Matematiska Institutionen
KTH

**Kursprogram till kursen Diskret Matematik, 5B1118, för CL3, vt2005.**

**Kursledare, föreläsare, övningsledare och examinator**:
Olof Heden
Lindstedtsvägen 25 rum 3641
Tel:7906296 (hem: 08-716 80 34)
e-post: olohed@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.

**Undervisningform:** Föreläsningar och lektioner.

**Examination:** Tentamensskrivning bestående av ungefär sju uppgifter. Inga hjälpmedel kommer att vara tillåtna vid tentamensskrivningen. Under kursens gång kommer att delas ut uppgifter som ger bonuspoäng vid tentamensskrivningen. Information om detta i samband med undervisningen och på kurshemsidan.

# UNDERVISNINGSPLAN

### Föreläsningar och lektioner

| **Innehåll** | **Avsnitt** |
|---|---|
| 17/1 Kursintroduktion, Aritmetik, primtal och diofantiska ekvationer | 3.1, 3.3 |
| 19/1 Talbaser, bevis av Aritmetikens fundamentalsats | 3.2, 3.3.4.1 |
| 21/1 Övning på kapitel 3.1-3.3 | |
| 25/1 Modulär aritmetik | 3.4 |
| 26/1 Modulär aritmetik forts. mängdlära | 3.4.1, 2.1-2.5 |
| 27/1 Övning på 3.4 och 2.1-2.5 | |
| 31/1 Rekursion, induktion, funktion | 2.6, 4.1-4.2, 8.2 |
| 2/2 Relationer, funktioner, kardinalitet | 8 |
| 3/2 Övning på 2.6, 4.1-4.2, 8 | |
| 8/2 Multiplikationsprincipen, lite sannolikhetslära | 5.1-5.3 |
| 11/2 Permutationer och urval | 5.4-5.5 |
| 11/2 Övning på kapitel 5.1-5.5 | |
| 16/2 Postfacksprincipen, inklusion exklusion | 5.6-5.7 |
| 17/2 Stirlingtal och andra uppdelningar | 5.7-5.8 |
| 18/2 Övning på kapitel 5 | |
| 22/2 Grupper introduktion, exempel | 2.1-2.1.3 i del II |
| 23/2 Cykliska grupper, Lagranges sats | 2.1.4-2.1.5 i del II |
| 24/2 Övning på kapitel 2.1-2.1.5 i del II | |
| 1/3 Isomorfa grupper, Permutationsgrupper | 2.1.6-2.1.7, 5.1-5.1.2 i del II |
| 8/3 Mer om permutationsgrupper | 5.1.3-5.1.4 i del II |
| 11/3 Övning på kapitel 2.1.6-2.1.7 och 5.1 i del II | |
| 5/4 Ringar och kroppar | 2.1.8 i del II |
| 6/4 Felkorrigerande koder | 3.1 i del II |
| 7/4 Övning på kapitel 2.1.8 och 3.1 i del II | |
| 12/4 Kryptering | 3.2 i del II |
| 13/4 Boolesk algebra | 7.4 |
| 14/4 Övning på kapitel 3.2 i del II och 7.4 | |
| 19/4 Grafer, Eulerkretsar och Hamiltoncykler | 6.1, 6.2, 6.4 |
| 20/4 Planära grafer | 7.1 i del II |
| 21/4 Övning på 6.1, 6.2 och 6.4 i del I och 7.1 i del II | |
| 26/4 Träd | 6.5-6.6 |
| 27/4 Färgläggning av grafer | 7.2-7.2.4 i del II |
| 28/4 Övning på 6.5-6.6 i del I och 7.2 i del II | |
| 3/5 Halls bröllopssats | 9.1 i del II |
| 10/5 Maximal matchning, alternerande stig | 9.2 i del II |
| 12/5 Övning på 9.1-9.2 i del II | |
| 17/5 Repetition, reservtid | |

**Rekommenderade övningstal och veckoöversikt**:

**Kursvecka 1, 2 och 3**:

Dessa tre veckor handlar om elementär talteori och mängdlära. Centrala begrepp är *största gemensamma delare*, *primtal* och *aritmetikens fundamentalsats*. Den satsen säger att varje tal på ett unkit sätt kan skrivas som en produkt av primtal. För att bstämma den största gemensamma delaren 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.

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

**Kursvecka 4 och 5**:

Dessa två veckor ägnas främst åt *kombinatorik*. Där ges olika metoder att få svar på frågan *på hur många sätt kan en uppgift utföras*. Viktiga metoder är *Inklusion exklusion*, *multiplikationsprincipen*, *Stirlingtal* och *kalkyl med binomialkoefficienter*.

Vi kommer även att se den viktiga *induktionsprincipen*. Den kan ibland användas för att verifiera att påståenden gäller allmänt för alla naturliga tal 1,2,3,... .

Under dessa veckor bör följande uppgifter räknas, antingen på övningstimmen eller hemma:

**Kap 4:** 5, 9, 10, 11, 16, 17, 18, 19, 20, 45, 46, 47, 66.
**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 6, 7 och 8**:

Under dessa tre 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 på övningstimmen 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 5 i del II:** 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 16, 20, 21, 51.

**Kursvecka 9 och 10**:

*Ringar* och *kroppar* är andra viktiga exempel på algebraiska strukturer som man måste känna till som lärare i diskret matematik. I mängden $Z_n$, som är ett viktigt exempel på en ring, kan vi både addera och multiplicera elementen. När $n$ är ett primtal kan vi även dividera och då är $Z_n$ en kropp.

Den *Booleska algebran* fick ett viktigt användningsområde när datorena började konstrueras. Tekniken med *karnaughdiagram* för att minimera antalet grindar kommer att presenteras.

Tillämpningar av abstrakt algebra finns inom teorin för *felkorrigerande koder* och inom *kryptologin*. Vi kommer att få RSA-*krypteringen* förklarad och se 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 på övningstimmen eller hemma:

**Kap 3 i del II:** 4, 5, 8, 9, 14, 17, 18, 19, 20, 29, 31, 34, 35, 37, 38, 40.
**Kap 7:** 54, 55, 56, 66, 67, 69, 83, 91.

**Kursvecka 11, 12, 13 och 14**:

Främst handlar dessa sista 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 bröllopssats*.

Under dessa veckor bör följande uppgifter räknas, antingen på övningstimmen eller hemma:

**Kap 6:** 9, 10, 11, 12, 24, 31, 33, 34, 47, 48, 49, 55, 56, 62, 67, 86, 92.
**Kap 7.1 och 7.2 i del II:** 1, 2, 7, 14, 15, 23, 24, 25, 27, 31, 32, 33.
**Kap 9.1-9.2 i del II:** 1, 2, 3, 4, 5, 7, 10.