DMat-08

4.2: Repræsentation af (positive) heltal.

Lad $b \in \mathbb{Z}$, $b \geq 2$.
Et positivt helt tal n kan skrives entydigt på formen

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0,$$

hvor $a_i \in \{0, 1, \ldots, b-1\}$ for $i = 0, \ldots, k$ og $a_k \neq 0$.

Grundtal b repræsentationen af n er da

$$n = (a_k a_{k-1} \ldots a_1 a_0)_b.$$

Binær repræsentaion: grundtal $b = 2$

Decimal repræsentaion: grundtal $b = 10$

Hexadecimal repræsentaion: grundtal $b = 16$
svarer til binær repræsentaion hvor cifrene opdeles i blokke med 4.
$10, 11, \ldots, 15$ skrives hhv. $A, B, \ldots, F$.

procedure *base b expansion*(n, b: heltal, $n \geq 1, b \geq 2$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q \mod b$
    $q := q \text{ div } b$
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0$

$\{(a_{k-1} \ldots a_1 a_0)_b$ er n skrevet i talsystem med grundtal $b\}$

EKS $n = (253)_7 = 2 \cdot 7^2 + 5 \cdot 7 + 3 = 98 + 35 + 3$

$= 136$

Omregn n til binær

$q := 136$, $k := 0$

$a_0 = 136 \bmod 2 = 0$, $q = 136 \operatorname{div} 2 = 68$, $k := 1$

$a_1 = 68 \bmod 2 = 0$, $q = 68 \operatorname{div} 2 = 34$, $k := 2$

$a_2 = 34 \bmod 2 = 0$, $q = 34 \operatorname{div} 2 = 17$, $k := 3$

$a_3 = A \bmod 2 = 1$, $q = 17 \operatorname{div} 2 = 8$, $k := 4$

$a_4 = 8 \bmod 2 = 0$, $q = 8 \operatorname{div} 2 = 4$, $k := 5$

$a_5 = 4 \bmod 2 = 0$, $q = 4 \operatorname{div} 2 = 2$ $k = 6$

$a_6 = 2 \mod 2 = 0$, $q = 2 \operatorname{div} 2 = 1$ $k=7$

$a_7 = 1 \mod 2 = 1$ $q = 1 \operatorname{div} 2 = 0$ $k=8$

$n = (1000\,1000)_2 = (88)_{16}$

8 8

q - værdier: 136, 68, 34, 17, 8, 4, 2, 1

Udregn $2^{136} \mod 9$

$2^1 = 2$

$$2^2 = 4$$

$$2^4 = 2^2 \cdot 2^2 = 4 \cdot 4 = 16 \equiv 7 \pmod 9$$

$$2^8 = 2^4 \cdot 2^4 \equiv 7 \cdot 7 = 49 \equiv 4 \pmod 9$$

$$2^{17} = 2^8 \cdot 2^8 \cdot 2 \equiv 4 \cdot 4 \cdot 2 = 32 \equiv 5 \pmod 9$$

$$2^{34} = 2^{17} \cdot 2^{17} \equiv 5 \cdot 5 = 25 \equiv 7 \pmod 9$$

$$2^{68} = 2^{34} \cdot 2^{34} \equiv 7 \cdot 7 \equiv 4 \pmod 9$$

$$2^{136} = 2^{68} \cdot 2^{68} \equiv 4 \cdot 4 \equiv 7 \pmod 9$$

4.3: Primtal og gcd

$p \in \mathbb{Z}, p \geq 2$ er et primtal hvis 1 og p er de eneste positive hele tal, der går op i p
Hvis p ikke er et primtal så siger vi at at p er et sammensat tal.

Entydig faktorisering: Ethvert helt tal n, $n \geq 2$ er et (produkt af) primtal.

Der findes uendeligt mange primtal.

Det største primtal man kender er $2^{57885161} - 1$.

Største fælles divisor

$a, b \in \mathbb{Z}$. ($a \neq 0$ eller $b \neq 0$)
Største fælles divisor af a og b, skrives gcd(a, b)
er det største tal der går op i både a og b.

Hvis

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \text{ og } b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n},$$

hvor $e_i \geq 0$ og $f_i \geq 0$ er hele tal for alle i så er

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_n^{\min(e_n, f_n)}.$$

Hvis gcd$(a, b) = 1$ så siger vi at a og b er indbyrdes primiske..

$$a = 2^2 \cdot 3^3 \cdot 5 \cdot 11^2$$

$$b = 2^5 \cdot 3 \cdot 7^2 \cdot 11 \cdot 19$$

$$\gcd(a,b) = 2^2 \cdot 3 \cdot 11$$

$$\operatorname{lcm}(a,b) = 2^5 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 \cdot 19$$

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

Det **mindste fælles multiplum** af a og b, skrives $\mathrm{lcm}(a, b)$ er det mindste tal $m \in \mathbb{Z}^+$ som opfylder $a \mid m$ og $b \mid m$.

Hvis

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \text{ og } b = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n},$$

hvor $e_i \geq 0$ og $f_i \geq 0$ er hele tal for alle i så er

$$\mathrm{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_n^{\max(e_n, f_n)}.$$

$\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$

Euklids algoritme

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

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n \quad + 0$$

Så er $\gcd(a, b) = r_n$

procedure gcd(a, b: positive heltal)
$x := a$
$y := b$
while $y \neq 0$
    $r := x \mod y$
    $x := y$
    $y := r$
return x

$\{x = \gcd(a, b)\}$

EKS Find $\gcd(55, 36)$

$55 = 1 \cdot 36 + 19$ $\quad 19 = 55 - 36$

$36 = 1 \cdot 19 + 17$ $\quad 17 = 36 - 19$

$19 = 1 \cdot 17 + 2$ $\quad 2 = 19 - 17$

$17 = 8 \cdot 2 + 1$ $\quad 1 = 17 - 8 \cdot 2$

$2 = 2 \cdot 1 + 0$

$\gcd(55, 36) = 1 = 17 - 8 \cdot 2 = \underline{17} - 8 \cdot (\underline{19} - \underline{17}) =$

$9 \cdot 17 - 8 \cdot 19 = 9 \cdot (36 - 19) - 8 \cdot 19 = 9 \cdot 36 - 17 \cdot 19 =$

$$9 \cdot 36 - 17 (55 - 36) = 26 \cdot 36 - 17 \cdot 55$$

$$= -17 \cdot 55 + 26 \cdot 36$$

$$s = -17 , \; t = 26.$$

Euklids udvidede algoritme

Lad $a, b \in \mathbb{Z}$ (enten $a \neq 0$ eller $b \neq 0$).
Så findes der $s, t \in \mathbb{Z}$ som opfylder:

$$\gcd(a, b) = s \cdot a + t \cdot b.$$

(s og t er *ikke* entydige, f.eks.:

$$(s + b) \cdot a + (t - a) \cdot b = s \cdot a + t \cdot b.)$$

Lemma
Hvis gcd$(a, b) = 1$ og a går op i bc, så går a op i c.

Lemma
Hvis p er primtal og $p \mid bc$
så er enten $p \mid b$ eller $p \mid c$

Bevis
Divisorer i p: 1 og p
$\gcd(p, b) = 1$ eller p

Hvis $\gcd(p, b) = p$ så er $p \mid b$

Hvis $\gcd(p, b) = 1$ så er $p \mid c$

Gilje lemma.