Bevis og Bevisteknikker

Se på påstanden

"Summen av to partall er et partall"

Dette er sant!

For å være sikker på at dette er sant for alle partall, må vi gi et generelt bevis.

Først: hva er et partall?

Et heltall n er et partall dersom det finnes et heltall m slik at $n = 2 \cdot m$.

Vi kan nå bevise at

"Hvis x og y er partall, så er $x+y$ et partall".

Anta at x og y er partall.

Da er $x = 2 \cdot n$ og $y = 2 \cdot m$ for to heltall n og m.

Videre er $x+y = 2n + 2m = \underbrace{2(n+m)}$

Partall, siden $n+m$ er et heltall.

Så $x+y$ er et partall hvis x og y er partall. ∎

Hva er et bevis?

Vi kan si at et bevis er en logisk forklaring på hvorfor noe er sant.

Ulike grader av grundighet eller formalitet:

- Muntlige forklaringer
- Skriftlig (med flere eller færre detaljer)
- Bevis som kan leses (og verifiseres) av en datamaskin.

Menge ulike bevisteknikker:

- Direkte bevis (Eksempelet i starten, $P \to Q$)
- Kontrapositivt bevis ($P \to Q \equiv \neg Q \to \neg P$)
- Motsigelsesbevis ($\neg P \to \bot$)
- Motbevis
- Induksjonsbevis (om noen uker)
- ...

Eksempel (Bevis ved moteksempel/motbevis)

Se på påstanden

"Fire heltall addert sammen blir alltid et partall"

Dette er usant!

Kan motbevises ved ett moteksempel:

$$1+1+1+2 = 5$$

Generelt kan en påstand på formen

$\forall x P(x)$ (som ikke er sann) motbevises ved å

bevise $\neg \forall x P(x) \equiv \exists x \neg P(x)$ (ofte ved å finne en passende x)

Ikke-konstruktive bevis

Vi ønsker å bevise en påstand $\exists x\, P(x)$.

Én mulighet: finn en passende x (konstruktivt bevis)

Eksempel

Påstand: $\exists x \in \mathbb{N}$ slik at $x^2 = 4$.

Bevis: La $x = 2$.

En annen mulighet: Vis indirekte at en passende x må finnes, uten nødvendigvis å finne den.

Eksempel

La $U = \{1, 2, \dots, 15\}$.

La A, B og C være delmengder av U, alle med 11 elementer. Altså $|A| = |B| = |C| = 11$.

Påstand: $\exists x \in U$ slik at $x \in A \wedge x \in B \wedge x \in C$, med andre ord $A \cap B \cap C \neq \emptyset$.

Bevis

La oss undersøke $\overline{A \cap B \cap C}$.

Vi har at $\overline{A \cap B \cap C} = \underbrace{\bar{A} \cup \bar{B} \cup \bar{C}}_{\uparrow}$.

Hvor mange elementer har vi her?

Vi har at $|\bar{A}| = |\bar{B}| = |\bar{C}| = 4$.

Så vi har maksimalt $4 \cdot 3 = 12$ elementer i

$$\bar{A} \cup \bar{B} \cup \bar{C} = \overline{A \cap B \cap C}$$

Siden $\overline{A \cap B \cap C} = U \setminus A \cap B \cap C$ har maks 12 elementer,

så har $A \cap B \cap C$ minst 3 elementer.

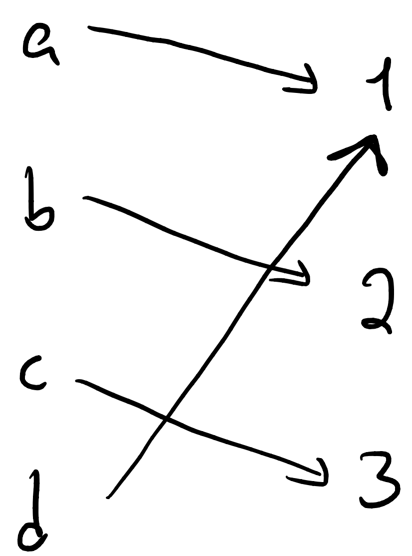
Altså må det eksistere en x i $A \cap B \cap C$. $\square$

Beviset over kan kalles et "bevis ved telling".
I slike bevis brukes ofte det såkalte
"<u>due-hull-prinsippet</u>" (pigeon hole principle):

Hvis 10 duer skal plasseres i 9 fuglekasser, må det være minst to duer i minst én av kassene.

