Noter om induktion

Christoffer Øhrstrøm

4. november 2015

Indhold

1 Introduktion

Induktion er en bevisteknik til at vise, at en påstand gælder for et basistilfælde og derefter også gælder for alle efterfølgende tilfælde. Et klassisk eksempel er at bevise, at summen af alle naturlige tal fra 1 til n er givet ved

$$\frac{n \cdot (n+1)}{2}$$

Påstanden er altså:

$$P(n) : \sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$$

Vi vil gerne bruge induktion til at vise, at dette gælder for alle $n \in \mathbb{N}$. Dette gør vi ved at vise et basistilfælde og et induktionstrin.

Basistilfælde Da påstanden skal vises at være sand for alle $n \in \mathbb{N}$, så må basistilfældet fås for $n = 1$, da 1 er det mindste naturlige tal. Ved indsættelse af $n = 1$ fås

$$\sum_{i=1}^{1} i = 1 = \frac{1 \cdot (1+1)}{2}$$

Det ses deraf, at $P(1)$ er sand, hvorfor vi har fundet et basistilfælde.

Induktionstrin I et induktionstrinnet antages det, at påstanden $P(k)$ er sand for et $k \geq b$, hvor b er tallet fra basistilfældet. I dette tilfælde er $b = 1$. Førnævnte antagelse kaldes for induktionsantagelsen. Under induktionsantagelsen vil vi nu vise, at $P(k+1)$ er sand. Hvis vi kan vise dette, vil det sætte en kædereaktion i gang: Hvis påstanden gælder for $n = 1$, så gælder den også for $n = 2$; hvis påstanden gælder for $n = 2$, så gælder den også for $n = 3$ osv.
Påstanden $P(k+1)$ er

$$\sum_{i=1}^{k+1} i = \frac{(k+1) \cdot ((k+1)+1)}{2} \tag{1}$$

Når vi gerne vil vise en påstand omkring en sum, så er det ofte et nyttigt trick at hive det sidste led ud af summen. I dette tilfælde giver det ligheden

$$\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i \right) + (k+1)$$

Det smarte ved dette trick er, at vi nu har omskrevet summen til en form, hvor et af ledene kan erstattes med et lukket udtryk, da det passer med induktionsantagelsen. Ofte vil man i induktionstrinnet omskrive et udtryk, så det bliver muligt at anvende induktionsantagelsen.

$$\left(\sum_{i=1}^{k} i \right) + (k+1) = \frac{k \cdot (k+1)}{2} + (k+1)$$

Resten af dette induktionstrin går nu ud på at omskrive udtrykket, så vi får det på samme form som i ligning (1).

$$\begin{aligned}
\frac{k \cdot (k+1)}{2} + (k+1) &= \frac{k \cdot (k+1)}{2} + \frac{2}{2} \cdot (k+1) \\
&= \frac{k \cdot (k+1) + 2 \cdot (k+1)}{2} \\
&= \frac{(k+2) \cdot (k+1)}{2} \\
&= \frac{(k+1) \cdot ((k+1)+1)}{2}
\end{aligned}$$

Altså ses det, at udtrykket er sandt for $k+1$, hvis det er sandt for k.

Konklusion Jævnfør princippet for matematisk induktion er

$$\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$$

for alle $n \in \mathbb{N}$.

2 Basistilfældets betydning

Induktion fungerer ikke, hvis der ikke er et basistilfælde, da der i så fald ikke er noget, som sætter kædereaktionen i gang. Lad os illustrere det i følgende eksempel, hvor vi betrager følgen defineret ved

$$\begin{aligned} a_1 &= 1 \\ a_n &= a_{n-1} + 2 \qquad\qquad\qquad n > 1 \end{aligned}$$

Følgen definerer altså alle de positive ulige tal. Vi vil nu forsøge at bevise påstanden

$$P(n) : 2 \mid a_n$$

for alle $n \in \mathbb{N}$. Påstanden kan også formuleres sådan, at a_n er et lige tal (påstanden er naturligvis falsk). I første omgang bekymrer vi os ikke om basistilfældet og går direkte til induktionstrinnet.

Induktionstrin Induktionsantagelsen er, at $2 \mid a_k$ for et $k \geq b$, hvor b endnu ikke er bestemt. Vi vil nu vise, at $2 \mid a_{k+1}$. Husk at $a_{k+1} = a_k + 2$. Det vides fra induktionsantagelsen, at 2 er en divisor i a_k, og 2 er trivielt en divisor i sig selv. Altså har vi

$$2 \mid a_k \;\wedge\; 2 \mid 2 \implies 2 \mid (a_k + 2) \implies 2 \mid a_{k+1}$$

Det ses således, at hvis a_k er et lige tal, så er a_{k+1} også et lige tal. Deraf ses det, at på trods af at påstanden er falsk, så kan vi godt fuldføre induktionstrinnet.

