(Diskret matte F, ht17: L1, må 30 okt 2017)

Något om heltalen, $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$

Sats (division med rest): Om $a, b \in \mathbb{Z},\ b \neq 0$, finns entydiga $q, r \in \mathbb{Z}$ med

$$a = bq + r \text{ och } 0 \leq r < |b|.$$

Talet q kallas **kvoten** av a och b, r kallas (den principala) **resten**.

[(r är det minsta talet som är ≥ 0 och kan skrivas $a - by,\ y \in \mathbb{Z}$).
Man kan också visa att motsvarande gäller för **polynom** (med rationella, reella eller komplexa koefficienter), där resten $r(x)$:s grad<divisorn $b(x)$:s grad och för **gaussiska heltal** (komplexa tal $m + in$ $(m, n \in \mathbb{Z})$), där $|r|^2 < |b|^2$.]

Om **talbaser**, att skriva ett naturligt tal i bas t, där $t \geq 2$:

Satsen ovan ger att vi för ett godtyckligt naturligt tal x får

$$\begin{cases} x & = q_0 t + r_0 \\ q_0 & = q_1 t + r_1 \\ & \vdots \qquad\qquad 0 \leq r_i < t \\ q_{n-1} & = q_n t + r_n, \qquad q_n = 0 \text{ (gäller för något } n) \end{cases}$$

och därur

$$\begin{aligned} x &= ((\dots((r_n t + r_{n-1})t + r_{n-2})t + \dots + r_2)t + r_1)t + r_0 \\ &= r_n t^n + r_{n-1} t^{n-1} + \dots + r_2 t^2 + r_1 t + r_0, \end{aligned}$$

dvs x uttryckt i bas t är $x = (r_n r_{n-1} \dots r_2 r_1 r_0)_t$.

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

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

Definition: Om $m, n \in \mathbb{Z}$ är en **största gemensam delare**, sgd (eng. gcd), till m och n ett $d \in \mathbb{Z}$ 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 (visar det sig) entydighet

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

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

m och n har samma gemensamma delare som n och $m - nq$, $q \in \mathbb{Z}$, så $\boldsymbol{\text{sgd}(m, n) = \text{sgd}(n, m - nq)}$. Genom att använda det upprepat kommer man till $\text{sgd}(m, n) = \text{sgd}(d, 0) = d$, så d, a, b fås med **Euklides algoritm**
(Eftersom $\text{sgd}(m, n) = \text{sgd}(n, m) = \text{sgd}(|m|, |n|)$ och $\text{sgd}(0, 0) = 0$ kan vi anta att $m \geq n > 0$.)

$$\begin{aligned} m &= nq_1 + r_1 && 0 \leq r_1 < n \\ n &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && 0 \leq r_3 < r_2 \\ &\vdots \\ r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && 0 \leq r_{k-1} < r_{k-2} \\ r_{k-2} &= r_{k-1} q_k + 0 \end{aligned}$$

vilket ger $\boldsymbol{\text{sgd}(m, n) = r_{k-1}}$
($r_k = 0$ för något $k \in \mathbb{Z}_+$, ty alla $r_i \in \mathbb{N}$ och $r_1 > r_2 > \dots \geq 0$).

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 $a, b \in \mathbb{Z}$.

Följdsats: Om $d, m, n \in \mathbb{Z},\ d \mid mn$ och $\text{sgd}(d, m) = 1$ så $d \mid n$.
(Om $\text{sgd}(d, m) = 1$ sägs d och m vara **relativt prima**.)

Definition: ("dual" till sgd) Om $m, n \in \mathbb{Z}$, är en **minsta gemensam multipel**, mgm (eng. lcm), till m och n ett $g \in \mathbb{Z}$ 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 $m, n \in \mathbb{Z}$ finns $\text{mgm}(m, n)$ entydigt och

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

Om kedjebråk

Räkningarna i Euklides algoritm ger kedjebråk för rationella tal:

Ex. $\begin{cases} 1323 = 924 \cdot 1 + 399, \\ 924 = 399 \cdot 2 + 126, \\ 399 = 126 \cdot 3 + 21, \\ 126 = 21 \cdot 6 + 0 \end{cases}$ ger $\begin{cases} \frac{1323}{924} = 1 + \frac{399}{924}, \\ \frac{924}{399} = 2 + \frac{126}{399}, \\ \frac{399}{126} = 3 + \frac{21}{126}, \\ \frac{126}{21} = 6 + 0, \end{cases}$

dvs $\frac{1323}{924} = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \frac{1}{6}}}$ betecknat $\frac{1323}{924} = [1; 2, 3, 6] = [a_0; a_1, a_2, a_3]$

med **konvergenter**:

$\frac{p_0}{q_0} = [1;] = 1,$

$\frac{p_1}{q_1} = [1; 2] = 1 + \frac{1}{2} = \frac{3}{2},$

$\frac{p_2}{q_2} = [1; 2, 3] = 1 + \cfrac{1}{2 + \frac{1}{3}} = \frac{10}{7},$

$\frac{p_3}{q_3} = [1; 2, 3, 6] = \frac{63}{44} (= \frac{1323}{924}).$

p_k, q_k i $\frac{p_k}{q_k}$ väljs med $\text{sgd}(q_k, p_k) = 1$, $q_k \in \mathbb{Z}_+$, $p_k \in \mathbb{Z}$ och man låter $\mathbf{v}_k = (q_k, p_k)$ för $k \in \mathbb{N}$, $\mathbf{v}_{-2} = (1, 0)$, $\mathbf{v}_{-1} = (0, 1)$.

Sats: $\mathbf{v}_k = a_k \, \mathbf{v}_{k-1} + \mathbf{v}_{k-2}$ för $k \in \mathbb{N}$,
så $1 = q_0 \leq q_1 < q_2 < \ldots$

$\mathbf{v}_k$ för $[1; 2, 3, 6]$ fås som

k	-2	-1	0	1	2	3
a_k			1	2	3	6
p_k	0	1	1	3	10	63
q_k	1	0	1	2	7	$44.$

Alla rationella tal har (enligt Euklides algoritm) ändliga kedjebråk, medan irrationella tal har oändliga kedjebråk, vars värden definieras av:

$$[a_0; a_1, a_2, \ldots] = \lim_{n \to \infty} [a_0; a_1, a_2, \ldots, a_n],$$

där gränsvärdet alltid existerar om alla $a_i \in \mathbb{Z}_+$, alla $i \in \mathbb{Z}_+$.

Det gäller alltid att $\boldsymbol{\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}}$

och att $\boldsymbol{\frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k \, q_{k-1}}}$ för alla $k \in \mathbb{Z}_+$ med q_k, p_k definierade.

Sats: För α:s kedjebråk gäller (om q_{k+1} är definierat, dvs $\alpha \neq \frac{p_k}{q_k}$):

$$\boldsymbol{|\alpha - \frac{p_k}{q_k}| \leq \frac{1}{q_k q_{k+1}},}$$

med likhet omm a_{k+1} är den sista termen i kedjebråket (dvs $\alpha = \frac{p_{k+1}}{q_{k+1}}$).

För alla $k \in \mathbb{Z}_+$ är $\frac{p_k}{q_k}$ en **bästa (rationell) approximation till $\boldsymbol{\alpha}$**,

dvs $|\alpha - \frac{p'}{q'}| \leq |\alpha - \frac{p_k}{q_k}| \Rightarrow (\frac{p'}{q'} = \frac{p_k}{q_k}$ eller $|q'| > q_k)$ (om $\frac{p_k}{q_k}$ är definierad).