

Sidste gang

Rekursive def. & struktural induction
(afsnit 5.3)

Eks 6:

Bitstringe

$$\lambda \in \Sigma^*$$

$$\beta \in \Sigma^* \wedge b \in \Sigma \Rightarrow \beta b \in \Sigma^*$$

Eks 5:

$$S_1 = \{3\}$$

$$S_n = S_{n-1} \cup \{x+y \mid x, y \in S_{n-1}\}, \quad n \geq 2$$

$$S = \bigcup_{n=1}^{\infty} S_n$$

Eks 10:

$$S = A, \quad \text{hvor } A = \{3n \mid n \in \mathbb{Z}^+\}:$$

$A \subseteq S$: induktion over n

$$3n \in S \Rightarrow 3(n+1) = \underset{\substack{\uparrow \\ \in S}}{3n} + \underset{\substack{\uparrow \\ \in S_1 \subseteq S}}{3} \in S$$

$S \subseteq A$: Struktural induction

$$\begin{aligned} s \in S_{n+1} - S_n &\Rightarrow s = x+y, \quad x, y \in S_{n-1} \subseteq A \\ &\Rightarrow s \in A \end{aligned} \quad \begin{array}{c} \uparrow \\ \text{ind. ant.} \end{array}$$

Struktural induction:

Bevis $P(S_n)$, for alle $n \geq 1$

Bevis $P(S_1)$

Bevis $P(S_n) \Rightarrow P(S_{n+1})$, for alle $n \geq 1$

Fulde binære træer

$$S_1 = \{\bullet\}$$

$$S_n = S_{n-1} \cup \left\{ \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ T_1 \quad T_2 \end{array} \mid T_1, T_2 \in S_{n-1} \right\}, n \geq 2$$

$$S_2 = \{\bullet, \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \bullet \quad \bullet \end{array}\}$$

$$S_3 = \{\bullet, \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \bullet \quad \bullet \end{array}, \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \bullet \quad \bullet \end{array}, \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \bullet \quad \bullet \end{array}, \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \bullet \quad \bullet \end{array}\}$$

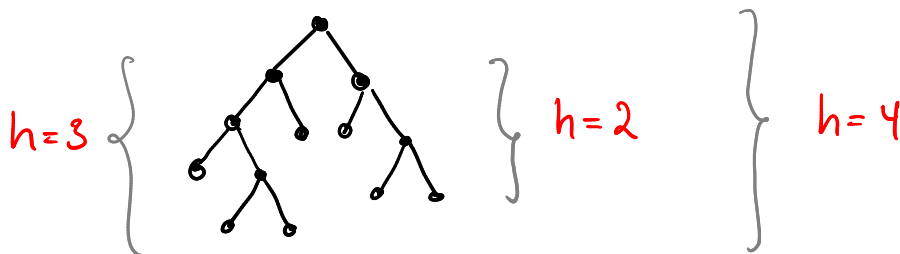
$$S_4 = \{\dots, \begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ \bullet \quad \bullet \end{array}, \dots\}$$

Def: højde

$$h(\bullet) = 0$$

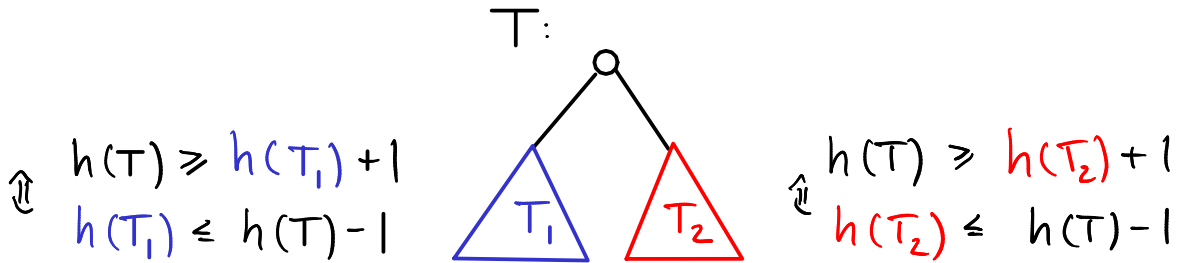
$$h\left(\begin{array}{c} \bullet \\ \swarrow \quad \searrow \\ T_1 \quad T_2 \end{array}\right) = 1 + \max\{h(T_1), h(T_2)\}$$

