

# 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

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

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

Grundtal  $b$  repræsentationen af  $n$  er da

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

Binær repræsentation: grundtal  $b = 2$

Decimal repræsentation: grundtal  $b = 10$

Hexadecimal repræsentation: grundtal  $b = 16$

svarer til binær repræsentation hvor cifrene opdeles i blokke med 4.

10, 11, ..., 15 skrives hhv.  $A, B, \dots, F$ .

**procedure** *base  $b$  expansion*( $n, b$ : heltal,  $n \geq 1, b \geq 2$ )

$q := n$

$k := 0$

**while**  $q \neq 0$

$a_k := q \bmod b$

$q := q \operatorname{div} b$

$k := k + 1$

**return**  $(a_{k-1}, \dots, a_1, a_0)$

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

### 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  $p$  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.

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

Det **mindste fælles multiplum** af  $a$  og  $b$ , skrives  $\text{lcm}(a, b)$  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

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

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

## Euklids algoritme

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

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

⋮

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n$$

Så er  $\gcd(a, b) = r_n$

**procedure** gcd( $a, b$ : positive heltal)

$x := a$

$y := b$

**while**  $y \neq 0$

$r := x \bmod y$

$x := y$

$y := r$

**return**  $x$

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



## 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  $c$ .