Sidste gang:

- Stærk induktion
- Rekursive def.
- Strukturel induktion

Illustration:

Simpel induktion:

Basis

$P(k)$

$P(k) \Rightarrow P(k+1)$

$P(k+1) \Rightarrow P(k+2)$

$\vdots$

Stærk induktion:

Basis

$\bigwedge_{i=k}^{l} P(i), \quad l \geq k$

$\bigwedge_{i=k}^{l} P(i) \Rightarrow P(l+1)$

$\bigwedge_{i=k}^{l+1} P(i) \Rightarrow P(l+2)$

$\vdots$

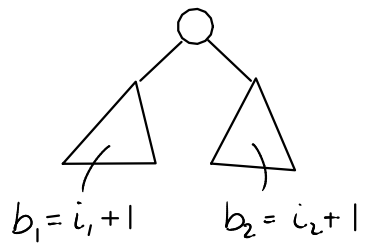
Fibonacci-tallene:

$f_0 = 0, \quad f_1 = 1$

$f_n = f_{n-1} + f_{n-2}, \quad$ for $n \geq 2$

Fulde binære træer:

#blade = # indre knuder + 1



$$\left.\begin{aligned} i &= i_1 + i_2 + 1 \\ b = b_1 + b_2 &= (i_1 + 1) + (i_2 + 1) \\ &= (i_1 + i_2 + 1) + 1 \\ &= i + 1 \end{aligned}\right\}$$

Talteori (afsnit 4.1)

Anvendelser: Kryptologi, hash-funktioner, pseudo-tilfældige tal, ...

Def 4.1.1:

Lad $a, b \in \mathbb{Z}$ og $a \neq 0$.

$$a \mid b \quad \Updownarrow \quad \frac{b}{a} \in \mathbb{Z}$$

(a går op i b)

Bemærk:

$$\frac{b}{a} \in \mathbb{Z}$$
$$\Updownarrow$$
$$\exists c \in \mathbb{Z} : \frac{b}{a} = c$$
$$\Updownarrow$$
$$\exists c \in \mathbb{Z} : b = c \cdot a$$
$$(\Updownarrow \quad b \bmod a = 0)$$

Hvis $a \mid b$, siger man også, at
a er en faktor i b, eller
b er et multiplum af a.

$a \nmid b$: a går ikke op i b.

Sætning 4.1.1:

Lad $a, b, c \in \mathbb{Z}$. Da gælder

(i) $a \mid b \wedge a \mid c \Rightarrow a \mid (b+c)$

(ii) $a \mid b \Rightarrow \forall c \in \mathbb{Z} : a \mid bc$

(iii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (d.v.s. transitiv relation)

Bevis:

(i):

Som bogen:

$a \mid b \wedge a \mid c$

Def. 1 $\Updownarrow$ $b = ka \wedge c = la$, hvor $k, l \in \mathbb{Z}$

$\Downarrow$ $b + c = ka + la = (k+l)a$, hvor $k+l \in \mathbb{Z}$

Def. 1 $\Downarrow$ $a \mid (b+c)$

Eller:

$a \mid b \wedge a \mid c$

Def. 1 $\Updownarrow$ $\frac{b}{a} \in \mathbb{Z} \wedge \frac{c}{a} \in \mathbb{Z}$

$\Downarrow$ $\frac{b}{a} + \frac{c}{a} \in \mathbb{Z}$

$\Updownarrow$ $\frac{b+c}{a} \in \mathbb{Z}$

Def. 1 $\Updownarrow$ $a \mid (b+c)$

(ii): Beviset selv! (Opgave 4.1.3)

$$
\begin{aligned}
&\Updownarrow \quad a \mid b \\
&\Updownarrow \quad \exists k \in \mathbb{Z} : b = ka \\
&\Updownarrow \quad \forall c \in \mathbb{Z} : \exists k \in \mathbb{Z} : bc = \underbrace{ck}_{\in \mathbb{Z}} a \\
&\Updownarrow \\
&\quad \forall c \in \mathbb{Z} : a \mid bc
\end{aligned}
$$

Eller:

$$
\begin{aligned}
&\Updownarrow \quad a \mid b \\
&\Updownarrow \quad \frac{b}{a} \in \mathbb{Z} \\
&\Downarrow \quad \forall c \in \mathbb{Z} : c \cdot \frac{b}{a} \in \mathbb{Z} \\
&\Updownarrow \quad \forall c \in \mathbb{Z} : a \mid (cb)
\end{aligned}
$$