Eks:



$$n(T) \leq 2^{h(T)+1} - 1$$

Beweis:



$$n(T_1) \leq 2^{h(T_1)+1} - 1 \quad n(T_2) \leq 2^{h(T_2)+1} - 1 \quad (\text{ind. anl.})$$

$$\begin{aligned}
 n(T) &= 1 + n(T_1) + n(T_2) \\
 &= 1 + 2^{h(T_1)+1} - 1 + 2^{h(T_2)+1} - 1 \\
 &\leq 1 + 2^{h(T)} - 1 + 2^{h(T)} - 1 \\
 &= 2 \cdot 2^{h(T)} - 1 \\
 &= 2^{h(T)+1} - 1
 \end{aligned}$$

□

Talteori (Afsnit 4.1)

Anvendelser:

Kryptologi (DM534 november)

Hashing (DM534 uge 39, DM507)

Pseudo-tillfældige tal

⋮

Eks:

$$3 \mid 15 : \quad \frac{15}{3} = 5 \iff 15 = 5 \cdot 3$$

$$3 \nmid 16 : \quad \frac{16}{3} = 5, \bar{3}$$

$$3 \mid 24 : \quad \frac{24}{3} = 8 \iff 24 = 8 \cdot 3$$

Def. 4.1.1:

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

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

" a går op i b "

" a er en faktor i b "

" b er et multiplum af a "

Eks:

$$(i) \quad 3 \mid 39: \quad \frac{39}{3} = \frac{15+24}{3} = \frac{15}{3} + \frac{24}{3} = 5+8$$

$$15+24 = 5 \cdot 3 + 8 \cdot 3 = (5+8) \cdot 3$$

$$(ii) \quad 3 \mid 75: \quad \frac{75}{3} = \frac{5 \cdot 15}{3} = 5 \cdot \frac{15}{3} = 5 \cdot 5$$

$$5 \cdot 15 = 5 \cdot 5 \cdot 3$$

$$\text{Kor. 1} \quad 3 \mid 270: \quad \frac{270}{3} = \frac{2 \cdot 15 + 10 \cdot 24}{3} = 2 \cdot 5 + 10 \cdot 8$$

$$2 \cdot 15 + 10 \cdot 24 = (2 \cdot 5 + 10 \cdot 8) \cdot 3$$

Sætning 4.1.1:

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

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

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

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

} $\Rightarrow$

Korollar 4.1.1:

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

Eks:

$$\text{Sætning 4.1.1 (iii)} \Downarrow \begin{cases} 3 \mid 15: & 15 = 5 \cdot 3 \\ 15 \mid 60: & 60 = 4 \cdot 15 \\ 3 \mid 60: & 60 = 4 \cdot 15 = 4 \cdot 5 \cdot 3 \end{cases}$$

Bevis for Sætning 4.1.1 (i):

$$\text{Def. 4.1.1} \Updownarrow a|b \wedge a|c$$

$$\Downarrow b = k \cdot a \wedge c = l \cdot a, \quad k, l \in \mathbb{Z}$$

$\Downarrow$

$$b + c = k \cdot a + l \cdot a = (k + l)a, \quad k + l \in \mathbb{Z}$$

Def. 4.1.1 $\Updownarrow$

$$a|(b+c)$$

□

Bevis for Sætning 4.1.1 (ii) og (iii): Opgave 3 og 4

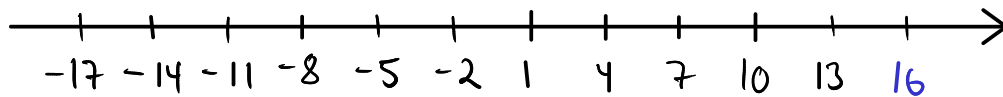
Hvis en division ikke går op, bliver der en rest:

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

Der bliver en rest på 1, når man dividerer 16 med 3.

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

$$16 \bmod 3 = 1$$



Sætning 4.1.2 (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

kootient

rest

Def. 4.1.2

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

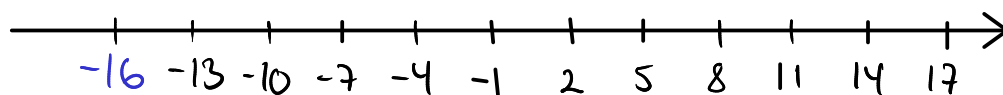
$$r = a \bmod d \quad \text{„a modulo d“}$$

Eks: $-16 = 3 \cdot (-6) + 2$

Der bliver en rest på 2, når man dividerer -16 med 3.

$$-16 \text{ div } 3 = -6$$

$$-16 \bmod 3 = 2$$



Modulær aritmetik

Def 4.1.3

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

„a og b er kongruente modulo m“
(*)

