4.2: Repræsentation af (positive) heltal.

$(748)_{10} = 748 = 7 \cdot 10^2 + 4 \cdot 10 + 8$, grundtal $b = 10$

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 repræsentation, $b = 2$

$(10.1101)_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 =$

$$32 + 8 + 4 + 1 = 45$$

Hexadecimal, $b = 16$

cifre: $0, 1, \dots, 9, A, B, C, D, E, F$

$$(B)_{16} = 11 = 8 + 2 + 1 = (1011)_2$$

$$(9B5)_{16} = 9 \cdot 16^2 + 11 \cdot 16 + 5 = 2485$$

$$(\underbrace{1001}_{9}\ \underbrace{1011}_{B}\ \underbrace{0101}_{5})_2$$

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

$$n \bmod b = a_0$$

$$n \operatorname{div} b = (a_k \cdots a_1)_b$$

$$n = (a_k \cdots a_1)_b \cdot b + a_0$$

EKS $n = 100$, $b = 2$

$100 = 50 \cdot 2 + 0$

$50 = 25 \cdot 2 + 0$

$100 \bmod 2 = 0 = a_0$

$50 \bmod 2 = 0 = a_1$

$$25 = 12 \cdot 2 + 1 \qquad 25 \bmod 2 = 1 = a_2$$

$$12 = 6 \cdot 2 + 0 \qquad 12 \bmod 2 = 0 = a_3$$

$$6 = 3 \cdot 2 + 0 \qquad 6 \bmod 2 = 0 = a_4$$

$$3 = 1 \cdot 2 + 1 \qquad 1 = a_5$$

$$1 = 0 \cdot 2 + 1 \qquad 1 = a_6$$

$$100 = (1100100)_2$$

Multiplikation

$b = 10$

$$
\begin{array}{r}
123 \cdot 45 \\
\hline
135 \\
90 \\
45 \\
\hline
5535
\end{array}
$$

$b = 2$, Computer med 8-bit tal, $2^8 = 256$

$5 \cdot 100$

$5 = (101)_2 = 00000101$

$100 = (01100100)_2$

$$
\begin{array}{r}
00000101 \cdot 01100100 \\
\hline
01100100 \\
01100100\,0 \\
01100100\,00 \\
\hline
1\,1111010\,0
\end{array}
$$

$5 \cdot 100 = 500 \equiv 244 \pmod{256}$

$\equiv -12 \pmod{256}$

4.3

Divisorer i et helt tal n. (Altså tal der går op i n.)
Nok at se på positive divisorer.

$d \mid n \Leftrightarrow \exists c (n = dc) \Leftrightarrow \exists c \left(n = (-d)(-c)\right) \Leftrightarrow -d \mid n$

Definition

Lad $p \in \mathbb{Z}$, $p \geq 2$.
p siges at være et primtal hvis de eneste positive divisorer i p er 1 og p.

Hvis $p = ab$ hvor $a, b \in \mathbb{Z}$, $a \geq 2$, $b \geq 2$
så er p et sammensat tal (ikke et primtal).

Primtal: $2, 3, 5, 7, 11, 13, \ldots$

Sætning 1: Faktorisering i primtal.

Lad $n \in \mathbb{Z}$, $n \geq 2$.

Så kan n skrives entydigt som produkt af primtal.

(Entydig: bortset fra faktorernes rækkefølge.

EKS $\quad n = 90 = 2 \cdot 3 \cdot 3 \cdot 5 = 2 \cdot 3^2 \cdot 5$

Sætning
Der findes uendeligt mange primtal.

Bevis ved modstrid

Antag at $p_1, p_2, \ldots, p_n$ er listen af alle primtal.

Sæt $Q = p_1 p_2 p_3 \cdots p_n + 1$

Q er produkt af primtal

Der findes p_j så $p_j \mid Q$

Desuden $p_j \mid p_1 p_2 \cdots p_n$

$p_j \mid Q - p_1 p_2 \cdots p_n = 1$ Modstrid

Der er uendeligt mange primtal.

