Forrige gang: Euklids alg for å finne $\gcd(a,b)$

2.5 Diofantiske ligninger

Def: En Diofantisk ligning er en ligning med en eller flere ukjente hvor vi kun søker heltallsløsninger.

Eksempler: (1) Ligningen $3x = 1$ har ingen løsn. som Diof. ligning.

(2) Som Diof. ligning har

$$x^2 + y^2 = 4$$

fire løsninger:

$$(x,y) \in \{(0,2), (0,-2), (2,0), (-2,0)\}$$

(3) Som Diof. ligning har

$$x^n + y^n = z^n \quad (n \geq 3)$$

ingen løsn med $xyz \neq 0$ (Fermats siste teorem)

(4) Påstand: som Diof. ligning har

$$x^2 + y^2 = 3z^2$$

kun den trivielle løsningen $x=y=z=0$.

Steg 1: Hvis en løsning x_0, y_0, z_0 eksisterer, så eksisterer det også en løsning x_1, y_1, z_1 med $\gcd(x_1, y_1, z_1) = 1$. Vis dette.

Steg 2: Anta x_0, y_0, z_0 er en løsning med $\gcd(x_0, y_0, z_0) = 1$. Da vil $3 \nmid x_0$ og $3 \nmid y_0$. Vis dette.

Steg 3: Anta ligningen er løsbar. Fra Steg 1 og 2 finnes det da en løsn x_0, y_0, z_0 med

(a) $\gcd(x_0, y_0, z_0) = 1$

(b) $3 \nmid x_0$ og $3 \nmid y_0$

Både x_0 og y_0 er derfor på formen $3k+1$ eller $3k+2$. Så $\exists$ $m, n \in \mathbb{Z}$ med

$$x_0 = 3m + i$$
$$y_0 = 3n + j$$

hvor $i, j \in \{1, 2\}$. Dette gir

$$\begin{aligned} 3z_0^2 &= x_0^2 + y_0^2 \\ &= (3m+i)^2 + (3n+j)^2 \\ &= 3(3m^2 + 2mi + 3n^2 + 2nj) + (i^2 + j^2) \end{aligned}$$

som igjen gir

$$i^2 + j^2 = 3(z_0^2 - 3m^2 - 2mi - 3n^2 - 2nj)$$

Det betyr at $3 \mid (i^2 + j^2)$. Umulig siden $i, j \in \{1, 2\}$.

(5) Konsekvens av (4): sirkelen $x^2 + y^2 = 3$ har ingen rasjonale punkter (vis).

Teorem 2.9

La $a, b, c \in \mathbb{Z}$ og sett $d = \gcd(a,b)$. Den lineære Diof. ligningen

$$ax + by = c$$

er løsbar hvis og bare hvis $d \mid c$. Hvis x_0, y_0 er en løsning, så er alle løsningene gitt ved

$$x = x_0 + (b/d)t$$
$$y = y_0 - (a/d)t$$

for $t \in \mathbb{Z}$ (én løsn for hver $t \in \mathbb{Z}$).

Bevis: Vi har vist første del tidligere. Anta nå at x_0, y_0 er en løsning, dvs $ax_0 + by_0 = c$, og la $t \in \mathbb{Z}$. Da er

$$a\left(x_0 + \tfrac{b}{d}t\right) + b\left(y_0 - \tfrac{a}{d}t\right) = ax_0 + by_0 + \tfrac{ab}{d}t - \tfrac{ab}{d}t$$
$$= c$$

så $x_0 + (b/d)t$, $y_0 - (a/d)t$ er en løsning $\forall t \in \mathbb{Z}$. Anta nå at x, y er en løsning. Da får vi

$$ax_0 + by_0 = c = ax + by$$

som gir

$$b(y_0 - y) = a(x - x_0)$$

Siden $\gcd(a,b) = d$ finnes $q_1, q_2 \in \mathbb{Z}$ med $a = q_1 d$ og $b = q_2 d$, og $\gcd(q_1, q_2) = \gcd(a/d, b/d) = 1$ fra korollar til Teorem 2.4. Setter inn over og får da

$$q_2(y_0 - y) = q_1(x - x_0)$$

Siden $q_2 \mid q_1(x - x_0)$ og $\gcd(q_1, q_2) = 1$ gir Euklids lemma at $q_2 \mid (x - x_0)$, dvs $x - x_0 = q_2 t$ for en $t \in \mathbb{Z}$. Dette igjen gir

$$q_2(y_0 - y) = q_1(x - x_0) = q_1 q_2 t$$

dvs

$$y_0 - y = q_1 t$$

Konklusjon:

$$x = x_0 + q_2 t = x_0 + (b/d)t$$
$$y = y_0 - q_1 t = y_0 - (a/d)t$$

Så alle løsn av $ax + by = c$ er på denne formen. □

Eksempel: Eksamen K2017, oppg 1:

Finn alle heltallsløsn av $143x + 364y = 13$ som oppfyller $0 < x < 10$

Euklids alg:

$$364 = 2 \cdot 143 + 78$$
$$143 = 1 \cdot 78 + 65$$
$$78 = 1 \cdot 65 + 13$$
$$65 = 5 \cdot 13$$

Så $\gcd(143, 364) = 13$ (og ligningen er løsbar siden $13 \mid 13$). Bakover:

$$13 = 78 - 65 = 78 - (143 - 78) = 2 \cdot 78 - 143 = 2(364 - 2 \cdot 143) - 143$$
$$= 143 \cdot (-5) + 364 \cdot 2$$

En løsn er derfor $x_0 = -5$, $y_0 = 2$. Alle løsn da gitt ved

$$x = -5 + (364/13)t = -5 + 28t$$
$$y = 2 - (143/13)t = 2 - 11t$$

for $t \in \mathbb{Z}$. Har nå

$$0 < x \Rightarrow 0 < -5 + 28t \Rightarrow 0.18 \approx 5/28 < t$$
$$x < 100 \Rightarrow -5 + 28t < 100 \Rightarrow t < 105/28 = 3.75$$

Dette betyr at $0 < x < 100$ når $t \in \{1, 2, 3\}$. De tre løsn av ligningen som oppfyller $0 < x < 100$ er derfor:

$x = 23$, $y = -9$ $(t = 1)$
$x = 51$, $y = -20$ $(t = 2)$
$x = 79$, $y = -31$ $(t = 3)$