$\Leftrightarrow$

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

Sætning 4.1.3

$\Leftrightarrow$

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

Sætning 4.1.4

$\Leftrightarrow$

$$\exists k \in \mathbb{Z} : a = b + km \quad (**)$$

Eks:

$$16 \equiv 7 \pmod{3}, \text{ da } 3 \mid 9$$

$$-16 \not\equiv 16 \pmod{3}, \text{ da } 3 \nmid 32$$

$$4 \equiv 4 \pmod{10}, \text{ da } 10 \mid 0$$

Bevis for Sætning 4.1.3: Opgave 21-22

Bevis for Sætning 4.1.4:

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

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

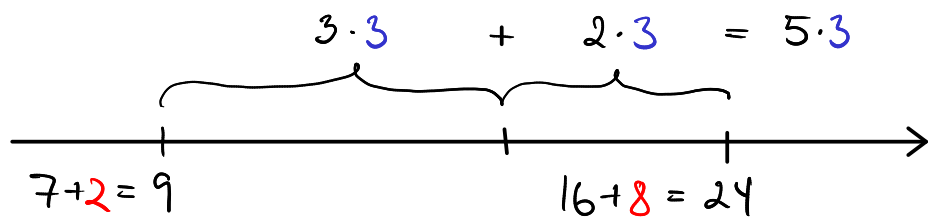
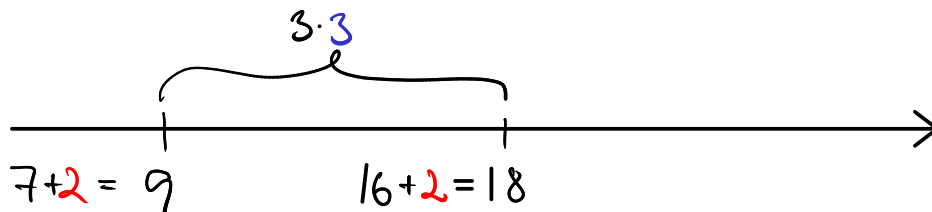
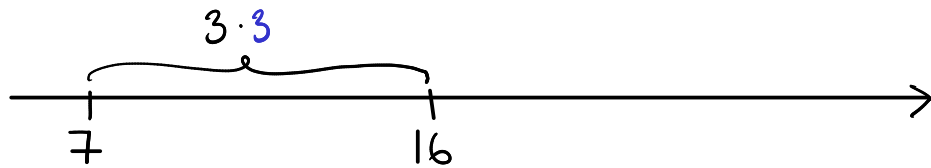
$$\Leftrightarrow a-b = km, \quad k \in \mathbb{Z}, \quad \text{ifølge Def. 4.1.3}$$

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

□

Eks:

$$\begin{aligned} & 16 \equiv 7 \pmod{3}, \text{ da } 3 \mid (16-7) \\ \Downarrow & 16+2 \equiv 7+2 \pmod{3}, \text{ da } (16+2)-(7+2) = 16-7 \\ \Downarrow & 16+8 \equiv 7+2 \pmod{3}, \text{ da } (16+8)-(7+2) = 16-7+2 \cdot 3 \end{aligned}$$



OK at addere 2 på den ene side og 8 på den anden side, fordi $2 \equiv 8 \pmod{3}$

Eks:

$$\begin{aligned} & 16 \equiv 7 \pmod{3}, \text{ da } 3 \mid (16-7) \\ \Downarrow & 16 \cdot 2 \equiv 7 \cdot 2 \pmod{3}, \text{ da } 16 \cdot 2 - 7 \cdot 2 = (16-7) \cdot 2 \\ \Downarrow & 16 \cdot 2 \equiv 7 \cdot 8 \pmod{3}, \text{ da } 16 \cdot 2 - 7 \cdot 8 = (16-7) \cdot 2 - 7 \cdot 6 \\ & \quad \quad \quad = (16-7) \cdot 2 - 7 \cdot 2 \cdot 3 \end{aligned}$$

OK at gange med 2 på den ene side og med 8 på den anden side, da $2 \equiv 8 \pmod{3}$.

