3.2: Store O notation.

$f(x, y)$ og $g(x, y)$ er funktioner af to variable.

Vi siger at $f(x, y)$ er $O(g(x, y))$ hvis der findes konstanter k_1, k_2, C

$$|f(x, y)| \leq C|g(x, y)|,$$

for alle (x, y), der opfylder $x > k_1, y > k_2$.

Eksempel:
Algoritme til løsning af m lineære ligninger med n ubekendte har kompleksitet $O(m^2n)$.

3.4 Divisionsalgoritme

Hvis a og d er hele tal, $d > 0$, så findes entydige hele tal q og r så

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

Skrives $r = a \mod d$.

Eksempel: Hash-funktion $h : \mathbb{Z} \mapsto \{0, 1, 2, \ldots, m-1\}$

$h(k) = k \mod m$

Lad m være et positivt helt tal, og x_0, a og c være hele tal så $0 \leq x_0 < m$, $0 \leq c < m$ og $2 \leq a < m$.

Følge af “tilfældige” tal:

$$x_0, x_1, x_2, \ldots,$$

hvor $x_{i+1} = (ax_i + c) \mod m$.

F.eks. $c = 0$. (Men så er det bedst hvis m er et primtal.)

3.4

Hvis a og d er hele tal, $d \neq 0$, så siger vi at d går op i a, skrives $d \mid a$, hvis der findes et helt tal c så $a = cd$.

3.5

Lad a og b være hele tal som ikke begge må være 0. Det største tal d som opfylder $d \mid a$ og $d \mid b$ kaldes den største fælles divisor af a og b, skrives $d = \mathrm{gcd}(a, b)$.

3.6

Lemma 1. $\gcd(a, b) = \gcd(b, a \mod b)$.

Algoritme 6: Euklids algoritme Side 229

procedure gcd(a, b: positive heltal)
x:=a
y:=b
while $y \neq 0$
begin
. $r := x \mod y$
. $x := y$
. $y := r$
end
$\{ x = \gcd(a, b) \}$