Indhold

1

Indtroduktion

Deductive Reasoning (deduktion på dansk) er måden hvorpå vi finder svar i matematik, for eksempel ved at finde x i en ligning. Deduktion bruges også i *beviser*, som er hvad vi kigger på i den her bog.

Definition 1.1 (Primtal)
Et primtal er et tal der ikke kan blive skrevet som et produkt af to mindre positive tal.

Definition 1.2 (Sammensat tal)
Et sammensat tal er det et primtal ikke er, altså et tal som kan findes ved produktet af to andre tal. (*Composite Number* på engelsk.)

Definition 1.3 (Formodning)
Formodning, på engelsk *conjecture* er en erklæring som endnu ikke er bevist.

Der bliver i bogen givet følgende eksempel med heltal fra 2 til 10,

n	*Er n et primtal?*	$2^n - 1$	*Er $2^n - 1$ et primtal?*
2	ja	3	ja
3	ja	7	ja
4	nej, $4 = 2 \cdot 2$	15	nej, $15 = 3 \cdot 5$
5	ja	31	ja
6	nej, $6 = 2 \cdot 3$	63	nej, $63 = 7 \cdot 9$
7	ja	127	ja
8	nej, $8 = 2 \cdot 4$	255	nej, $255 = 15 \cdot 17$
9	nej, $9 = 3 \cdot 3$	511	nej, $511 = 7 \cdot 73$
10	nej, $10 = 2 \cdot 5$	1023	nej, $1023 = 31 \cdot 33$

Tabel 1.1: Primtalssammenhæng mellem positive heltal og $2^n - 1$

hvorvidt de er primtal, og 2 opløftet i tallet minus 1, og om hvorvidt disse også er primtal:

Ud fra den her tabel kan man som matematiker lave det man på engelsk kalder *conjectures* (i disse noter, og måske generelt på dansk, formodninger), hvor vi *gætter* på at en erklæring er sand.

Formodning 1.4

Antag at n er et heltal større end 1 og n er et primtal. Så er $2^n - 1$ også et primtal.

Formodning 1.5

Antag at n er et heltal større end 1 og n ikke er et primtal. Så er $2^n - 1$ ikke et primtal.

Desværre er disse formodninger forkerte, så snart $n > 10$. Hvis $n = 11$ får vi 11 som er et primtal, men $2^{11} - 1 = 2047 = 23 \cdot 89$, altså er det et sammensat tal. Dermed er $n = 11$ er *modeksempel* til

Formodning 1.4. Vi har dog stadig ikke modbevist Formodning 1.5. Vi kan aldrig være helt sikre på at denne formodning er sand udelukkende ved brug af eksempler. Dog kan vi bevise det ved et *bevis*: **Bevis:**

Siden n ikke er et primtal, så er der positive heltal a og b således at $a < n$ og $b < n$, og $n = ab$. Lad $x = 2^b - 1$ og $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$. Så

$$
\begin{aligned}
xy &= (2^b - 1) \cdot (1 + 2^b 2^{2b} + \cdots + 2^{(a-1)b}) \\
&= 2^b \cdot (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1}b) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\
&= (2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}) - (1 + 2^b 2^{2b} + \cdots + 2^{(a-1)b}) \\
&= 2^{ab} - 1 \\
&= 2^n - 1
\end{aligned}
$$

Fordi $b < n$ kan vi konkludere at $x = 2^b - 1 < 2^n - 1$. Og siden $ab = n > a$ gælder det at $b > 1$. Derfor $x = 2^b - 1 > 2^1 - 1 = 1$, så $y < xy = 2^n - 1$. Dermed har vi vist at $2^n - 1$ kan skrives som produktet af to positive tal x o y, begge som har en værdi mindre end $2^n - 1$. Dermed er $2^n - 1$ **ikke** et primtal. □

Nu når den her formodning er bevist kalder vi den et *teorem*.

Cirka år 300 f.v.t. beviste Euklid følgende teorem:

Teorem 1.6

Der er uendeligt mange primtal.