Definition

Lad $a, b \in \mathbb{Z}$ hvor enten $a \neq 0$ eller $b \neq 0$.

Det største tal $d \in \mathbb{Z}$ som opfylder $d \mid a$ og $d \mid b$ kaldes den største fælles divisor af a og b, skrives $d = \gcd(a, b)$.

EKS

$\gcd(a, 0) = |a|$ hvis $a \neq 0$

$1 \mid a$ og $1 \mid b$

$\gcd(a, b) \geq 1$

EKS

$$a = 90 = 2 \cdot 3^2 \cdot 5$$

$$b = 165 = 3 \cdot 5 \cdot 11$$

$$\gcd(90, 165) = 3 \cdot 5 = 15$$

Lemma Lad $a, b \in \mathbb{Z}$ hvor $b \neq 0$.
Antag $a = bq + r$ hvor q og r er hele tal og $0 \leq r < b$, altså $r = a$ mod b.
Så er $\gcd(a, b) = \gcd(b, r)$.

Bevis

Vise: $d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$

$\Rightarrow$ Vise $d \mid r$.

$r = a + (-q) \cdot b$

Vi ved $d \mid a$ og $d \mid b \Rightarrow d \mid (-q) \cdot b$

Derfor $d \mid a + (-q)b = r$

$\Leftarrow$ Vise $d \mid a$.

$a = bq + r$. $d \mid a$ da $d \mid bq$ og $d \mid r$.

□

EKS $a = 90$, $b = 165$

$90 = 0 \cdot 165 + 90$, $r = a \bmod b = 90$

$\gcd(90, 165) = \gcd(b, r) = \gcd(165, 90)$

Sæt $a = 165$, $b = 90$ i Lemma

$165 = 1 \cdot 90 + 75$ $\quad r = 165 \bmod 90 = 75$

$\gcd(165, 90) = \gcd(90, 75)$

Sol $a = 90$, $b = 75$ i Lemma

$90 = 1 \cdot 75 + 15$ $\quad r = 15$

$\gcd(90, 75) = \gcd(75, 15)$

$75 = 5 \cdot 15 + 0$ $\quad r = 0$

$\gcd(90, 165) = \gcd(75, 15) = \gcd(15, 0) = 15$

Sætning

Lad $a, b \in \mathbb{Z}$ hvor enten $a \neq 0$ eller $b \neq 0$.

Der findes $s, t \in \mathbb{Z}$ som opfylder $\gcd(a, b) = s \cdot a + t \cdot b$.

EKS

$a = 35, \quad b = 13$

$35 = 2 \cdot 13 + 9$ $\qquad$ $9 = 35 - 2 \cdot 13$

$13 = 1 \cdot 9 + 4$ $\qquad$ $4 = 13 - 1 \cdot 9$

$9 = 2 \cdot 4 + 1$ $\qquad$ $1 = 9 - 2 \cdot 4$

$$4 = 4 \cdot 1 + 0$$

$$\gcd(35, 13) = \gcd(13, 9) = \gcd(9, 4) = \gcd(4, 1) = \gcd(1, 0) = 1$$

$$1 = 9 - 2 \cdot 4 = 9 - 2(13 - 1 \cdot 9) = 3 \cdot 9 - 2 \cdot 13 =$$

$$3(35 - 2 \cdot 13) - 2 \cdot 13 = 3 \cdot 35 - 8 \cdot 13$$

$$s = 3, \quad t = -8$$

Setning

Hvis $\gcd(a,b) = 1$ og $a \mid bc$

så er $a \mid c$.

Bevis

Der finnes $s,t \in \mathbb{Z}$ så $\gcd(a,b) = 1 = sa + tb$

Så er $c = sac + tbc$

$a \mid sac$ og $a \mid tbc$ da $a \mid bc$

$a \mid sac + tbc = c$

□