Øvingsforelesning 5

TMA4140 Diskret Matematikk

Oktober 2019

"KRT, Fermats lille og kombinatorikk"

Dagen i dag

- KRT og Fermats lille
- Repetere deler av kombinatorikk: addisjonssetningen, produktssetningen, uordnede utvalg, permutasjoner med mere.
- Det blir en del midtsemesterprøve oppgaver underveis (for mange til å liste!)
- Generaliserte permutasjoner og kombinasjoner
- Å generere permutasjoner
- Rekurrensrelasjoner

Kinesisk restteorem I

Theorem

La m_1, m_2, m_3 være parvis relativt primiske positive heltall større enn en og a_1, a_2, a_3 vilkårlige heltall. Da har systemet

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ x &\equiv a_3 \mod m_3 \end{aligned}$$

en unik løsning modulo $m_1 m_2 m_3$.

Merk: Ingenting spesielt med 3 kongruenser. Det fungerer like godt med et vilkårlig endelig antall (såfremt moduliene er parvist relativt primiske).

MS14.2

Finn den negative heltallsløsningen x som har minst absoluttverdi til kongruensligningene:

$$x \equiv 3 \mod 10$$
$$x \equiv 9 \mod 17$$
$$x \equiv 12 \mod 31$$

Enkel primtallsfaktorisering

Hvordan ser vi om $n \in \mathbb{N}$ er et primtall? Hvis ingen av primtallene $p \leq \sqrt{n}$ deler n så er n et primtall. Hvis en av de deler n, så er n sammensatt.

Eksempler:

- 47
- 69

Fermats lille teorem

Theorem

La p være et primtall og $a \in \mathbb{N}$ slik at $\gcd(p, a) = 1$*. Man har da at*

$$a^{(p-1)} \equiv 1 \mod p.$$

MS15.11

Hvilke av følgende kongruensligninger er riktige?

Alt 1) $99^{99} + 1 \equiv 0 \mod 101$

Alt 2) $99^{99} \equiv 1 \mod 98$

Alt 3) $99^{99} \equiv 8 \mod 97$

Alt 4) $99^{99} + 1 \equiv 0 \mod 100$

Kombinatorikk

- Bruker noen få grunnleggende prinsipper til å gjøre mye, men ingen "oppskrifter" for hvordan man løser oppgaver

Kombinatorikk

- Bruker noen få grunnleggende prinsipper til å gjøre mye, men ingen "oppskrifter" for hvordan man løser oppgaver
- Må tenke "kreativt" i hvert enkelt tilfelle

Kombinatorikk

- Bruker noen få grunnleggende prinsipper til å gjøre mye, men ingen "oppskrifter" for hvordan man løser oppgaver
- Må tenke "kreativt" i hvert enkelt tilfelle
- Man må regne mange eksempler/oppgaver for å bli vant til tankemåten/teknikkene

Kombinatorikk

- Bruker noen få grunnleggende prinsipper til å gjøre mye, men ingen "oppskrifter" for hvordan man løser oppgaver
- Må tenke "kreativt" i hvert enkelt tilfelle
- Man må regne mange eksempler/oppgaver for å bli vant til tankemåten/teknikkene
- "Prøv alltid å tegne situasjonen"

Addisjonssetningen

Prinsipp

Hvis en handling kan gjøres på en av n_1 måter eller på en av n_2 måter, hvor ingen av de n_1 måtene er lik noen av de n_2 måtene, så er det $n_1 + n_2$ å gjennomføre handlingen.

Eksempel: På et spisested kan man som hovedrett velge mellom syv forskjellige burgere, eller tre forskjellige taco'er. Til sammen er det $7 + 3 = 10$ forskjellige ting å velge mellom til hovedrett.

Utvalg/kombinasjoner I

- Med utvalg/kombinasjoner mener vi uordnede utvalg av elementer fra en mengde.

Utvalg/kombinasjoner I

- Med utvalg/kombinasjoner mener vi uordnede utvalg av elementer fra en mengde.
- **Eksempel:** La S være $\{1, 2, 3, 4\}$. $\{2, 3, 4\}$ er en 3-kombinasjon fra S. Som kombinasjon er denne lik både $\{3, 2, 4\}$ og $\{4, 3, 2\}$.

