hos kvadratiske kongruenser
- använda diskreta logaritmer (index kalkyl)
- använda metoder från talteorin inom tillämpningsområden som till exempel krypteringsteori
- beskriva resultat och tillämpningar från talteorin för icke-expertter som till exempel elever i grundskola och gymnasium.

### 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 kongruensekvationer. Kinesiska restsatsen. Fermats och Eulers satser.

- Substitutionskrypton. Blockkrypton. Kryptosystem med öppna nycklar som till exempel RSA.
- Kvadratiske rester. Legendresymbolen. Gauss reciprocitetsats.
- Primitiva rötter. Index kalkyl. Slumtalsgeneratorer. Kryptosystemet ElGamal.

## Undervisningsformer

Föreläsningar och övningar. Grupparbeten och obligatoriska moment kan förekomma.

## Examinationsformer

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 och/eller muntlig tentamen. Kontinuerlig examination genom skriftliga och/eller muntliga redovisningar kan dessutom förekomma. Den huvudsakliga formen för examination bestäms vid kursstart.

## Kursvärdering

I samband med kursavslutningen genomförs en kursvärdering enligt universitetets riktlinjer. Resultatet av kursvärderingen arkiveras på institutionen.

## 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.