DMat-07

3.3: Kompleksitet af algoritme.

n : mål for størrelsen af input.

$f(n)$: det største antal skridt algoritmen bruger hvis inputtet har størrelse n. (worst case)

Find et simpelt udtryk $g(n)$ så $f(n)$ er $O(g(n))$.

Vi siger at algoritmen har (tids-) kompleksitet $O(g(n))$.

4.1: Hele tal: divisibilitet og modulær aritmetik.

$a, b \in \mathbb{Z}$, $a \neq 0$.
Vi siger at a går op i b, skrives $a \mid b$,
hvis der findes $c \in \mathbb{Z}$ så $b = ac$

$a, b, c \in \mathbb{Z}$
$a \mid b \ \wedge \ a \mid c \ \Rightarrow \ a \mid b + c$,
$a \mid b \ \Rightarrow \ a \mid bc$, for alle heltal c.
$a \mid b \ \wedge \ b \mid c \ \Rightarrow \ a \mid c$.

Division med rest.

$a, d \in \mathbb{Z}$, $d \geq 1$.
Der findes entydige tal $q, r \in \mathbb{Z}$ så

$$a = dq + r, \quad 0 \leq r < d.$$

Vi skriver: $r = a \mod d$.

Hvis $d \geq 1$: $\quad d \mid a \;\Leftrightarrow\; a \mod d = 0$.

$m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$.
a er kongruent med b modulo m, skrives $a \equiv b \pmod{m}$,
hvis $m \mid a - b$.

$a \equiv b \pmod{m} \;\Leftrightarrow (a \mod m) = (b \mod m)$.

Hvis $a \equiv b \pmod{m}$ og $c \equiv d \pmod{m}$ så er

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

I udregninger modulo m kan et tal a altså erstattes af (f.eks.) $a \bmod m$.

(Dette gælder ikke tal i en eksponent.)