Utvalg/kombinasjoner I

- Med utvalg/kombinasjoner mener vi uordnede utvalg av elementer fra en mengde.
- **Eksempel:** La S være $\{1, 2, 3, 4\}$. $\{2, 3, 4\}$ er en 3-kombinasjon fra S. Som kombinasjon er denne lik både $\{3, 2, 4\}$ og $\{4, 3, 2\}$.
- **Eksempel:** Hvor mange forskjellige komiteer kan dannes ut av en gruppe av fire studenter? (Hint: samme som å velge en student!)

Utvalg/kombinasjoner I

Theorem

Antallet r-kombinasjoner av en mengde av n elementer, hvor $n \in \mathbb{N}$ *og* $0 \leq r \leq r$*, er lik*

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

Husk: $n! = n \cdot (n-1) \cdots 2 \cdot 1$ og at vi også skriver $C(n, r) = \binom{n}{r}$.

MS14.6

Hvor mange binære strenger av lengde 12 inneholder nøyaktig fem eller nøyaktig syv 0'er?

Alt 1) 12

Alt 2) 792

Alt 3) 1584

Alt 4) $5^{12} + 7^{12}$

Trediagram

- Vi kan bruke trediagram til å telle. Trær består av en rot, grener, og eventuelt flere grener som forlater endepunktene av andre grener. **Prinsipp**: En gren for hvert valg.

Trediagram

- Vi kan bruke trediagram til å telle. Trær består av en rot, grener, og eventuelt flere grener som forlater endepunktene av andre grener. **Prinsipp**: En gren for hvert valg.
- **Eksempel 1:** Hvor mange binære strenger av lengde tre som inneholder minst én 1'er finnes det?

Trediagram

- Vi kan bruke trediagram til å telle. Trær består av en rot, grener, og eventuelt flere grener som forlater endepunktene av andre grener. **Prinsipp**: En gren for hvert valg.
- **Eksempel 1:** Hvor mange binære strenger av lengde tre som inneholder minst én 1'er finnes det?
- **Eksempel 2:** Hvor mange binære strenger av lengde fire som ikke inneholder to eller flere 1'ere på rad finnes det?
- **Digresjon:** Finnes bedre måter å telle eksempel 1 på, f.eks. ved å se at alle bitstrenger av lengde tre utgjøres av de med minst én 1'er og de med ingen 1'ere.

MS12.5: Trediagram, eller add.setning og utvalg, eller annet

La $f : \{a, b, c\} \to \{1, 2\}$. Hvor mange surjektive funksjoner f finnes det?

Alt 1) 9

Alt 2) 12

Alt 3) 6

Alt 4) 8

Produktsetningen

Prinsipp

Anta at en prosedyre kan brytes ned i en sekvens av to handlinger. Hvis det er n_1 måter å gjøre den første handlingen og n_2 måter å gjøre den andre handlingen, så er det $n_1 \cdot n_2$ måter å gjøre handlingen på.

Produktsetningen

Prinsipp

Anta at en prosedyre kan brytes ned i en sekvens av to handlinger. Hvis det er n_1 måter å gjøre den første handlingen og n_2 måter å gjøre den andre handlingen, så er det $n_1 \cdot n_2$ måter å gjennomføre hele handlingen.

Eksempler:

- En pinkode til et bankkort består av fire siffer. Gitt at det er ti forskjellige siffer, blir det 10^4 forskjellige mulige pinkoder.

Produktsetningen

Prinsipp

Anta at en prosedyre kan brytes ned i en sekvens av to handlinger. Hvis det er n_1 måter å gjøre den første handlingen og n_2 måter å gjøre den andre handlingen, så er det $n_1 \cdot n_2$ måter å gjennomføre hele handlingen.

Eksempler:

- En pinkode til et bankkort består av fire siffer. Gitt at det er ti forskjellige siffer, blir det 10^4 forskjellige mulige pinkoder.
- Hvis det er 7 forskjellige burgere, 2 forskjellig typer fries og 2 forskjellige måter å oppgradere fries på, så er det $7 \cdot (2 \cdot 3) = 42$ forskjellige kombinasjoner av burgere og fries.

MS15.12: Utvalg og produktsetningen

En gruppe på 8 menn og 5 kvinner skal fordeles på en komite bestående av 6 personer. Hvor mange komiteer kan man danne som har 4 menn og 2 kvinner?