(iii): Beviset selv! (Opgave 4.1.4)

$$
\begin{aligned}
&\Updownarrow \quad a \mid b \ \wedge \ b \mid c \\
&\Updownarrow \quad b = ka \ \wedge \ c = \ell b, \quad k, \ell \in \mathbb{Z} \\
&\Downarrow \quad c = \ell k a, \quad \text{hvor } \ell k \in \mathbb{Z}
\end{aligned}
$$

Eller:

$$
\begin{aligned}
&\Updownarrow \quad a \mid b \ \wedge \ b \mid c \\
&\Updownarrow \quad \frac{b}{a} \in \mathbb{Z} \ \wedge \ \frac{c}{b} \in \mathbb{Z} \\
&\Downarrow \quad \frac{\cancel{b}}{a} \cdot \frac{c}{\cancel{b}} \in \mathbb{Z} \\
&\Updownarrow \quad \frac{c}{a} \in \mathbb{Z} \\
&\Updownarrow \quad a \mid c
\end{aligned}
$$

Korollar 4.1.1:

Lad $a, b, c \in \mathbb{Z}$ og $a \neq 0$. Da gældr:

$$a \mid b \wedge a \mid c$$
$$\Downarrow$$
$$\forall k, \ell \in \mathbb{Z}: \; a \mid (kb + \ell c)$$

Bevis

$$a \mid b \wedge a \mid c$$
Sætn. 1(ii) $\Downarrow$
$$\forall k, \ell \in \mathbb{Z}: (a \mid kb \wedge a \mid \ell c)$$
Sætn. 1(i) $\Downarrow$
$$\forall k, \ell \in \mathbb{Z}: \; a \mid (kb + \ell c)$$
$\square$

Sætning 4.1.2 (Divisions-algoritmen)

Lad $a \in \mathbb{Z}$ og $d \in \mathbb{Z}^+$. Da gældr

$$\exists! \, q, r \in \mathbb{Z}: 0 \leq r < d \wedge a = dq + r$$

dividend, divisor, kvotient, rest — Def. 4.1.2

$q = a \text{ div } d$

$r = a \text{ mod } d$ ("a modulo b")

skrives som % i mange prg.sprog

Eks:

$47 \text{ div } 5 = 9$ (kvotient)

$47 \text{ mod } 5 = 2$ (rest) — divisionen går ikke op

$47 = 5 \cdot 9 + 2$

$-47 \text{ div } 5 = -10$

$-47 \text{ mod } 5 = 3$

$-47 = 5 \cdot (-10) + 3$

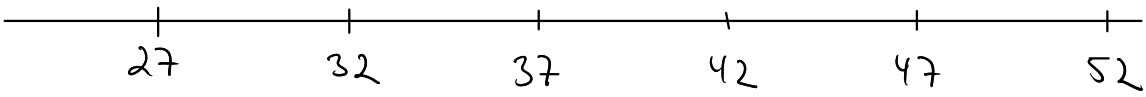
$42 \text{ div } 7 = 6$

$42 \text{ mod } 7 = 0$ — divisionen går op

$42 = 7 \cdot 6 + 0$

$32 = 5 \cdot 6 + 2$

$\Rightarrow \quad 47 \equiv 32 \pmod 5$



Alle disse tal er kongruente med hinanden modulo 5.

Def. 4.1.3:

Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$. Da gælder

$$a \equiv b \pmod{m}$$
$$\Updownarrow$$
$$m \mid (a-b)$$

$a \equiv b \pmod{m}$: a og b er kongruente modulo m

$a \not\equiv b \pmod{m}$: a og b er ikke kongruente modulo m

Eks:

$5 \equiv 15 \pmod{5}$? $\quad 15-5 = 10 = 2 \cdot 5$ ✓

$7 \equiv 16 \pmod{5}$? $\quad 16-7 = 9 = 5+4$ ✗

$7 \equiv 16 \pmod{3}$? $\quad 16-7 = 3 \cdot 3$ ✓

Kongruens kan defineres på mange måder:

Def. 4.1.3 ⇕ $a \equiv b \pmod{n}$

$m \mid (a-b)$ (*)

Sætn. 4.1.3 ⇕ $a \bmod m = b \bmod m$

Sætn. 4.1.4 ⇕ $\exists k \in \mathbb{Z} : a = b + km$ (*)

Bevis for Sætning 4.1.3: Opgave 4.1.13

Bevis for Sætning 4.1.4:

(**) er en ren omskrivning af (*):

$m \mid (a-b)$

Def. 4.1.1 ⇕ $a-b = km, \quad k \in \mathbb{Z}$

⇕ $a = b + km, \quad k \in \mathbb{Z}$

Sætning 4.1.5:

Lad $m \in \mathbb{Z}^+$. Da gælder

$$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases}$$

$$\Downarrow$$

$$\begin{cases} a+c \equiv b+d \pmod m \\ ac \equiv bd \pmod m \end{cases}$$

D.v.s. man må addere og gange med det "samme" tal på begge sider.

