Forrige gang: * $\gcd(a,b)$: egenskaper ($\exists$ x,y med $ax+by=\gcd(a,b)$)

* Ligningen $ax+by=c$ løsbar $\Leftrightarrow$ $\gcd(a,b)$ deler c

2.4 Euklids algoritme

Problem: Hvordan finne $\gcd(a,b)$?

Lemma Hvis $a=qb+r$ så er $\gcd(a,b)=\gcd(b,r)$

Bevis: Hvis $d|a$ og $d|b$ så vil $d|(a-qb)$, dvs $d|r$. Altså vil da $d|b$ og $d|r$. Hvis $d'|b$ og $d'|r$ vil $d'|(qb+r)$, dvs $d'|a$. Altså vil $d'|a$ og $d'|b$. Vis at dette er nok $\square$

Euklids algoritme

Anta $a \geq b \geq 0$. Div alg gir

$$a = q_1 b + r_1 \qquad 0 \leq r \leq b-1$$

Hvis $r_1 \neq 0$, gjenta med b og r_1:

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 \leq r_1 - 1$$

Hvis $r_2 \neq 0$, gjenta med r_1 og r_2:

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 \leq r_2 - 1$$

Fortsett til vi får

$$r_{n-1} = q_{n+1} r_n + 0$$

dvs r_n er siste rest ulik null. Fra lemmaet er da

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_n,0) = r_n$$

Merk: (1) Dette vil stoppe siden $b > r_1 > r_2 > \cdots \geq 0$.

(2) Ved å bruke alle likhetene kan vi nøste oss opp bakover og uttrykke $\gcd(a,b)=r_n$ som en lin. komb av a og b:

$$ax_0 + by_0 = r_n$$

(3) $\gcd(a,b) = \gcd(|a|,|b|)$, så kan anta $a \geq b \geq 0$.

Eksempler: (1) $\gcd(84,30)$:

$$84 = 2\cdot 30 + 24$$
$$30 = 1\cdot 24 + 6$$
$$24 = 4\cdot 6 + 0$$

Så $\gcd(84,30) = 6$. Nøster oss bakover:

$$\begin{aligned} 6 &= 30 - 24 \\ &= 30 - (84 - 2\cdot 30) \\ &= 84\cdot(-1) + 30\cdot 3 \end{aligned}$$

(2) $\gcd(154,-350)$:

$$350 = 2\cdot 154 + 42$$
$$154 = 3\cdot 42 + 28$$
$$42 = 1\cdot 28 + 14$$
$$28 = 2\cdot 14 + 0$$

Så $\gcd(154,-350) = 14$. Nøster oss bakover:

$$\begin{aligned} 14 &= 42-28 \\ &= 42-(154-3\cdot 42) \\ &= 154\cdot(-1) + 42\cdot 4 \\ &= 154\cdot(-1) + (350-2\cdot 154)\cdot 4 \\ &= 154\cdot(-9) + 350\cdot 4 \\ &= 154\cdot(-9) + (-350)\cdot(-4) \end{aligned}$$

(3) Har ligningen $256x + 560y = 112$ heltallsløsn? Hvis ja, finn en løsning.

Har sett (Teorem 2.9) at den er løsbar $\iff \gcd(256,560)$ deler 112.

$$560 = 2\cdot 256 + 48$$
$$256 = 5\cdot 48 + 16$$
$$48 = 3\cdot 16 + 0$$

Så $\gcd(256,560) = 16$. Siden $112 = 7\cdot 16$ er ligningen løsbar.

$$\begin{aligned} 16 &= 256 - 5\cdot 48 \\ &= 256 - 5(560 - 2\cdot 256) \\ &= 256\cdot 11 + 560\cdot(-5) \end{aligned}$$

Så

$$\begin{aligned} 112 = 7\cdot 16 &= 256\cdot(11\cdot 7) + 560\cdot((-5)\cdot 7) \\ &= 256\cdot 77 + 560\cdot(-35) \end{aligned}$$

En løsn er derfor $x = 77$, $y = -35$.

Skal se: Hvis $ax+by=c$ er løsbar, har den uendelig mange løsn. Hvis x_0, y_0 er en løsning, er <u>alle</u> løsningene gitt ved

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

hvor $t \in \mathbb{Z}$ (og $d = \gcd(a,b)$).

Eksempel: For ligningen $256x + 560y = 112$ fant vi løsningen

$$x_0 = 77, \quad y_0 = -35$$

Siden $\gcd(256, 560) = 16$ er alle løsn gitt ved

$$x = 77 + \frac{560}{16} t$$

$$y = -35 - \frac{256}{16} t$$

dvs

$$x = 77 + 35t$$

$$y = -35 - 16t$$

hvor $t \in \mathbb{Z}$. For $t = -2$ for eksempel, får vi løsningen

$$x = 77 + 35 \cdot (-2) = 7$$

$$y = -35 - 16 \cdot (-2) = -3$$

(Sjekk at $x = 7, y = -3$ er en løsning.)

Oppgave: Vis at $104x - 120y = 40$ er løsbar (heltallsløsn), og finn alle løsningene.