Alt 1) 280

Alt 2) 1716

Alt 3) 700

Alt 4) 225

MS14.6

Betrakt funksjoner $f : X \to Y$, der $X = \{a, b, c\}$ og $Y = \{1, 2, 3, 4, 5, 6\}$. Hvilke av følgende utsagn er sanne?

Alt 1) Det er 216 forskjellige funksjoner f.

Alt 2) Det er 120 injektive funksjoner f.

Alt 3) Det er 3^6 forskjellige funksjoner f.

Alt 4) Det er $\binom{6}{3}$ injektive funksjoner f.

Hanske-skuffe-prinsippet

Theorem

Hvis k er et positivt heltall og $k+1$ eller flere objekter blir plassert i k esker, så må det være minst en eske som inneholder to eller flere av objektene.

Merk: På engelsk er dette "the Pigeonhole Principle".

Hanske-skuffe-prinsippet

(**Merk:**På engelsk er dette "the Pigeonhole Principle".)

Theorem

Hvis k er et positivt heltall og $k+1$ eller flere objekter blir plassert i k esker, så må det være minst en eske som inneholder to eller flere av objektene.

Eksempler:

- I enhver gruppe av 367 mennesker finnes det minst to som har samme bursdag siden det er kun 366 mulige fødselsdager.

Hanske-skuffe-prinsippet

(**Merk:**På engelsk er dette "the Pigeonhole Principle".)

Theorem

Hvis k er et positivt heltall og $k+1$ eller flere objekter blir plassert i k esker, så må det være minst en eske som inneholder to eller flere av objektene.

Eksempler:

- I enhver gruppe av 367 mennesker finnes det minst to som har samme bursdag siden det er kun 366 mulige fødselsdager.
- En funksjon $f : X \to Y$ med $|Y| = k < |X| < \infty$ kan ikke være injektiv.

Hanske-skuffe-prinsippet

(**Merk:**På engelsk er dette "the Pigeonhole Principle".)

Theorem

Hvis k er et positivt heltall og $k+1$ eller flere objekter blir plassert i k esker, så må det være minst en eske som inneholder to eller flere av objektene.

Eksempler:

- I enhver gruppe av 367 mennesker finnes det minst to som har samme bursdag siden det er kun 366 mulige fødselsdager.
- En funksjon $f : X \to Y$ med $|Y| = k < |X| < \infty$ kan ikke være injektiv.
- Hvor mange tall må velges fra mengden $\{1, 2, 3, 4, 5, 6\}$ for å garantere at det minst et par av tallene som adderer opp til 7?

MS14.12

La A være en delmengde av $\{1, 3, 5, 7, 9, 11, 13, 15\}$. Hvilke av følgende verdier av $|A|$ ($=$ antall elementer i A) garanterer at minst et par av (distinkte) tall i A adderer til et tall større enn 20?

Alt 1) 6

Alt 2) 4

Alt 3) 7

Alt 4) 5

Permutasjoner I

- Med en permutasjon av en mengde **distinkte** elementer, mener vi en bestemt måte å sette elementene i en (**ordnet**) rekkefølge.

Permutasjoner I

- Med en permutasjon av en mengde **distinkte** elementer, mener vi en bestemt måte å sette elementene i en (**ordnet**) rekkefølge.
- En er også interessert i ordnede rekkefølger undermengder av en gitt mengde, og snakker derfor om r-permutasjoner.

Permutasjoner I

- Med en permutasjon av en mengde **distinkte** elementer, mener vi en bestemt måte å sette elementene i en (**ordnet**) rekkefølge.
- En er også interessert i ordnede rekkefølger undermengder av en gitt mengde, og snakker derfor om r-permutasjoner.
- **Eksempel 1:** La $S = \mathbf{1,2,3,4}$. Da er $1, 2, 3, 4$ og $2, 3, 4, 1$ to forskjellige permutasjoner av S. Disse er forskjellige.

Permutasjoner I

- Med en permutasjon av en mengde **distinkte** elementer, mener vi en bestemt måte å sette elementene i en (**ordnet**) rekkefølge.
- En er også interessert i ordnede rekkefølger undermengder av en gitt mengde, og snakker derfor om r-permutasjoner.
- **Eksempel 1:** La $S = \mathbf{1,2,3,4}$. Da er $1, 2, 3, 4$ og $2, 3, 4, 1$ to forskjellige permutasjoner av S. Disse er forskjellige.
- **Eksempel 2:** La S være som i forrige. $2, 3, 4$ er da en 3-permutasjon av S. $1, 4$ er en 2-permutasjon av S.

