MA1301 Tallteori - høst 2018

$\mathbb{N} = \{1, 2, 3, \ldots\}$ de naturlige tall

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ heltallene

$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ rasjonale tall

$\mathbb{R}$ = reelle tall

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$ komplekse tall

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Tallteori: Studiet av heltallene $\mathbb{Z}$. Eksempler på resultater (teoremer):

* Hvis p er et primtall og $p \mid ab$, så må $p \mid a$ eller $p \mid b$
* For $n \geq 3$ har ligningen $x^n + y^n = z^n$ ingen heltallsløsninger hvor $x, y, z \neq 0$.

Dette kurset:

* Heltall og delelighet (divisjonsalgoritmen, gcd, Euklids alg, diofantiske ligninger)
* Primtall (aritmetikkens fundamentalteorem)
* Kongruenser (lineære, kinesiske restteorem)
* Fermats teorem / Eulers teorem
* RSA-kryptografi
* Noe mer avansert på slutten

1.1 Induksjon

Induksjonsbevis: Type bevis(teknikk) ofte brukt i matematikken, typisk for å bevise utsagn på formen

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad \text{for alle } n \geq 1$$

Baserer seg på Velordningsprinsippet.

Velordningsprinsippet

La S være en delmengde av $\mathbb{Z}$ bestående av ikke-negative heltall (dvs $S \subseteq \mathbb{N} \cup \{0\}$), og anta S ikke er tom: $S \neq \emptyset$. Da har S et minste element: det finnes et elt $m \in S$ slik at $m \leq n$ for alle $n \in S$ ($\exists\, m \in S$ med $m \leq n$ $\forall\, n \in S$).

Teorem 1.2 (Matematisk induksjon – vår praktiske versjon)

La $P(n)$ være et utsagn (typisk: formel) som avhenger av $n \in \mathbb{N}$.

Anta (a) $P(1)$ er sant

(b) hvis $P(k)$ er sant, så er også $P(k+1)$ sant.

Da er $P(n)$ sant $\forall n \in \mathbb{N}$

Bevis: Anta at $\exists\, n \in \mathbb{N}$ med $P(n)$ usant. Da er mengden

$$S = \{n \in \mathbb{N} \mid P(n) \text{ usant}\}$$

en ikke-tom delmengde av $\mathbb{N}$. Velordningsprinsippet garanterer at S inneholder et minste elt $m \in S$. Siden $P(m)$ er usant og $P(1)$ er sant fra (a), må $m \geq 2$. Se på $m-1$. Siden $m \geq 2$ må $m-1 \geq 1$, altså er $m-1$ et naturlig tall. Hvis $P(m-1)$ er usant vil $m-1 \in S$, men det går ikke siden m er det minste elt i S. Altså må $P(m-1)$ være sant. Fra (b) er da også $P((m-1)+1)$ sant, altså $P(m)$. Dette er en motsigelse. Det kan derfor ikke eksistere en $n \in \mathbb{N}$ med $P(n)$ usant. □

Merk: Dette var et motsigelsesbevis.

Eksempler: (1) Standard førsteeksempel: formelen

$$1+2+\cdots+n = \frac{(n+1)n}{2} \qquad \left(\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right)$$

er sann for alle $n \geq 1$ (oppg 1.1.1.(a) i boka).

(a) Formelen stemmer for $n=1$, for da står det 1 på VS og $\frac{(1+1)\cdot 1}{2}$ på HS (og $1 = \frac{(1+1)\cdot 1}{2}$).

(b) Anta formelen stemmer for et k, dvs

$$1+\cdots+k = \frac{k(k+1)}{2} \qquad (*)$$

Vi må vise at den da også stemmer for $k+1$. Legg til $k+1$ på begge sider i $(*)$ og se hva som skjer:

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

Dette viser at formelen da stemmer for $k+1$ (hvis den stemmer for k).

Konklusjon: formelen stemmer $\forall n \in \mathbb{N}$.

(2) Kontrollsamen august 2017, oppg 2:

$$\sum_{i=1}^{n} i \cdot 2^i = 2 + (n-1)2^{n+1} \qquad \forall\ n \geq 1$$

For $n=1$ blir VS lik $1 \cdot 2^1 = 2$, mens HS blir $2+(1-1)2^{1+1} = 2$, så formelen stemmer for $n=1$.

Anta formelen stemmer for en k, dvs $\sum_{i=1}^{k} i \cdot 2^i = 2+(k-1)2^{k+1}$.

Må vise at da stemmer formelen også for $k+1$. Manipulerer:

$$\begin{aligned}
\sum_{i=1}^{k+1} i \cdot 2^i &= \underbrace{\sum_{i=1}^{k} i \cdot 2^i} + (k+1)2^{k+1} \\
&= \left(2 + (k-1)2^{k+1}\right) + (k+1)2^{k+1} \\
&= 2 + \Big([k-1] + [k+1] \Big) 2^{k+1} \\
&= 2 + (2k) \cdot 2^{k+1} \\
&= 2 + k \cdot 2^{k+2} \\
&= 2 + \big([k+1]-1\big) 2^{[k+1]+1}
\end{aligned}$$

Dette viser at formelen stemmer for $k+1$ hver gang den stemmer for k.

Konklusjon: den stemmer $\forall\ n \in \mathbb{N}$.