(F7, fr 24 jan)

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** $(b > 0)$

$$\begin{array}{ll}
a = bq_1 + r_1 & 0 \leq r_1 < b \\
b = r_1 q_2 + r_2 & 0 \leq r_2 < r_1 \\
r_1 = r_2 q_3 + r_3 & 0 \leq r_3 < r_2 \\
\quad \vdots & \\
r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} & 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} = r_{k-1} q_k + 0 &
\end{array}$$

Detta ger $sgd(a, b) = r_{k-1}$.

Enkel **Diofantisk ekvation**

$ax + by = c, \quad x, y \in \mathbb{Z}$

lösbar omm $d = sgd(a, b) \mid c$

$$\text{Allmän lösning: } \begin{cases} x & = x_0 + k\frac{b}{d} \\ y & = y_0 - k\frac{a}{d} \end{cases} \quad k \in \mathbb{Z}$$

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

Sats: Varje heltal ≥ 2 kan skrivas som en produkt av primtal.

Sats: 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 $n \geq 2$ är unik, bortsett från ordningen.