Permutasjoner II

Theorem

Hvis n er et positivt heltall og r er et heltall med $1 \leq r \leq n$, så er det

$$P(n, r) = n \cdot (n-1) \cdot \cdots \cdot (n-r+1)$$

forskjellige r-permutasjoner av en mengde med n distinkte elementer.

Permutasjoner II

Theorem

Hvis n er et positivt heltall og r er et heltall med $1 \leq r \leq n$, så er det

$$P(n, r) = n \cdot (n-1) \cdot \cdots \cdot (n-r+1)$$

forskjellige r-permutasjoner av en mengde med n distinkte elementer.

Eksempler:

- Det er $3 \cdot 2 = 6$ forskjellige 2-permutasjoner av $\{1, 2, 3\}$.

MS15.5

Hvor mange forskjellige strenger kan dannes av bokstavene i AARDVARV dersom de tre A'ene skal forekomme i rekkefølge etter hverandre?

Alt 1) 1680

Alt 2) 180

Alt 3) 720

Alt 4) 360

Generaliserte kombinasjoner

Hvordan teller man hvor mange måter man kan plassere n ikke-distingverbare elementer i r distingverbare bokser?
$C(r + n - 1, n)!$

Å generere permutasjoner I

- Av og til ønsker man å kunne skrive ned alle permutasjonene av en mengde.

Å generere permutasjoner I

- Av og til ønsker man å kunne skrive ned alle permutasjonene av en mengde.
- Vi kan sette alle n-elements mengder i en-til-en samsvar med $\{1, 2, 3, \ldots, n\}$.

Å generere permutasjoner I

- Av og til ønsker man å kunne skrive ned alle permutasjonene av en mengde.
- Vi kan sette alle n-elements mengder i en-til-en samsvar med $\{1, 2, 3, \ldots, n\}$.
- Vi bruker leksikografisk ordning av permutasjoner: $a_1 a_2 \cdots a_n$ forekommer før $b_1 b_2 \cdots b_n$ hvis det finnes en $1 \leq k \leq n$ slik at $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_{k-1} = b_{k-1}$ og $a_k < b_k$.

Å generere permutasjoner I

- Av og til ønsker man å kunne skrive ned alle permutasjonene av en mengde.
- Vi kan sette alle n-elements mengder i en-til-en samsvar med $\{1, 2, 3, \ldots, n\}$.
- Vi bruker leksikografisk ordning av permutasjoner: $a_1 a_2 \cdots a_n$ forekommer før $b_1 b_2 \cdots b_n$ hvis det finnes en $1 \leq k \leq n$ slik at $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_{k-1} = b_{k-1}$ og $a_k < b_k$.
- Dette er også kjent som en "dictionary ordering".

Å generere permutasjoner I

- Av og til ønsker man å kunne skrive ned alle permutasjonene av en mengde.
- Vi kan sette alle n-elements mengder i en-til-en samsvar med $\{1, 2, 3, \ldots, n\}$.
- Vi bruker leksikografisk ordning av permutasjoner: $a_1 a_2 \cdots a_n$ forekommer før $b_1 b_2 \cdots b_n$ hvis det finnes en $1 \leq k \leq n$ slik at $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_{k-1} = b_{k-1}$ og $a_k < b_k$.
- Dette er også kjent som en "dictionary ordering".
- 23415 forekommer før 23514.

Å generere permutasjoner II

Eksempler:

- Alle permutasjonene på $\{1, 2, 3\}$.

Å generere permutasjoner II

Eksempler:

- Alle permutasjonene på $\{1, 2, 3\}$.
- **6.6 Oppgave 5c):** Finn den neste permutasjonen etter 12453.

Rekurrensrelasjoner

Theorem

En lineær homogen rekurrensrelasjon av grad k med konstante koeffisienter er en rekurrens relasjon av formen

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdot + c_k a_{n-k}$$

hvor $c_1, c_2, \ldots, c_k$ *er reelle tall, og* $c_k \neq 0$.