(F8, on 8 feb 2006)

Delbarhet: $y \mid x$ betyder $x = yq$, något $q \in \mathbb{Z}$

Om $a, b \in \mathbb{Z}$ och för $c > 0$ gäller $c \mid a, c \mid b$ kallas c en **gemensam delare** till a och b.
Om $a, b \in \mathbb{Z}$ och
i) $c \mid a, c \mid b$
ii) d gemensam delare till a och $b \Rightarrow d \mid c$
iii) $c \geq 0$
kallas c en **största gemensam delare**, sgd, till a och b.
(Boken har $d \mid a, d \mid b \Rightarrow d \leq c$ i stället för ii) och iii))

Sats: Om $a, b \in \mathbb{Z}$, $b \geq 1$, finns entydigt $q, r \in \mathbb{Z}$ med $0 \leq r < b$ och $a = bq + r$.

Talet q kallas **kvoten** av a och b, r kallas **resten**

Sats: Om inte $a = b = 0$, existerar $d = sgd(a, b)$ entydigt och $d = ma + nb$ för några $m, n \in \mathbb{Z}$

d, m, n fås med **Euklides algoritm** ($b > 0$)

$$\begin{array}{ll}
a = bq_1 + r_1 & 0 \leq r_1 < b \\
b = r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\
r_1 = r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \\
\quad \vdots & \\
r_{k-2} = r_{k-1} q_k + r_k & 0 \leq r_k < r_{k-1} \\
r_{k-1} = r_k q_{k+1} + 0 &
\end{array}$$

Detta ger $sgd(a, b) = r_k$.

Primtal är heltal $p \geq 2$, sådana att $n > 0, n \mid p \Rightarrow n = 1$ eller $n = p$.

Sats(Euklides): Det finns oändligt många primtal.

Sats: Varje heltal ≥ 1 kan skrivas som en produkt av primtal.
(1 är "den tomma produkten".)

Lemma: Om p primtal och $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, så $p \mid x_1 x_2 \ldots x_n \Rightarrow p \mid x_i$, något i.

Aritmetikens huvudsats: Primfaktoriseringen av $n \geq 1$ är unik, bortsett från ordningen.