Noen sentrale punkter i MAT 1030 pensum våren 2005

Kapittel 6: Funksjoner

Hva vil det si at en funksjon f : X --> Y er injektiv, surjektiv, bijektiv?

Hva er sammensetningen g o f : X -->Z av f : X --> Y og g : Y --> Z?

Kapittel 7: Induksjon og rekursjon

Rekursiv definisjon av en tallfølge t(n) for $n \geq 1$: gi t(1) og et uttrykk for t(n+1) som funksjon av t(n) for $n \geq 1$, evnt. som funksjon av t(1), ..., t(n).

Induksjonsbevis: For å vise at en påstand P(n) er sann for alle $n \geq 1$ er det nok å vise at P(1) er sann, og at dersom P(n) er sann så er P(n+1) sann, for hver $n \geq 1$.

Finn rekursiv karakterisering av en gitt tallfølge.

Vis ved induksjon at en rekursivt definert tallfølge er gitt ved en bestemt formel.

Annenordens lineære rekursjoner: $a\,t(n+2) + b\,t(n+1) + c\,t(n) = 0$ har løsninger $t(n) = A\,r_1^n + B\,r_2^n$ der r_1 og r_2 er røttene i den karakteristiske likningen $a\,r^2 + b\,r + c = 0$.

Kapittel 9: Kombinatorikk

n forskjellige objekter kan ordnes på n! ulike måter.

r forskjellige objekter kan velges fra n forskjellige objekter, i ordnet rekkefølge, på $n\,(n-1)\,...\,(n-r+1) = n!/(n-r)!$ ulike måter.

r forskjellige objekter kan velges fra n forskjellige objekter, uten hensyn til rekkefølgen, på $n\,(n-1)\,...\,(n-r+1)/r! = n!/r!(n-r)!$ ulike måter.

Kapittel 10: Grafteori

Summen av graden til hjørnene er lik to ganger antallet kanter.

Antallet hjørner av odde grad er et partall.

Matriserepresentasjon av en graf.

Isomorfi av grafer. Veier. Løkker.

Eulerveier og -løkker. Algoritme for å finne en Eulerløkke.

Karakterisering av eksistens av Eulervei eller -løkke ved antallet hjørner av odde grad.

Hamiltonveier og -løkker.

Kapittel 11: Trær

Vektmatriserepresentasjon av en vektet graf.

Minimale utspennende trær: Prims algoritme.

Minimal avstand: Dijkstras algoritme.

Kapittel 12: Tallteori

Heltallsdivisjon og -rest: $a = kb + r$ med $0 \leq r < b$.

Delelighet, primtall, entydig primfaktorisering.

Største felles faktor. $\gcd(a, b) = \gcd(b, r)$. Euklids algoritme.

Kongruens modulo m: Addisjon og multiplikasjon i Z/mZ.

RSA-kryptering.

Euklids algoritme baklengs: Finne y med $xy = 1 \bmod m$, når $\gcd(m, x) = 1$.

Kapittel 13: Kompleksitetsteori

Fire forenklinger.

Kompleksitetsfunksjonen f(n) = antallet dominerende operasjoner (i "worst case") som en funksjon av n = antallet bits i input, for store n.

O(g)-notasjonen.

Polynomiell kompleksitet: f(n) er $O(n^k)$ for en $k < \infty$.
