(Diskret matte CL, vt10: F2, to 21 jan 2010)

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

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

$$
\begin{array}{ll}
m = q_1 n + r_1 & 0 \le r_1 < n \\
n = q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 \le r_3 < r_2 \\
\quad \vdots & \\
r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & 0 \le r_{k-1} < r_{k-2} \\
r_{k-2} = q_k r_{k-1} + 0 &
\end{array}
$$

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

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 $sgd(d, m) = 1$ (dvs 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 så att

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

Sats: För alla heltal m, n finns $mgm(m, n)$ entydigt och

$$\boldsymbol{mgm(m, n) sgd(m, n) = mn}.$$

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

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

är lösbar **omm** $sgd(m, n) \mid c$.

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

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

Modulär aritmetik

$$x \equiv y \pmod m, \quad \text{eller} \quad x \equiv_m y$$

betyder $m | (x - y)$ och läses "x är kongruent med y modulo m".

Sats: $x_1 \equiv_m x_2,\ y_1 \equiv_m y_2 \ \Rightarrow\ x_1 + y_1 \equiv_m x_2 + y_2,\ x_1 y_1 \equiv_m x_2 y_2$.

Varje heltal är kongruent med precis ett av $0, 1, 2, \dots, m - 1$ (i fallet $m = 2$ är alla jämna tal kongruenta med 0 och de udda med 1) och att räkna **modulo** $\boldsymbol{m}$ innebär att räkna "som vanligt, men med rest mod m".
Man låter $\mathbb{Z}_m = \{0, 1, \dots, m - 1\}$ och skriver t.ex.

$$4 \cdot 6 \equiv 3 \pmod 7, \quad 4 \cdot 6 \equiv_7 3 \quad \text{eller} \quad 4 \cdot 6 = 3 \text{ i } \mathbb{Z}_7.$$