Bevis:

Antag at der kun er endeligt mange primtal. Lad $p_1, p_2, \ldots, p_n$ være en liste af alle primtal (vi kan have denne liste præcis fordi der er et endeligt antal primtal.) Lad $m = p_1 \cdot \cdots \cdot p_n + 1$. Bemærk at m ikke er deleligt med p_1, da m divideret med p_1 giver en kvotient af $p_2 p_3 \cdots p_n$ og en rest af 1. Af samme grund er m ikke deleligt med nogen af $p_2, p_3 \cdots p_n$.

Siden det nye tal m er større end 1, så er det enten et sammensat tal eller et primtal. Hvis vi tantager at m er et primtal, så har vi fundet et nyt primtal (da det ikke er et af alle hidtil kendte primtal.) Dette går imod vores antagelse at vores liste indeholder alle primtal.

Hvis vi så antager at m er et produkt af primtal. Lad q være en af de primtal i produktet. Så er m deleligt med q. Men vi har allerede set at m ikke er deleligt af nogen af tallene i listen (som vi har antaget er *alle* primtal.) Dermed har vi igen et modstrid mod vores antagelse.

Dermed må der være uendeligt mange primtal. □

Definition 1.7 (Mersenne Primtal)
Mersenne Primtal er primtal af formen $2^n - 1$, opkaldt efter Fader Marin Mersenne (1588-1648), en Fransk monk og lærd som studerede disse tal.

Vi ved ikke om der er uendeligt mange Mersenne primtal, eller om de stopper på et tidspunkt. Mange af de største fundne primtal er Mersenne primtal. Pr. februar 2019 er det størst kendte primtal et Mersenne primtal, $2^{82,589,933} - 1$, som er et tal med over 24 millioner cifre.

Definition 1.8 (Perfekte Tal)
Perfekte Tal (*Perfect Numbers* på engelsk) er tal som er lig med summen af alle positive heltal mindre end tallet som er delelige med tallet.

Et eksempel på et perfekt tal er 6, da $6 = 1 + 2 + 3$.

Euklid beviste at hvis $2^n - 1$ er et primtal, så er $2^{n-1}(2^n - 1)$ et perfekt tal. Leonhard Euler beviste 2000 år efter Euklid at hvert lige perfekte tal forekommer på denne måde. Se for eksempel at $6 = 2^1(2^2 - 1)$. Et andet perfekt tal, $28 = 2^2(2^3 - 1)$. Dermed, fordi vi ikke ved om der er uendeligt mange Mersenne primtal, ved vi heller ikke om der er uendeligt mange perfekte tal.

Definition 1.9 (Fakultetstal)
Et fakultetstal er resultatet af en fakultet-funktion. Altså er 120 et fakultetstal som er resultat af 5!.

Teorem 1.10
For alle positive heltal n, er der en sekvens af n fortløbende positive heltal der indeholder *ingen* primtal.

Bevis:
Antag at n er et positivt heltal. Lad $x = (n+1)!+2$. Vi vil vise at *ingen* af tallene $x, x+1, x+2, \ldots, x+(n-1)$ er primtal. Siden dette er en sekvens, bevises teoremet.

Vi ved at x ikke er et primtal da ingen fakultetstal er primtal. Følgende ligning viser hvordan det kan splittes op til 2 tal.

$$\begin{aligned} x &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 \\ &= 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n+1) + 1) \end{aligned}$$

På samem måde kan vi bevise at $x + 1$ ikke er et primtal:

$$\begin{aligned} x + 1 &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 \\ &= 3 \cdot (1 \cdot 2 \cdot 4 \cdot (n+1) + 1) \end{aligned}$$

Dette gælder generelt for ethvert tal $x + i$, hvor $0 \leq i \leq n - 1$. Se:

$$\begin{aligned} x + i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + (i+2) \\ &= (i+2) \cdot (1 \cdot 2 \cdot 3 \cdots (i+1) \cdots (i+3) \cdots (n+1) + 1) \end{aligned}$$

$\square$

1.0.1 Øvelser

1. (a) Factor $2^{15} - 1 = 32,767$ into a product of two smaller positive integers.
   Siden 15 ikke er et primtal, ved vi at dette er muligt, fra Formodning 1.5. Tallene 7 og 4681 fungerer her.