Basistilfælde Vi kan lave et modstridsbevis til at vise, at der ikke findes noget b for hvilket, $P(b)$ er sand. Beviset fremføres kort her, men er ikke essentielt for at forstå betydningen af basistilfældet i induktion.

Antag at der findes et $b \in \mathbb{N}$, så $P(b)$ er sand. Dvs., at a_b er et lige tal. Det ses ud fra definitionen af følgen $(a_n)_{n\in\mathbb{N}}$, at $b \neq 1$, da $a_1 = 1$ er et ulige tal. Vi omskriver nu udtrykket for a_n for $n > 1$.

$$a_{n-1} = a_n - 2$$

Altså er $a_{b-1} = a_b - 2$ et lige tal ved samme type argumentation som i induktionstrinnet. Men da må også $a_{b-2}, a_{b-3}, \ldots, a_{b-(b-1)}$ være lige tal. Da $a_{b-(b-1)} = a_1 = 1$ ved vi, at dette ikke kan være sandt. Derfor er antagelsen forkert. Der findes altså ikke et $b \in \mathbb{N}$, så $P(b)$ er sand.

3 Eksempler på induktionsbeviser

I følgende eksempler vil der mest være fokus på nyttige tricks i forskellige typer induktionsbeviser og ikke på strukturen i et induktionsbevis, da denne er blevet gennemgået i de to foregående afsnit.

3.1 Sum af kvadrattal

Vi vil nu bevise påstanden

$$P(n) : \sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6}$$

for alle $n \in \mathbb{N}$.

Basistilfælde Det mindste naturlige tal er $b = 1$ og ved indsættelse fås

$$\sum_{i=1}^{1} i^2 = 1^2 = 1 = \frac{6}{6} = \frac{2 \cdot 1^3 + 3 \cdot 1^2 + 1}{6}$$

Basistilfældet ses altså at være sandt.

Induktionstrin Vi antager, at $P(k)$ er sand for et $k \geq 1$. Ligesom i introduktionen vil vi bruge tricket med at hive det sidste led ud af summen og derefter gøre brug af induktionsantagelsen.

$$\begin{aligned}\sum_{i=1}^{n+1} i^2 &= \left(\sum_{i=1}^{n} i^2\right) + (n+1)^2 \\ &= \frac{2n^3 + 3n^2 + n}{6} + (n+1)^2\end{aligned}$$

Den resterende del af induktionstrinnet går ud på at omskrive dette udtryk ved brug af aritmetik.

$$\begin{aligned}\sum_{i=1}^{n+1} i^2 &= \frac{2n^3 + 3n^2 + n}{6} + (n+1)^2 \\ &= \frac{2n^3 + 3n^2 + n + 6 \cdot (n+1)^2}{6} \\ &= \frac{2n^3 + 3n^2 + n + 6 \cdot (n^2 + 2n + 1)}{6} && \text{fordi } (n+1)^2 = n^2 + 2n + 1 \\ &= \frac{2n^3 + 3(n+1)^2 + n + 3n^2 + 3 \cdot (n^2 + 2n + 1)}{6} && \text{fordi } (n+1)^2 = n^2 + 2n + 1 \\ &= \frac{2(n+1)^3 + 3(n+1)^2 + (n+1)}{6} && \text{fordi } (n+1)^3 = n^3 + 3n^2 + 3n + 1\end{aligned}$$

Konklusion Jævnfør princippet for matematisk induktion er

$$\sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6}$$

for alle $n \in \mathbb{N}$.

3.2 Maksimale antal knuder i binært træ

Induktion kan også bruges i andre sammenhænge end summer. Her vil vi se på et eksempel med et binært træ, hvor tricket er at formulere egenskaben ved at bruge de naturlige tal. Husk at højden af et binært træ er antallet af kanter på den længste vej fra roden af træet til et blad.

Vi ønsker at bevise, at det maksimale antal knuder i et binært træ med højde h er $2^{h+1} - 1$. Lad $B(h)$ være det maksimale antal knuder i et binært træ med højde h. Vores påstand er altså:

$$P(h) : B(h) = 2^{h+1} - 1$$

for alle $h \in \mathbb{N} \cup \{0\}$.