Eks:

$$5 \equiv 8 \pmod 3$$
$$4 \equiv 10 \pmod 3$$

$$\Downarrow$$

$$\begin{cases} 9 \equiv 18 \pmod 3 & \text{(adder på begge sider)} \\ 20 \equiv 80 \pmod 3 & \text{(mult. ——— " ———)} \end{cases}$$

Må man trække det "samme" tal fra på begge sider?

Ja: $c \equiv d \pmod m \iff -c \equiv -d \pmod m$

Må man dividere med det "samme" tal på begge sider, hvis det går op?

Nej, ikke generelt:

$20 \equiv 30 \pmod 5$, men

$4 \not\equiv 6 \pmod 5$

Bevis:

Som bogen:

$$
\begin{aligned}
& a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \\
\Updownarrow \quad & a = b + km \quad \wedge \quad c = d + \ell m, \quad k, \ell \in \mathbb{Z} \\
\Downarrow \quad & a + c = (b + km) + (d + \ell m) = (b + d) + (k + \ell)m, \quad k + \ell \in \mathbb{Z} \\
\Updownarrow \quad & a + c \equiv b + d \pmod{m}
\end{aligned}
$$

Eller:

$$
\begin{aligned}
& a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \\
\text{Def 4.1.3} \quad \Updownarrow \quad & m \mid (a-b) \quad \wedge \quad m \mid (c-d) \\
\text{Sætn. 4.1.1 (i)} \quad \Downarrow \quad & m \mid (a-b+c-d) \\
\Updownarrow \quad & m \mid ((a+c)-(b+d)) \\
\text{Def. 4.1.3} \quad \Updownarrow \quad & a + c \equiv b + d \pmod{m}
\end{aligned}
$$

$$
\begin{aligned}
& a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \\
\text{Sætn. 4.1.4} \quad \Updownarrow \quad & a = b + km \quad \wedge \quad c = d + \ell m, \quad k, \ell \in \mathbb{Z} \\
\Downarrow \quad & a \cdot c = (b + km)(d + \ell m), \quad k, \ell \in \mathbb{Z} \\
\Downarrow \quad & a \cdot c = bd + b\ell m + kmd + k\ell m^2 \\
& \qquad = bd + \underbrace{(b\ell + kd + k\ell m)}_{\in \mathbb{Z}} m \\
\text{Sætn 4.1.4} \quad \Updownarrow \quad & \\
& ac \equiv bd \pmod{m}
\end{aligned}
$$

Eller:

$$
\begin{aligned}
& a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m} \\
\Updownarrow \quad & m \mid (a-b) \quad \wedge \quad m \mid (c-d) \\
\Downarrow \quad & m \mid (a-b)c \quad \wedge \quad m \mid (c-d)b \\
\Downarrow \quad & m \mid ((a-b)c + (c-d)b) \\
\Updownarrow \quad & m \mid (ac - bd) \\
\Updownarrow \quad & ac \equiv bd \pmod{m}
\end{aligned}
$$

Korollar 4.1.2 :

Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$. Da gælder

- $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
- $ab \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

Praktisk, da det kan spare a for at regne med store tal.

Bevis:

$$a \equiv (a \bmod m) \pmod m$$
$$b \equiv (b \bmod m) \pmod m$$

Eks:

$$12 \equiv 2 \pmod 5$$
$$24 \equiv 4 \pmod 5$$

P.v.s.

$$a+b \equiv (a \bmod m) + (b \bmod m) \pmod m, \text{ iflg. Sætn. 4.1.5}$$

Sætn. 4.1.3 ⇕

$$(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$$

Og

$$a \cdot b \equiv (a \bmod m)(b \bmod m) \pmod m, \text{ iflg. Sætn. 4.1.5}$$

Sætn. 4.1.3 ⇕

$$ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$$

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