Bevisteknikker

- **Induktionsbeviser** (Bevis $\forall n \in \mathbb{N} : P(n)$)

  Basis: Bevis $P(0), P(1), \ldots, P(k)$

  Induktionsskridt: Bevis, at
  $P(n-1) \Rightarrow P(n)$ eller
  $(P(0) \wedge P(1) \wedge \ldots \wedge P(n-1)) \Rightarrow P(n)$
  for $n \geq k+1$

- **Modstridsbeviser** (Bevis p)

  Bruger, at

$$\begin{array}{c} p \\ \Updownarrow \\ \neg p \Rightarrow F \end{array}$$

- **Kontrapositionsbeviser** (Bevis $p \Rightarrow q$)

  Bruger, at

$$\begin{array}{c} p \Rightarrow q \\ \Updownarrow \\ \neg q \Rightarrow \neg p \end{array}$$

Talteori

Aritmetikkens Fundamentalsætning

Ethvert heltal har netop én primtalsfaktorisering

Euklids algoritme

Finder gcd(a, b) i $\leq 5\lceil \log_{10} b \rceil$ skridt

ved at udnytte, at

gcd$(a, b) =$ gcd$(b, a \bmod b)$

Kongruens

$$a \equiv b \pmod{m}$$
$$\Updownarrow$$
$$m \mid (a - b)$$
$$\Updownarrow$$
$$a \bmod m = b \bmod m$$
$$\Updownarrow$$
$$\exists k \in \mathbb{Z} : a = b + km$$

Den Kinesiske Restklassesætning

Hvis $m_1, m_2, \ldots, m_n$ er
parvis indbyrdes primiske heltal, da har

$$x \equiv a_i \pmod{m_i}, \;\; 1 \le i \le n$$

en unik løsning modulo $m_1 m_2 \ldots m_n$.

Find løsning:

Lad $m = m_1 m_2 \ldots m_n$
Lad $M_i = m/m_i, \; 1 \le i \le n$
For $i = 1$ til n
    Find invers y_i til M_i modulo m_i
    D.v.s. find y_i, så $M_i y_i \equiv 1 \pmod{m_i}$
Lad $x = \sum_{i=1}^{n} a_i M_i y_i$
Da udgør $\{x + km \mid k \in \mathbb{Z}\}$ samtlige løsninger.

Gruppeteori

En *gruppe* er en mængde G og en binær operation $\odot$, så

- G er *lukket* under $\odot$
- $\odot$ er *associativ*
- $e \in G$
- Ethvert element i G har en *invers* i G

$$a \odot b = a \odot c \;\Rightarrow\; b = c$$

$$(a^{-1})^{-1} = a$$

$$(a \odot b)^{-1} = b^{-1} \odot a^{-1}$$

Frembringere

Lad $g \in G$.
Da er $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, g^0 = e, g, g^2, \ldots\}$
en undergruppe af G.

En gruppe, som frembringes af et enkelt element, kaldes *cyklisk*.

Lagrange

$$
\begin{aligned}
H < G \;&\Rightarrow\; |H| \,\big|\, |G| \\
a \in G \;&\Rightarrow\; |a| \,\big|\, |G| \\
a \in G \;&\Rightarrow\; a^{|G|} = e
\end{aligned}
$$

Tælleteknikker

$$C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Kombinationer og permutationer af en mængde med n elementer		
Type	Med tilbagelægning	Antal forskellige
r-komb.		$C(n,r)$
r-perm.		$\frac{n!}{(n-r)!}$
r-komb.	$\times$	$C(r+n-1,r)$
r-perm.	$\times$	n^r

k kasser

$n = \sum_{i=1}^{k} n_i$ forskellige elementer

n_i elementer i kasse nr. i, $1 \leq i \leq k$

Da er der $\dfrac{n!}{n_1!n_2!\dots n_k!}$ måder at fordele elementerne i kasserne.

Inklusion-eksklusion

$$\bigcup_{i=1}^{n} A_i = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \dots + (-1)^{n-1} |\bigcap_{i=1}^{n} A_i|$$

Lad $|A| = m$ og $|B| = n, m \geq n$. Da er der

$$n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - \dots + (-1)^{n-1} C(n,n-1)$$

surjektive funktioner fra A til B.

Sandsynlighedsregning

Betinget sandsynlighed:

$$p(A \mid B) = \frac{p(A \cap B)}{p(B)}$$

Hvis alle udfald er lige sandsynlige:

$$p(A \mid B) = \frac{|A \cap B|}{|B|}$$

Uafhængige hændelser:

$$\begin{aligned} & A \text{ og } B \text{ er uafhængige} \\ \Updownarrow \; & \\ & p(A)p(B) = p(A \cap B) \\ \Updownarrow \; & \\ & p(A \mid B) = p(A) \\ \Updownarrow \; & \\ & p(B \mid A) = p(B) \end{aligned}$$

Bernoulli-forsøg

Forsøg med to mulige udfald: succes eller fiasko

p: sands. for succes

q: sands. for fiasko — d.v.s. $q = 1 - p$

Geometrisk fordeling

X: # uafh. Bernoulli-forsøg t.o.m. første succes

$p(X = k) = pq^{k-1}$

$E[X] = \frac{1}{p}$

Binomialfordeling

X: # succeser i n uafh. Bernoulli-forsøg

$p(X = k) = \binom{n}{k} p^k q^{n-k}$

$E[X] = np$

Rekursionsligninger

Lineære homogene rek.ligninger af orden 2 med konst. koeff. — d.v.s. ligninger på formen $\mathbf{a_n = c_1 a_{n-1} + c_2 a_{n-2}}$:

Opskriv karakteristisk ligning $r^2 - c_1 r - c_2 = 0$, og find rødder r_1 og r_2.

$r_1 \neq r_2$: $\quad a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$
$r_1 = r_2$: $\quad a_n = \alpha_1 r_1^n + \alpha_2 n r_1^n$

α_1 og α_2 bestemmes ud fra beg.betingelserne.

Lineære homogene rek.ligninger af orden ≥ 3

med konst. koeff. — d.v.s. ligninger på formen

$\mathbf{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}, \; k \geq 3}$:

- Opskriv kar. ligning $r^k - c_1 r^{k-1} - \ldots - c_k = 0$, og find rødder $r_1, r_2, \ldots, r_k$.

  Hvis alle k rødder er forskellige, da er $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \ldots + \alpha_k r_k^n$

- Brug frembringerfunktion

Lineære *in*homogene rek.ligninger med konst. koeff.

D.v.s. ligninger på formen

$\mathbf{a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k} + F(n), \; F(n) \neq 0}$

- Iterativ metode (hvis kun ét a-led på højresiden)

- Frembringerfunktion

- Gæt en løsning p_n. Da udgør $\{p_n + h_n \mid h_n = c_1 h_{n-1} + \ldots + c_k h_{n-k}\}$ samtlige løsninger.

Relationer

Ækvivalensrelationer

Refleksive, symmetriske og transitive

Partielle ordninger

Refleksive, antisymmetriske og transitive