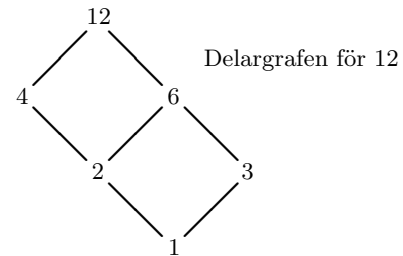


(SF1662 Diskret matte, vt17: F2, to 19 jan 2017)

Definition: Om d, m är heltal betyder ” **d delar m** ”, ” d är en delare till m ”, ” m är en multipel av d ” osv, med symboler $d \mid m$, att det finns ett heltal q så att $m = dq$ (dvs (om $d \neq 0$) att division av m med d ger rest 0).

Delargrafen för ett naturligt tal innehåller alla talets delare och det går en ”kant uppåt” mellan a och b precis om $a \mid b$ och det inte finns $c \neq a, b$ med $a \mid c, c \mid b$.

För två tal i grafen, d och m , gäller att $d \mid m$ om och endast om det går en följd (0 eller fler) kanter uppåt från d till m .



Definition: Ett **primtal** är ett heltal $p > 1$ som bara har delarna $\pm 1, \pm p$.

Definition: Om m, n är heltal, är en **största gemensam delare**, sgd (eng. gcd), till m och n ett heltal d sådant att

- i) $d \mid m, d \mid n$ gemensam delare
- ii) $c \mid m, c \mid n \Rightarrow c \mid d$ ”störst”
- iii) $d \geq 0$ ger (skall vi se) entydighet

(Boken har $c \mid m, c \mid n \Rightarrow c \leq d$ i stället för ii) och iii). De två definitionerna ger samma resultat, **utom** då $m = n = 0$.)

Sats: För alla heltal m, n (enligt boken: utom $m = n = 0$) finns en entydig största gemensam delare $d = \text{sgd}(m, n)$ och $d = am + bn$ för några heltal a, b .

m och n har samma gemensamma delare som n och $m - nq$, q heltal, så $\text{sgd}(m, n) = \text{sgd}(n, m - nq)$. Genom att upprepa det kommer man till $\text{sgd}(d, 0) = |d|$, så d, a, b fås med **Euklides algoritmen** ($n > 0$)

($\text{sgd}(m, n) = \text{sgd}(n, m) = \text{sgd}(\pm m, \pm n)$.)

$$\begin{aligned} m &= q_1 n + r_1 & 0 \leq r_1 < n \\ n &= q_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 \leq r_3 < r_2 \end{aligned}$$

$\vdots$

$$\begin{aligned} r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} & 0 \leq r_{k-1} < r_{k-2} \\ r_{k-2} &= q_k r_{k-1} + 0 \end{aligned}$$

vilket ger $\text{sgd}(m, n) = r_{k-1}$.

Näst sista ekvationen ger $d = r_{k-1}$ uttryckt i r_{k-2} och r_{k-3} , r_{k-2} uttrycks med ekvationen före i r_{k-3} och r_{k-4} etc, slutligen $d = am + bn$ för några heltal a, b .

Följdsats: Om d, m, n är heltal så att $d \mid mn$ och $\text{sgd}(d, m) = 1$ (dvs om d och m är **relativt prima**), så $d \mid n$.

Definition: Om m, n är heltal, är en **minsta gemensam multipel**, mgm (eng. lcm) till m och n ett heltal g sådant att

- i) $m \mid g, n \mid g$
- ii) $m \mid h, n \mid h \Rightarrow g \mid h$
- iii) $g \geq 0$

Sats: För alla heltal m, n finns $\text{mgm}(m, n)$ entydigt och

$$\text{mgm}(m, n) \cdot \text{sgd}(m, n) = |m \cdot n|.$$

Det bestämmer $\text{mgm}(m, n)$, utom för $m = n = 0$ (då $\text{sgd}(m, n) = 0$). $\text{mgm}(0, 0) = 0$.