

(SF1662 Diskret matte, vt17: F3, ti 24 jan 2017)

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

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

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 heltal ges **alla** lösningar till ekvationen av

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

(Om $m = n = 0$ är $\text{sgd}(m, n) = 0$ och ekvationen är lösbar omm $c = 0$, med lösningar alla x, y .)

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 algoritmen), 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 algoritmen: $108 = 33 \cdot 3 + 9$, $33 = 9 \cdot 3 + 6$, $9 = 6 \cdot 1 + 3$, $6 = 3 \cdot 2 + 0$, 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: $36 = 11 \cdot 3 + 3$, $11 = 3 \cdot 3 + 2$, $3 = 2 \cdot 1 + 1$, ($2 = 2 \cdot 1 + 0$) 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".)

[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 (då $m, n > 0$)

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

(Hanns inte på föreläsningen:)

Sats (Euklides): Det finns oändligt många primtal.

Visades med ett motsägelsebevis: Om $p_1, p_2, \dots, p_N$ vore alla primtal skulle talet $p_1 \cdot p_2 \cdot \dots \cdot p_N + 1$ inte vara delbart med något primtal.

Det gäller t.o.m. att " $\sum_{p \text{ primtal}} \frac{1}{p} = \infty$ ", men det visade vi inte.