



[Kontakt] (**Aktiviteter**) [Medlemmer] [Arkiv] [Links]
 [Matilde] [MatNyt] [Nationalkomite] [Publikationer] [Preprints] [Årsmødet] [Bibliotek]
 [Sommertraef]

DMF Sommerskole Sandbjerg Gods 29.-31. august 2001

Dansk Matematisk Forening agter at afholde sommerskole i matematik på **Sandbjerg Gods** i dagene 29.- 31. august 2001.

Sommerskolen har 2. dels studerende i matematik ved landets universiteter som primære målgruppe og forudsætter en tilsvarende matematisk modenhed; skolen er dog åben for andre interesserede og er tænkt som årligt tilbagevendende.

DMF sommerskolen har et dobbelt overordnet sigte, nemlig

- at medvirke til at styrke samarbejdet i dansk matematik
- at præsentere aktuelle matematiske temaer for målgruppen

Sommerskolen vil i 2001 beskæftige sig med to forskellige aktuelle temaer.

Grafiske Modeller i Retsgenetik

v/Steffen L. Lauritzen, Institut for Matematiske Fag, Aalborg Universitet.

Moderne retsgenetik anvender DNA teknologi i stor stil for at løse identifikationsproblemer, for eksempel til at fastslå identiteten af en morder eller voldtægtsforbryder eller til at identificere lig, herunder eventuelt lig som findes i massegrave eller ved flykatastrofer o.l. Mindre morbide anvendelser omhandler dokumentation af slægtskabsforhold.

For at løse disse problemer må der foretages en sandsynlighedsberegning, som ved første øjekast ser meget uoverskuelig ud. Ved hjælp af den moderne teori for grafiske modeller i form af bayesianske netværk kan man imidlertid løse en del af disse beregningsproblemer meget simpelt og effektivt.

Der vil blive givet en introduktion dels til grundlæggende genetiske begreber, dels til bayesianske netværk, alt illustreret med eksempler fra konkrete identifikationsager.

Kendskab til elementær sandsynlighedsregning (inklusive betingede sandsynligheder og Bayes' formel) er en nødvendig forudsætning.

Algebra set fra tre synsvinkler

ved NN fra firmaet **CRYPTOMATHIC**

Kirsti Andersen og Henrik Kragh Sørensen, Institut for de Eksakte Videnskabers Historie, Aarhus Universitet

Johan P. Hansen, Matematisk Institut, Aarhus Universitet.

Den første synsvinkel er fra et aktuelt anvendelsesområde i voldsom vækst. Den personlige underskrift giver en meddelelse troværdighed. Ved overgang til elektronisk kommunikation er det nødvendigt at anvende en tilsvarende troværdighedskabende sikkerhedsfunktion - en *digital signatur*. Brevhemmeligheden sikres ganske enkelt ved at meddelelsen sendes i en lukket kuvert evt. med betroet kurer. I den elektroniske kommunikation opnås en tilsvarende brevhemmelighed ved *kryptering*. Den digitale signatur og kryptering beror i sin kerne på matematik, især talteori og algebra - vi vil se hvordan.

Den anden synsvinkel er fra en klassisk matematisk position, idet der foretages en grundlæggende matematisk behandling af dele af algebraen udvalgt med særlig relevans for kryptering, men også med et blik paa aktuelle forskningstemaer. Udgangspunktet vil være elementær talteori, men vi behandler også mere abstrakte grupper, herunder sådanne, der hidrører fra elliptiske kurver, der netop har en særlig kryptografisk interesse.

Den tredje synsvinkel er historisk med fokus på emnet "fra ligninger til abstrakt algebra". Algebraens udvikling hænger stærkt sammen med teorien for polynomiumsligninger. Forsøget på at løse ligninger og at overskue, hvilke der kan løses algebraisk, frembragte nye objekter og nye metoder. Løsning af tredjegradsligningen i 1500-tallet bevirkede, at de komplekse tal dukkede op. Studiet af deres fundament og en generalisering af dem i 1800-tallet førte til teorien for algebraer. Lagrange analyserede i slutningen af 1700-tallet ligningsløsninger og inddrog grupper af permutationer - en kim til gruppeteorien. Abel viste i 1824, at ikke alle ligninger kan løses algebraisk, hvorefter han gav sig til at studere, hvad der karakteriserer dem, der kan. Galois fortsatte denne linie og oversatte problemet til en undersøgelse af egenskaber ved visse grupper - endnu en kim til gruppeteorien og den moderne Galois-teori. Der vil i den historiske del være to foredrag og læsning af en klassisk matematisk tekst.

Lisbeth Fajstrup og Johan P. Hansen

[[Kontakt](#)] ([Aktiviteter](#)) [[Medlemmer](#)] [[Arkiv](#)] [[Links](#)]
 [[Matilde](#)] [[MatNyt](#)] [[Nationalkomite](#)] [[Publikationer](#)] [[Preprints](#)] [[Årsmødet](#)] [[Bibliotek](#)]
 [[Sommertraef](#)]

Dansk Matematisk Forening



Opdateret sidst: mandag den 3. september, 2001

<webmaster@mathematics.dk>