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 4.1.5:

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

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

Beweis:

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & \\ & a = b + km \wedge c = d + lm, \quad k, l \in \mathbb{Z}, \quad \text{ifølge Sætning 4.1.4} \\ \Downarrow & \\ & a + c = (b + km) + (d + lm), \quad k, l \in \mathbb{Z} \\ \Updownarrow & \\ & a + c = b + d + (k+l)m, \quad k+l \in \mathbb{Z} \\ \Updownarrow & \\ & a + c \equiv b + d \pmod{m}, \quad \text{ifølge Sætning 4.1.4} \end{aligned}$$

Tilsvarende:

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & \\ & a = b + km \wedge c = d + lm, \quad k, l \in \mathbb{Z}, \quad \text{ifølge Sætning 4.1.4} \\ \Downarrow & \\ & ac = (b + km)(d + lm), \quad k, l \in \mathbb{Z} \\ \Downarrow & \\ & ac = bd + blm + kmd + kmlm, \quad k, l \in \mathbb{Z} \\ \Updownarrow & \\ & ac = bd + (bl + kd + kml)m, \quad bl + kd + kml \in \mathbb{Z} \\ \Updownarrow & \\ & ac \equiv bd \pmod{m}, \quad \text{ifølge Sætning 4.1.4} \end{aligned}$$

□

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*:

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

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

$$18 \equiv 30 \pmod{4}, \text{ men}$$

$$3 \not\equiv 5 \pmod{4}$$

Nogle gange går det godt:

$$18 \equiv 30 \pmod{4}, \text{ og}$$

$$6 \equiv 10 \pmod{4}$$

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

Korollar 4.1.2:

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

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

Intuition:

Når man tager mod, trækker man et multiplum af m fra. Det giver det samme, om man trækker det hele fra til sidst, eller splitter det op i flere mindre multipla, der trækkes fra undervejs.

Eks:

$$(11+22) \bmod 4 = 33 \bmod 4 = 1 = 33 - 8 \cdot 4$$

$$11 \bmod 4 = 3 = 11 - 2 \cdot 4$$

$$22 \bmod 4 = 2 = 22 - 5 \cdot 4$$

$$(3+2) \bmod 4 = 1 = 5 - 1 \cdot 4$$

Bevis for Kor. 4.1.2:

$$\begin{cases} a \equiv a \bmod m \pmod{m}, & \text{ifølge Sætning 4.1.3} \\ b \equiv b \bmod m \pmod{m}, & \text{ifølge Sætning 4.1.3} \end{cases}$$

$$\Downarrow \quad a+b \equiv (a \bmod m) + (b \bmod m) \pmod{m}, \quad \text{ifølge Sætning 4.1.5}$$

$$\Uparrow \quad (a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m, \quad \text{ifølge Sætning 4.1.3}$$

Tilsvarende gås:

$$\begin{aligned} \Uparrow \quad ab &\equiv (a \bmod m)(b \bmod m) \pmod{m}, && \text{ifølge Sætning 4.1.5} \\ ab \bmod m &= ((a \bmod m)(b \bmod m)) \bmod m, && \text{ifølge Sætning 4.1.3} \end{aligned}$$

□

D.v.s. man kan nøjes med at regne med tallene i

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

Printal (afsnit 4.3)

Def. 4.3.1

Lad $p \in \mathbb{Z}^+ - \{1\}$.

Hvis 1 og p er de eneste tal, der går op i p ,
er p et **printal**.

Ellers er p **sammensat**.

Eks:

Printal: 2, 3, 5, 7, 11, 13, 17

Sammensat: 4, 6, 8, 9, 10, 12, 14, 15, 16

Sætning 4.3.1 (Aritmetikkens Fundamentalsætning)

Enhvert heltal $n \geq 2$

kan skrives som et produkt af printal
på præcis én måde

(hvis man sorterer faktorerne efter størrelse)

Eks:

$$2 = 2$$

$$10 = 2 \cdot 5$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5$$

$$3 = 3$$

$$12 = 2 \cdot 2 \cdot 3$$

$$4 = 2 \cdot 2$$

$$30 = 2 \cdot 3 \cdot 5$$

Def. 4.3.2

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

$$\gcd(a, b) = \max \{d \mid d|a \wedge d|b\}$$

kaldes *største fælles divisor* for a og b

(greatest common divisor)

Eks:

$$\gcd(18, 24) = 6$$

$$18 = 2 \cdot 3 \cdot 3$$

$$24 = 2 \cdot 2 \cdot 2 \cdot 3$$

$$\gcd(12, 24) = 12$$

$$12 = 2 \cdot 2 \cdot 3$$

$$24 = 2 \cdot 2 \cdot 2 \cdot 3$$

$$\gcd(12, 25) = 1 \Rightarrow 12 \text{ og } 25 \text{ er indbyrdes primiske}$$

Def. 4.3.3
(relatively prime)

$$12 = 2 \cdot 2 \cdot 3$$

$$25 = 5 \cdot 5$$

Def. 4.3.5

Lad $a, b \in \mathbb{Z}^+$

$$\text{lcm}(a, b) = \min \{m \mid a|m \wedge b|m\}$$

kaldes *mindste fælles multiplum* af a og b