(Diskret matte D, ht16: F8, ti 13 sep 2016)

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

$$\begin{cases} x & = tq_0 + r_0 \\ q_0 & = tq_1 + r_1 \\ & \vdots \qquad\qquad 0 \leq r_i < t \\ q_{n-1} & = tq_n + r_n, \qquad q_n = 0 \text{ (gäller för något } n) \end{cases}$$

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 upprepa det kommer man till $\text{sgd}(d, 0) = d$, så d, a, b fås med **Euklides algoritm** ($n > 0$)
($\text{sgd}(m, n) = \text{sgd}(n, m) = \text{sgd}(\pm m, \pm n)$.)

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

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

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 $g \in \mathbb{Z}$ så att

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

Sats (nämndes kort F8): För alla $m, n \in \mathbb{Z}$ finns $\text{mgm}(m, n)$ entydigt och

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

Den **linjära diofantiska** (dvs vi söker heltalslösningar x, y) **ekvationen**

$$\boldsymbol{mx + ny = c} \qquad \boldsymbol{m, n, c} \text{ heltal}$$

är lösbar **omm** $\text{sgd}(m, n) \mid c$.

Om villkoret är uppfyllt, inte $m = n = 0$, och $d = \text{sgd}(m, n) = am + bn$ med $a, b \in \mathbb{Z}$ ges **alla** lösningar till ekvationen av $\begin{cases} x = \frac{c}{d}a + \frac{n}{d}k \\ y = \frac{c}{d}b - \frac{m}{d}k \end{cases}$, $k \in \mathbb{Z}$.

Den "normala" metoden för att lösa en sådan ekvation är att göra som i beviset för satsen, dvs bestämma $\text{sgd}(m, n) = d$ (med Euklides algoritm), dividera ekvationen med d, uttrycka 1 som en linjärkombination av (den nya) ekvationens koefficienter och multiplicera med dess högerled för att få en heltalslösning. **Eulers metod** (inte behandlad i boken) tar med högerledet från början och leder i allmänhet till mindre tal i den första lösningen.
Säg t.ex. att vi söker alla heltalslösningar till ekvationen $108x + 33y = 78$.
Euklides algoritm: $108 = 33 \cdot 3 + 9$, $33 = 9 \cdot 3 + 6$, $9 = 6 \cdot 1 + 3$, $6 = 3 \cdot 2 + 0$, så $d = \text{sgd}(108, 33) = 3$.
Division med d ger den ekvivalenta ekvationen $36x + 11y = 26$, där $\text{sgd}(36, 11) = 1$.
"Normala" metoden:
Från ovan: $36 = 11 \cdot 3 + 3$, $11 = 3 \cdot 3 + 2$, $3 = 2 \cdot 1 + 1$, $(2 = 1 \cdot 2 + 0)$ och "baklänges" ger det $1 = 3 - 2 = 3 - (11 - 3 \cdot 3) = -11 + 4 \cdot 3 = -11 + 4(36 - 3 \cdot 11) = 4 \cdot 36 - 13 \cdot 11$.
Multiplikation med 26 ger att $x_0 = 4 \cdot 26 = 104$, $y_0 = (-13) \cdot 26 = -338$ löser ekvationen.
Om x, y löser ekvationen blir $36(x - x_0) + 11(y - y_0) = 26 - 26 = 0$, så $36(x - x_0) = -11(y - y_0)$ och $11 \mid (x - x_0)$ (ty $\text{sgd}(11, 36) = 1$), $x = x_0 + 11k$, k ett heltal. Det ger $y - y_0 = -36k$ och insättning visar att dessa x, y också löser ekvationen för alla heltal k.
Eulers metod:
Lös ut den obekanta med (till beloppet) lägst koefficient: $y = \frac{26}{11} - \frac{36x}{11} = 2 - 3x + \frac{4-3x}{11}$.
x, y är en heltalslösning omm x och $z = \frac{4-3x}{11}$ är heltal, så omm x, z heltal med $3x + 11z = 4$, dvs $x = \frac{4}{3} - \frac{11z}{3} = 1 - 3z + \frac{1-2z}{3}$, så omm $z, u = \frac{1-2z}{3}$ heltal, dvs omm z, u är heltal med $2z + 3u = 1$, dvs $z = -u + \frac{1-u}{2}$, så omm $u, k = \frac{1-u}{2}$ heltal, så $u = 1 - 2k$, där k är ett godtyckligt heltal.
Insättning ger $z = -(1 - 2k) + \frac{1-(1-2k)}{2} = -1 + 3k$, $x = 1 - 3(-1 + 3k) + \frac{1-2(-1+3k)}{3} = 5 - 11k$ och $y = 2 - 3(5 - 11k) + \frac{4-3(5-11k)}{11} = -14 + 36k$.
Båda metoderna ger samma lösningar (med olika k, $k_{\text{normal}} = -k_{\text{Euler}} - 9$).

Aritmetikens fundamentalsats:
Varje heltal ≥ 1 kan på ett entydigt (bortsett från ordningen) sätt uttryckas som en produkt av primtal. (1 är "den tomma produkten".)

[Beviset för satsen bygger på möjligheten till division med en rest som är "mindre" än divisorn. Det gör att motsvarande sats om entydig (nästan) faktorisering gäller också för polynom och gaussiska heltal (faktoriseringarna kan här skilja sig åt dels vad gäller ordningen och dels faktorer som är konstanter respektive $1, i, -1, -i$).]

Om $m = p_1^{s_1} \dots p_k^{s_k}, n = p_1^{t_1} \dots p_k^{t_k}$ är (hanns inte F8)
$\text{sgd}(m, n) = p_1^{min(s_1,t_1)} \dots p_k^{min(s_k,t_k)}$ och $\text{mgm}(m, n) = p_1^{max(s_1,t_1)} \dots p_k^{max(s_k,t_k)}$.