   (b) Find an integer x such that $1 < x < 2^{32,767} - 1$ and $2^{32,767} - 1$ is divisble by x.
   $2^{31} - 1$

2

Sætningslogik

Sætningslogik (engelsk *Sentential Logic*) er en gren af logik, også kaldt (på engelsk) *propositional calculus, propositional logic, statement logic, sentential calculus.*[1]

2.1 Deduktion og Logiske Konnektiver

Dedktivt ræsennoment er en måde hvorpå vi kan lave, hvad der i hvert fald ligner, nye påstande ud fra allerede kendte påstande.

Eksempel 2.1

Følgende er 2 eksempler på deduktiv ræsennoment:

1. Det kommer enten til at regne eller sne i morgen
2. Det er for varmt til at sne

[1] Dette er fra Wikipediasiden om Propositional Calculus

3. ∴ kommer det til at regne (∴ betyder derfor.)

1. Hvis det er Søndag behøver jeg ikke arbejde.

2. Det er søndag i dag.

3. ∴ behøver jeg ikke arbejde.

Vi siger at et argument er *velbegrundet* hvis premisserne ikke alle kan være sande uden at konklusionen også er sand.

Eksempel 2.2

Følgende er et eksempel på et argument der *ikke* er velbegrundet:

1. Enten er butleren eller stuepigen skyldig

2. Enten er stuepigen eller kokken skyldig

3. ∴ er enten butleren skyldig eller kokken er skyldig.

Dette argument er ikke velbegrundet, da selv hvis begge præmisser er korrekte, er konklusionen ikke nødvendigvis, for eksempel hvis stuepigen var skyldig men både butleren og kokken var uskyldige, ville begge præmisser være sande men konklusion falsk.

Det kan blive nemmere, at lave de forskellige præmisser om, og nedkoge dem til at være lettere at sluge, som for eksempel i Eksempel 2.2:

1. Enten Q eller P

2. Enten P eller Z

3. ∴ enten Z eller Q

Da er det lidt mere klart at se hvordan argumentet ikke er velbegrundet.

Faktisk kan vi gøre det endnu mere symbol-rigt, ved at bruge symboler til “eller”, “og” og “ikke”:

Symbol	*Betydning*
$\vee$	eller (disjunktion)
$\wedge$	og (konjunktion)
$\neg$	ikke (negation)

Ordene i parenteser er en mere ”logisk” måde at navngive disse operationer.

Eksempel 2.3

Følgende eksempel vil bruges til analyse:

1. Enten er John gået ud for at handle, eller vi har ikke flere æg
2. Joe går hjemmefra og kommer ikke tilbage
3. Enten er Bill på arbejde og Jane er ikke, eller Jane er på arbejde og Bill er ikke.

Vi analyserer disse i deres logiske form:

1. Givet P betyder “John er gået ud for at handle” og Q betyder “Vi har ikke flere æg”; så kan vi skrive denne sætning: $P \vee Q$.
2. Givet P betyder “Joe går hjemmefra” og Q betyder “Joe kommer ikke tilbage”, kan vi repræsentere dette som $P \wedge Q$, **men** det glemmer at Q er en negation, af at Joe kommer tilbage. I stedet kan vi lade R være “Joe kommer tilbage”, og dermed er $Q = \neg R$. Så kan vi også få en bedre analyse: $Q \wedge \neg R$.

3. Givet B betyder "Bill er på arbejde" og J betyder $Janeerp\hbar arbejde$, så er første halvdel $B \wedge \neg J$, og den anden halvdel $J \wedge \neg B$. Dermed får vi en stor logisk form $(B \wedge \neg J) \vee (J \wedge \neg B)$.