

Matematiska Institutionen  
KTH

**Kursprogram till kursen Diskret Matematik, SF1610, för CINTE, ht2011 (nyast).**

**Kursledare och lärare:**

Olof Heden  
Lindstedtsvägen 25 rum 3641  
Tel: 08 7906296 (0730 547 891)  
e-post: oloed@math.kth.se  
Mottagningstid: efter överenskommelse.

**Kurslitteratur:**

Eriksson K. och Gavel H., Diskret matematik och diskreta modeller, Studentlitteratur 2002.

Eriksson K. och Gavel H., Diskret matematik, Fördjupning, Studentlitteratur 2003.

**Kursinnehåll:** Kursinnehåll framgår av föreläsningsplanen nedan.

**Undervisningsform:** Lektioner.

**Examination:** Så kallad kontinuerlig examination samt möjlighet att bli godkänd på kursen vid en tentamensskrivning. Kursen delas upp i fem delmoment och varje delmoment examineras var för sig vid ett 60 minuter långt skriftligt prov, se plan över föreläsningar och övningar på nästa sida.

Tentamensskrivningen på hela kursen är uppdelad på tre delar, del I, del II och del III.

Del I består av 5 uppgifter, som vardera kan ge högst 3p. Godkänt delprov nr  $i$  ger automatiskt 3p på uppgift nr  $i$  ( $i=1,2,3,4,5$ ). Del II består av 3 uppgifter, som vardera kan ge högst 4p. Del III består av två uppgifter som vardera kan ge 5 poäng. Totalt är det alltså möjligt att få 37p på skrivningen.

För att få betyget godkänt, dvs minst betyget E, på kursen krävs dels minst 12p på del I, dels minst 15p totalt på skrivningen (inklusive bonus från kontrollskrivningar).

Betygsgränserna i övrigt är (preliminärt): betyg E: 15p, betyg D: 18p, betyg C: 22p, betyg B: 27p, betyg A: 32p.

Vid 13 eller 14 poäng får man Fx vilket innebär rätt till en kompletterande tentamen.

# UNDERVISNINGSPLAN

## Lektioner och delprov

| Innehåll  | Avsnitt                                   |
|---|---|
| 29/8 Kursintro., Aritmetik, printal. Eukl. algoritm     | 3.3.1-3.3.4                               |
| 30/8 Diofantiska ekvationer och aritmetikens fund.sats. | 3.3.5, 3.3.4.1                            |
| 1/9 Modulär aritmetik                                   | 3.4                                       |
| 2/9 Modulär aritmetik. Talbaser och talsystem           | 3.4, 3.2                                  |
| 5/9 Rekursion och induktion                             | 4   |
| 6/9 Mängdlära, relationer                               | 2.1-2.6                                   |
| 7/10 Funktioner och kardinalitet                        | 8   |
| 8/10 Multiplikationsprincipen och lite sannolikhetslära | 5.1-5.3                                   |
| 9/10 Permutationer och urval, postfacksprincipen        | 5.4-5.6                                   |
| 12/9 Övningar på de hittills genomgångna momenten       |   |
| 13/9 PROV PÅ DELMOMENT I, klockan 10.45-11.45           | 2, 3, 4, 8.1.1-8.1.2, 8.1.4-8.2.2.1       |
| 15/9 Inklusion exklusion, Stirlingtal och partitioner   | 5.7-5.8                                   |
| 16/9 Grupper introduktion, exempel                      | 2.1-2.1.3 i del II                        |
| 19/9 Övningar på avsnittet kombinatorik, dvs del II     |   |
| 20/9 PROV PÅ DELMOMENT II, klockan 10.45-11.45          | 5   |
| 21/9 Cykliska grupper, Lagranges sats                   | 2.1.4-2.1.7 i del II                      |
| 22/9 Permutationsgrupper                                | 5.1 i del II                              |
| 23/9 Kryptering   | 3.2 i del II                              |
| 26/9 Övningar på grupper, dvs del III                   |   |
| 27/9 PROV PÅ DELMOMENT III, klockan 10.45-11.45         | 2.1 i del II och 5.1 i del II             |
| 29/9 Felkorrigerande koder                              | 3.1 i del II                              |
| 30/9 Boolesk algebra                                    | 7.4                                       |
| 3/10 Grafer, Eulerkretsar och Hamiltoncykler, träd      | 6.1, 6.2, 6.4-6.6                         |
| 4/10 PROV PÅ DELMOMENT IV, klockan 10.45-11.45          | 3.1-3.2 i del II och 7.4.1-7.4.3, 7.4.5   |
| 6/10 Planära grafer                                     | 7.1 i del II                              |
| 7/10 Halls bröllopsats                                  | 9.1 i del II                              |
| 10/10 Maximal matchning, alternerande stig              | 9.2 i del II                              |
| 11/10 PROV PÅ DELMOMENT V, klockan 10.45-11.45          | 7.1-7.2.3, 9.1-9.2 i II, 6.1-6.2, 6.4-6.6 |
| 13/10 Repetition, reservtid                             |   |
| 14/10 Repetition, reservtid                             |   |

