DELELIGHET OG EUKLIDS ALGORITME

Vi har $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{N} = \{1, 2, 3, \dots\}$

- For $a, b \in \mathbb{Z}$ sier vi at b deler a dersom det finns $q \in \mathbb{Z}$ s.a. $a = qb$
- Alle tall vil dele 0

Teorem 1.1. La $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Da finns unike $q, r \in \mathbb{Z}$ s.a $0 \leq r < b$ og

$$a = qb + r$$

Bevis

EKSISTENS:

Anta at $a \geq 0$. Dersom $a = 0$ setter vi $q = r = 0$.

Ellers la q vær det største positive tallet s.a $qb \leq a$. Dersom $qb = a$ setter vi $r = 0$

Så anta at $qb < a$.

Da har vi $a - qb < b$

Sett $r = a - qb$

Da er $qb + r = a$.

For $a < 0$, anvend resultatet på $(-a)$.

Unikhet.

Anta at

$$q_1 b + r_1 = q_2 b + r_2$$

$$(q_1 - q_2)b + (r_1 - r_2) = 0 = qb + r$$

OK dersom $q = 0$

Hvis $q > 0$

$$qb + r \geq b + r > 0$$

$$r > -b$$

$q < 0$

DEF La $m,n \in \mathbb{Z}$. Ethvert heltall som deler både m og n kalles en felles divisor til m og n. Dersom m og n ikke begge er null finns en største felles divisor som vi betegner med (m,n).

Sett $(0,0) = 0$.

Dersom $(m,n) = 1$ sier vi at m og n er innbyrdisk primiske.

DEF: For $a,b \in \mathbb{Z}$ sier vi at $c \in \mathbb{Z}$ er en lineær kombinasjon av a, b dersom $c = sa + tb$ for $s,t \in \mathbb{Z}$

Vi lar $I(a,b)$ betegne mengden av alle lineære kombinasjoner.

Lemma 1.2. Anta at $d \mid a$ og $d \mid b$.

Da har vi at $d \mid c$ for alle $c \in I(a,b)$.

Pf: $a = pd$, $b = qd$.

$c = sa + tb$

$= spd + t \cdot qd = (sp + tq)d$ ∎

Lemma 1.3. La $a, b \in \mathbb{Z}$, og la d være det minste positive elementet i $I(a,b)$. Da består $I(a,b)$ nøyaktig av multiplum av d.

Bevis: $c \in I(a,b) \iff c = q \cdot d$

($\Leftarrow$) Anta at $c = qd$.

Da $qd = q(sa + tb) = (qs)a + (qt)b$

Anta at $c = ma + nb > 0$. Da har vi $c \geq d$.

Nå kan vi skrive $c = qd + r$, der $0 \leq r < d$.

Dersom $r = 0$ er vi ferdig. Ellers har vi

$$c = ma + nb = q(sa + tb) + r$$

og det impliserer

$$(m - qs)a + (n - qt)b = r,$$

og det er en motsigelse.

Teorem 1.4. La $a, b \in \mathbb{Z}$. Da består $I(a,b)$ av alle elementer som er delelige med (a,b).

Bevis: $I(a,b)$ består av alle elementer delelige med tidligere definert d, så vi viser at $d = (a,b)$.

Vi har vist at d deler alle elementer i $I(a,b)$, spesielt $d \mid a$, $d \mid b$.

ed (a,b)

lelige

ulter

La d' være en felles divisor for a og b. Da må d' også dele d siden d er en lineær kombinasjon av a og b.

Anta at vi har lyst til å løse en ligning

$$ax + by = c$$

der $a,b,c \in \mathbb{Z}$,

og vi bare ønsker løsninger i $\mathbb{Z}$.

Da har vi sett at $(a,b) \mid c$. $\quad c = q\,(a,b)$

La oss se om vi kan løse

$$ax + by = (a,b)$$

Diofantisk ligning

EUKLIDS ALGORITME

Gitt $a, b \in \mathbb{Z}$. Ønsker å løse

$ax + by = (a,b)$, med $x, y \in \mathbb{Z}$.

Vi antar at $b > 0$.

La oss skrive $r_0 = a$, $r_1 = b$

$$r_0 = q_1 r_1 + r_2$$
$$r_1 = q_2 r_2 + r_3$$
$$r_2 = q_3 r_3 + r_4$$
$$\vdots$$
$$r_j = q_{j+1} r_{j+1} + r_{j+2}$$
$$\vdots$$
$$r_n = q_{n+1} r_{n+1} + r_{n+2}$$
$$r_{n+1} = q_{n+2} r_{n+2}.$$

Påstand: $r_{n+2} = (a,b)$.

(1) $r_{n+2} \mid a$ og $r_{n+2} \mid b$.

Merk at r_{n+2} deler r_{n+1} og r_n.

Men dvs om r_{n+2} deler r_{j+2} og r_{j+1},

så deler r_{n+2} også r_j

Baklvendt induksjon gir resultatet.

(2) La d' være en felles divisor til a og b.

Ved induksjon hvis vi $d' \mid r_{n+2}$.

Lemma 1.8. Anta at $(a',b')=1$.
Anta at $a' \mid b'c$.
Da har vi $a' \mid c$.

Bevis. • $sa' + tb' = 1$

• $b'c = da'$

Da har vi $c = csa' + tb'c$

$= a'cs + tda' = a'(cs+td)$. ∎