

Sidste gang:

Bevis $P(n)$, $n \geq m$, ved stærk induktion:

- Bevis $P(m), P(m+1), \dots, P(l)$, $l \geq m$
- Bevis $\underbrace{\forall k \in \{m, m+1, \dots, n-1\} : P(k) \Rightarrow P(n)}_{P(n)}$, for $n \geq l+1$

Vi bruger en stærkere ind. ant. end ved simpel induktion

Eks: $\forall n \in \mathbb{N}, n \geq 4 : \underbrace{\exists a, b \in \mathbb{N} : n = 2a + 5b}_{P(n)}$

$$P(4), P(5)$$

$$P(4) \Rightarrow P(6)$$

$$P(5) \Rightarrow P(7)$$

$$P(6) \Rightarrow P(8)$$

$\vdots$

Eks: Rekursio def.:

$$f_0 = 0, f_1 = 1$$

(Basis)

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

(Rekursivt skridt)

$$\underbrace{f_n > \phi^{n-2}}_{P(n)}, \quad \text{for } n \geq 3, \quad \text{hvor } \phi = \frac{1+\sqrt{5}}{2} \approx 1,618$$

$$P(3), P(4)$$

$$P(3) \wedge P(4) \Rightarrow P(5)$$

$$P(4) \wedge P(5) \Rightarrow P(6)$$

$$P(5) \wedge P(6) \Rightarrow P(7)$$

$\vdots$

Eks: Fulde binære træer

Rekursiv def:

$$S_0 = \{\bullet\}$$

$$S_n = S_{n-1} \cup \left\{ \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ T_1 \quad T_2 \end{array} \mid T_1, T_2 \in S_{n-1} \right\}$$

(Basis)

(Rek. skridt)

Eks: Fulde binære træer

$b(T)$: # blade

$i(T)$: # indre knuder

$$b(T) = i(T) + 1$$

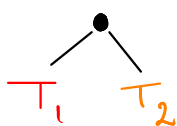
Beris: Ved strukturel induktion

Basis: $S_0 = \{\bullet\}$

$$b(T) = 1 = i(T) + 1$$

Ind. ant.: $\forall T \in S_{n-1} : b(T) = i(T) + 1$

Ind. skridt: $S_n, n \geq 1$



Ind. ant.: $b(T_1) = i(T_1) + 1$

$b(T_2) = i(T_2) + 1$

$$b(T) = b(T_1) + b(T_2)$$

$$= i(T_1) + 1 + i(T_2) + 1, \text{ ifølge ind. ant.}$$

$$= i(T) + 1$$

□

Talteori (Afsnit 4.1)

Anvendelser:

Kryptologi (DM547 + DM549 uge 44, DM534 dec.)

Hashing (DM534 uge 39, DM507)

Pseudo-tillfældige tal

:

Def. 1:

For $a, b \in \mathbb{Z}$, $a \neq 0$, gælder:

$$a \mid b \Leftrightarrow \frac{b}{a} \in \mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z}: b = k \cdot a$$

"a går op i b"

"a er en faktor i b"

"b er et multiplum af a"

Eks: $3 \mid 15 : \frac{15}{3} = 5 \Leftrightarrow 15 = 5 \cdot 3$

Sætning 1:

For $a, b, c \in \mathbb{Z}$, $a \neq 0$, gælder

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

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

(iii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

} $\Rightarrow$

Korollar 1:

$$a \mid b \wedge a \mid c \Rightarrow \forall m, n \in \mathbb{Z}: a \mid (mb + nc)$$

Eks: $3 \mid 6 \wedge 3 \mid 15 \xRightarrow{\text{Kor. 1}} 3 \mid (4 \cdot 6 + 2 \cdot 15) \Leftrightarrow 3 \mid 54$

$3 \mid 6 \wedge 6 \mid 30 \xRightarrow{\text{Sætning (iii)}} 3 \mid 30$

Sætning 2 (Divisionsalgoritmen):

For $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ gælder
 $\exists! q, r : (a = d \cdot q + r \wedge 0 \leq r < d)$

dividend

divisor

quotient

remainder

Def. 2

$$q = a \text{ div } d$$

$$r = a \text{ mod } d \quad \text{"a modulo d"}$$

Eks:

$$a = 16, d = 3$$

$$16 = 3 \cdot 5 + 1$$

Eks:

$$16 \text{ div } 3 = 5$$

$$16 \text{ mod } 3 = 1$$

Eks: $17 \text{ div } 5 = 3, \quad 17 \text{ mod } 5 = 2$

$$20 \text{ div } 4 = 5, \quad 20 \text{ mod } 4 = 0$$

$$-11 \text{ div } 3 = -4, \quad -11 \text{ mod } 3 = 1 :$$

$$-11 = 3 \cdot (-4) + 1$$

Def. 3:

For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

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

„a og b er kongruente modulo m”

Eks: $7 \equiv 16 \pmod{3}$, da $3 \mid (16-7)$

Kongruens kan defineres på mange måder:

Def. 3

$$a \equiv b \pmod{m}$$

$\Updownarrow$

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

(*)

Sætning 3

$\Updownarrow$

$$a \bmod m = b \bmod m$$

Sætning 4

$\Updownarrow$

$$\exists k \in \mathbb{Z}: a = b + km$$

(**)

Beris for Sætning 3: Opgave 13

Beris for Sætning 4:

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

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

$$\Updownarrow a-b = km, \quad k \in \mathbb{Z}, \quad \text{ifølge Def. 3}$$

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

□

For = må man addere og multiplicere med det samme tal på begge sider.

For $\equiv$ må man også **addere** og **multiplicere** med det "samme" tal på begge sider:

Sætning 5:

For $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

$$\begin{aligned} & \begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases} \\ \Downarrow & \\ & \begin{cases} a+c \equiv b+d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases} \end{aligned}$$

Eks:

$$\begin{aligned} & \begin{cases} 5 \equiv 8 \pmod{3} \\ 4 \equiv 10 \pmod{3} \end{cases} \\ \Downarrow & \\ & \begin{cases} 9 \equiv 18 \pmod{3} \\ 20 \equiv 80 \pmod{3} \end{cases} \end{aligned}$$

Bevis for Sætning 5.

Bogen bruger Sætning 4.

Man kan også bruge Sætning 1:

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & m \mid (a-b) \wedge m \mid (c-d), \text{ ifølge Def. 3} \\ \Downarrow & m \mid (a-b+c-d), \text{ ifølge Sætning 1(i)} \\ \Downarrow & m \mid (a+c-(b+d)) \\ \Downarrow & a+c \equiv b+d \pmod{m}, \text{ ifølge Def. 3} \end{aligned}$$

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & a = b + km \wedge c = d + lm, \quad k, l \in \mathbb{Z}, \text{ ifølge Sætning 4} \\ \Downarrow & ac = (b+km)(d+lm), \quad k, l \in \mathbb{Z} \\ \Downarrow & ac = bd + blm + kdm + klm, \quad k, l \in \mathbb{Z} \\ \Downarrow & ac = bd + (bl + kd + klm) \cdot m, \quad bl + kd + klm \in \mathbb{Z} \\ \Downarrow & ac \equiv bd \pmod{m}, \text{ ifølge Sætning 4} \end{aligned}$$

□

Må man også **subtrahere** det "samme" tal på begge sider?

Ja, for det er det samme som at addere:

$$c \equiv d \pmod{m} \Leftrightarrow -c \equiv -d \pmod{m}$$

Må man **dividere** med det samme tal på begge sider?

Nej, **ikke** generelt:

$$20 \equiv 30 \pmod{5}, \text{ men}$$

$$4 \not\equiv 6 \pmod{5}$$

Nedenstående resultat kan spare os for at regne med meget store tal:

Korollar 2:

For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

- $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $a \cdot b = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

Beweis:

$$\begin{cases} a \equiv a \bmod m, \\ b \equiv b \bmod m, \end{cases} \quad \begin{array}{l} \text{ifølge Sætning 3} \\ \hline \text{""} \end{array}$$

$\Downarrow$

$$\begin{aligned} \Updownarrow \quad a+b &\equiv (a \bmod m) + (b \bmod m), && \text{ifølge Sætning 5} \\ \Updownarrow \quad (a+b) \bmod m &= ((a \bmod m) + (b \bmod m)) \bmod m, && \text{ifølge Sætning 3} \end{aligned}$$

Tilsvarende fås:

$$\begin{aligned} \Updownarrow \quad ab &\equiv (a \bmod m)(b \bmod m) \pmod{m}, && \text{ifølge Sætning 5} \\ \Updownarrow \quad ab \bmod m &= ((a \bmod m)(b \bmod m)) \bmod m, && \text{ifølge Sætning 3} \end{aligned}$$

□

D.v.s. man kan nøjes med at regne med tallene i $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$