Basistilfælde Basistilfældet fås for en højde $h = 0$. Når $h = 0$ kan der ikke være mere end en enkelt knude i træet, da højden ellers ville være større end 0. Altså er

$$B(h) = 1 = 2^1 - 1 = 2^{0+1} - 1$$

Vi ved nu, at $P(0)$ er sand.

Induktionstrin Antag at $P(k)$ er sand for et $k \geq 0$. Dvs., at det maksimale antal knuder i et binært træ med højde k er $2^{k+1} - 1$. Vi ønsker nu at vise $P(k+1)$ - nemlig at det maksimale antal knuder i et binært træ med højde $k+1$ er $2^{(k+1)+1} - 1$.
Betragt nu et træ T_k med højde k som har det maksimale antal knuder for dets højde. Det er ensbetydende med, at alle knuder - som ikke er blade - har præcis 2 børn. Hvis hvert blad i T_k får 2 børn, vil der konstrueres et træ T_{k+1} med højde $k+1$, som har det maksimale antal knuder for dets højde. Antallet af børn der bliver lagt til T_k for at danne T_{k+1} er lig 2^{k+1}. Dette bør egentlig bevises (med induktion), men vi nøjes her med at give intuitionen bag det: Første niveau i træet har maks. $1 = 2^0$ knude (roden), andet niveau har maks. $2 = 2^1$ knuder, tredje niveau har maks. $4 = 2^2$ knuder osv. Derfor

er

$$\begin{aligned}B(k+1) &= B(k) + 2^{k+1}\\ &= (2^{k+1}-1) + 2^{k+1}\\ &= 2\cdot 2^{k+1} - 1\\ &= 2^{(k+1)+1} - 1\end{aligned}$$

Dermed har vi nu vist, at hvis $P(k)$ er sand, så er $P(k+1)$ også sand.

Konklusion Jævnfør princippet for matematisk induktion er det maksimale antal knuder i et binært træ med højde h lig $2^{h+1}-1$ for alle $h \in \mathbb{N} \cup \{0\}$.

4 Løkkeinvarianter

I algoritme studiet vil man typisk gerne vise, at ens algoritme er korrekt. Idet løkker ofte indgår i ens algoritmer, er løkkeinvarianter et nyttigt redskab til at vise korrekthed. Løkkeinvarianter knytter sig meget tæt til induktion: For at bevise en løkkeinvariant (påstand i induktion) skal man først vise, at den gælder før løkken køres (induktionsstart). Dernæst skal man, under antagelse af at løkkeinvarianten er sand før en iteration af løkken, vise, at den også er sand efter iterationen (induktionstrin). Til sidst skal man vise at løkken vil terminere og bruge løkkeinvarianten til at bevise korrekthed for algoritmen. Det er først i sidste trin, at løkkeinvarianter for alvor skiller sig ud fra induktion. Se følgende eksempel for, hvordan man kan bruge en løkkeinvariant til at bevise korrektheden af en algoritme.

Vi laver en algoritme Count, som skal beregne $\text{Count}(x) = x$ for $x \in \mathbb{N} \cup \{0\}$ og ønsker at bevise, at den laver beregningen korrekt. Algoritmen er skrevet i pseudokode i algoritme 1.

Algorithm 1 Count(x)

$y = 0$
$z = x$
while $z > 0$ **do**
    $y = y + 1$
    $z = z - 1$
end while
return y

Vi formulerer nu løkkeinvarianten:

$$x = y + z$$

Løkkestart Før løkken har kørt første iteration er $y = 0$ og $z = x$. Altså er $y + z = 0 + x = x$ og løkkeinvarianten er således sand i dette tilfælde.

Løkketrin Vi antager, at løkkeinvarianten gælder ved starten af en iteration af løkken i linje 3-6 og ønsker at vise, at løkkeinvarianten også gælder efter iterationen. Vi ved fra løkkeinvarianten, at $x = y + z$ ved starten af iterationen. I løbet af iteratonen udføres linje 4 og linje 5, der forøger værdien af y med 1 og formindsker værdien af z med 1. Efter iterationen fås der således

$$(y + 1) + (z - 1) = y + z + (1 - 1) = y + z = x$$

hvilket viser, at løkkeinvarianten også gælder efter iterationen.

Termination Da vi kun arbejder med $z \in \mathbb{N} \cup \{0\}$, løkken kun køres for $z > 0$, og z formindskes med 1 i hver iteration, så ved vi, at løkken må terminere. Når løkken terminerer, må det gælde, at $z = 0$. Vi kan nu bruge løkkeinvarianten til at se, at

$$x = y + z = y + 0 = y$$

Ved at returnere y, gives der altså x tilbage.