Generelt: hvis $n+1$ objekter skal fordeles i n grupper, vil det eksistere en gruppe med minst to objekter.

Dette fører også f.eks. til at en funksjon fra $\{a, b, c, d\}$ til $\{1, 2, 3\}$ umulig kan være injektiv:



Kan ikke unngå at to ting sendes til det samme.

Ikke injektiv!

Kontrapositive bevis

Noen ganger er det vanskelig å finne et direkte bevis for $P \to Q$.

Heldigvis: $P \to Q \equiv \neg P \lor Q \equiv Q \lor \neg P \equiv \neg(\neg Q) \lor \neg P$

$$\equiv \underbrace{\neg Q \to \neg P}_{\text{Noen ganger enklest å bevise denne!}}$$

$\neg Q \to \neg P$ kalles den kontrapositive til $P \to Q$.

Eksempel

Vis det følgende.

La n være et heltall.

Hvis n^2 er et partall, så er n et partall.

Altså, skal vi vise

$$\forall n \in \mathbb{Z}\,(n^2 \text{ partall} \rightarrow n \text{ partall}).$$

Prøver med direkte bevis:

Anta at n^2 er et partall. Da er $n^2 = 2m$, $m \in \mathbb{Z}$.

Vi får at $n = \sqrt{2m}$, men kommer ikke videre med det

☹

Prøver heller med den kontrapositive:

La $P(n) \equiv n^2$ er et partall og

$Q(n) \equiv n$ er et partall.

Kan bytte ut $P(n) \to Q(n)$ med $\neg Q(n) \to \neg P(n)$,

og heller vise at

$$\forall n \in \mathbb{Z} \left(\neg Q(n) \to \neg P(n) \right)$$

Hva betyr $\neg P(n)$?

$\neg P(n) \equiv$ "n^2 er ikke et partall" $\equiv$ "n^2 er et oddetall"

og $\neg Q(n) \equiv$ "n er et oddetall"

Så vi ønsker altså å vise at

Hvis n er et oddetall, så er n^2 et oddetall.

Hvis n er odde, kan vi skrive $n = 2m+1$, $m \in \mathbb{Z}$.

Da er $n^2 = (2m+1)^2 = 4m^2 + 4m + 1$

$$= 2(2m^2+2m)+1 = \underbrace{2m' + 1}_{\text{Oddetall!}}$$

der $m' = 2m^2 + 2m$

Siden vi har vist at

"n odde $\to$ n^2 odde" har vi også vist

"n^2 er partall $\to$ n er partall". $\square$

Motsigelsesbevis

Vi ønsker å bevise en påstand P.

Hvis det er vanskelig å bevise at P er sann, kan vi prøve å bevise at P umulig kan være usann.

Hvis vi viser at $\neg P$ fører til en motsigelse, må P være sann:

$$\neg P \to \bot \equiv \neg(\neg P) \vee \bot \equiv P \vee \bot \equiv P$$

Eksempel

Vis at $\sqrt{2}$ er et irrasjonalt tall.
Altså, vis at det ikke finnes heltall a, b slik at $\sqrt{2} = \frac{a}{b}$.

Bevis

Anta at $\sqrt{2}$ er et rasjonalt tall, altså at $\sqrt{2} = \frac{a}{b}$ for heltall a og b, hvor a og b ikke har noen felles faktorer.

Siden $\sqrt{2} = \frac{a}{b}$, vil $2 = \frac{a^2}{b^2}$ eller $a^2 = 2b^2$.

Da er a^2 et partall, og da er a et partall.

Så la $a = 2m$, $m \in \mathbb{Z}$.

Da er $2b^2 = a^2 = (2m)^2 = 4m^2$ og dermed $b^2 = 2m^2$.

Da er b^2 et partall, og dermed er b et partall.

Da er både a og b partall, og har felles faktorer, som går mot antakelsen vår.

Så det kan ikke stemme at $\sqrt{2} = \frac{a}{b}$, så $\sqrt{2}$ må være et irrasjonalt tall. ■