## Rekommenderade övningstal och veckoöversikt:

### Kursvecka 1 och 2:

Denna vecka handlar om elementär talteori och mängdlära. Centrala begrepp är *största gemensamma delare*, *primtal* och *aritmetikens fundamentalsats*. Den satsen säger att varje tal på ett unikt sätt kan skrivas som en produkt av primtal. För att bestämma den största gemensamma delaren till tv tal använder man *Euklides algoritm* som också kan användas för att lösa den viktiga *diofantiska ekvationen*  $ax + by = z$ . Den *modulära aritmetiken* är mycket viktig i många tillämpningar.

Viktiga begrepp i *mängdläran* är *snitt*, *union* och *komplement*.

Vi studerar även *relationer* på mängder, speciellt *ekvivalensrelationer* och *funktioner*. Viktiga begrepp är *surjektiv*, *injektiv* och *bijektiv* funktion.

Under dessa veckor bör följande uppgifter räknas, antingen i skolan eller hemma:

**Kap 3:** 2, 6, 7, 11, 12, 13, 14, 17, 18, 22, 29, 30, 31, 35, 45, 46, 47, 48, 49, 54.

**Kap 2:** 9, 11, 13, 17, 31, 33, 34, 37.

**Kap 4:** 5, 9, 10, 11, 16, 17, 18, 19, 20, 45, 46, 47, 66.

**Kap 8:** 4, 5, 21, 29, 32, 34, 36, 41, 63, 69, 79.

### Kursvecka 3:

Denna vecka ägnas åt *kombinatorik*. Där ges olika metoder att få svar på frågan *på hur många sätt kan en uppgift utföras*. Viktiga metoder är *multiplikationsprincipen*, *Stirlingtal* och *kalkyl med binomialkoefficienter*.

**Kap 5:** 3, 4, 7, 9, 10, 13, 14, 16, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 41, 43, 46, 47, 52, 54, 55, 56, 57, 61, 62, 63, 65, 66, 67, 68, 70, 71, 72, 73, 75, 77, 79, 80, 83, 84.

### Kursvecka 4 och 5:

Under dessa veckor studeras den abstrakt algebraiska strukturen *grupp*. Denna struktur har visat sig ligga bakom många andra matematiska objekt. Viktiga begrepp är *delgrupp*, *ordning*, *multiplikationstabell*, *cyklisk grupp*, *sidoklass till delgrupp* och den viktiga *Lagranges sats* med vars hjälp studiet av grupper förenklas.

Vi studerar också under dessa veckor *permutationer*. Det handlar om att beskriva omflyttningar av objekt. Viktigt är *cykel representation* av permutationer, *multiplikation*, *dekomposition i tvåcykler* och begreppen *udda jämn* permutation.

Tillämpningar av abstrakt algebra finns inom teorin för *felkorrigerande koder* och inom *kryptologin*. Vi kommer att få *RSA-krypteringen* förklarad och lära oss hur man konstruerar enkla felkorrigerande koder. I samband med detta är begrepp som *avstånd* och *kontrollmatriser* fundamentala.

Under dessa veckor bör följande uppgifter räknas, antingen i skolan eller hemma:

**Kap 2 i del II:** 1, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 21, 23, 24, 25, 26, 34, 35, 36, 38, 39, 40.

**Kap 3 i del II:** 4, 5, 8, 9, 14, 17, 18, 19, 20, 29, 31, 34, 35, 37, 38, 40.

**Kap 5 i del II:** 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 16, 20, 21, 51.

**Kap 7:** 54, 55, 56, 66, 67, 69, 83, 91.

### Kursvecka 6 och 7:

Främst handlar dessa två veckor om *grafteori*. En graf består av *kanter* och *noder* och kan i tillämpningar ses som en beskrivning av samband mellan olika objekt. Viktiga begrepp är *valens*, *stig* och *cykel*, *eulerkrets*, *hamiltocykel*, *planär graf*, *Eulers formel*, *träd*, *matchning i bipartit graf* och *Halls bröllopsats*.

Under dessa veckor bör följande uppgifter räknas, antingen i skolan eller hemma:

**Kap 6:** 9, 10, 11, 12, 24, 31, 33, 34, 47, 48, 49, 55, 56, 62, 67, 86, 92.

**Kap 7.1 i del II:** 1, 2, 7, 14, 15.

**Kap 9.1-9.2 i del II:** 1, 2, 3, 4, 5, 7, 10.