

(SF1662 Diskret matte CL1, vt12: F3, on 25 jan 2012)

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

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

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

Om villkoret är uppfyllt, inte $m = n = 0$, och $d = \text{sgd}(m, n) = am + bn$ med a, b heltal ges **alla** lösningar till ekvationen av

$$\begin{cases} x = \frac{c}{d}a + q\frac{n}{d} \\ y = \frac{c}{d}b - q\frac{m}{d}, \end{cases} \quad q \text{ godtyckligt heltal.}$$

Aritmetikens fundamentalsats:

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

[En väsentlig grund för beviset för satsen är möjligheten till division med en rest som är "mindre" än divisorn. Senare ska vi se att motsvarande metod kan användas för att visa (så gott som) entydig faktorisering för polynom och för gaussiska heltal.]

Om $m = p_1^{s_1} \dots p_k^{s_k}$ och $n = p_1^{t_1} \dots p_k^{t_k}$, där p_i :na är olika primtal är

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

Det ger vårt tidigare resultat

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