Tallteori

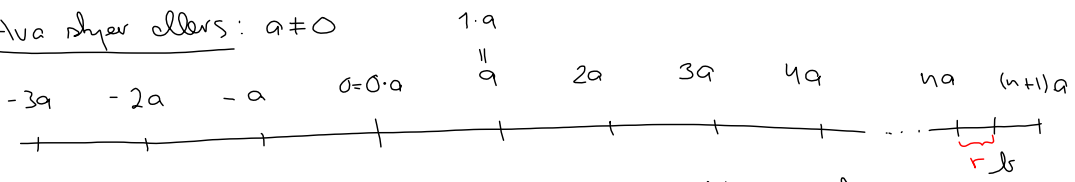
Husker om: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$

Grunnbegrep: Vi sier at $a \in \mathbb{Z}$ er delelig på $b \in \mathbb{Z}$ dersom det finnes et tall $n \in \mathbb{Z}$ slik at $a = nb$

(alternativt: $\frac{a}{b} \in \mathbb{Z}$)

Hva betyr ellers: $a \neq 0$



Divisjonsalgoritmen: Hvis $a, b \in \mathbb{Z}$ og $a \neq 0$, så finnes det $q, r \in \mathbb{Z}$ slik $0 \leq r < a$ og

$$b = qa + r$$

entydig bestemt. r kalles resten.

Eksempel: $b = 243$, $a = 7$:

$243 : 7 = 34$ — q

21

33

28

5 — r

$243 = 34 \cdot 7 + 5$

Hvis $a, b \in \mathbb{Z}$, heter c en felles faktor dersom $c \mid a$ og $c \mid b$ (c deler a)

Den største felles faktoren til a og b er det største tallet som går opp i både a og b. Dersom $a = b = 0$, setter vi $(0, 0) = 0$.

Hvordan finner vi største felles divisor?

Skolemetoden: $a = 54$, $b = 90$

Faktoriserer 54 og 90:

54 | 2
27 | 3
9 | 3
3

$54 = 2 \cdot 3 \cdot 3 \cdot 3$

90 | 2
45 | 3
15 | 3
5

$90 = 2 \cdot 3 \cdot 3 \cdot 5$

Største felles divisor: $2 \cdot 3 \cdot 3 = 18$

Sjekk: $54 = 3 \cdot 18$ og $90 = 5 \cdot 18$

Alternativ metoden: Hvis $a, b \in \mathbb{Z}$, så kalles c en lineærkombinasjon av a, b dersom det finnes tall $s, t \in \mathbb{Z}$ slik at

$$c = sa + tb$$

Annen formulering: c er en lin. komb. av a og b dersom ligningen

$$c = ax + by$$

har løsninger $x, y \in \mathbb{Z}$.

Mål: Finne ut når c er en lin. kombinasjon av a og b.

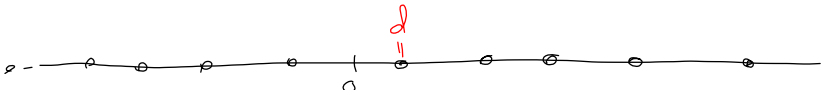
Def: $I(a,b) = \{sa+tb : s,t \in \mathbb{Z}\}$ = mengden av alle lin. komb. av a og b.

Lemma: Anta at $c|a$, $c|b$, da vil vilkårlige elementer i $I(a,b)$ være delelig med c.

Bevis: Siden $c|a$, finnes det en $m \in \mathbb{Z}$ slik at $a = mc$
Siden $c|b$ ——"—— $n \in \mathbb{Z}$ —"— $b = nc$
Hvis $d \in I(a,b)$, da er $d = sa+tb = smc + tnc = \underbrace{(sm+tn)}_{\in \mathbb{Z}}c$,
dvs $c|d$.

Eksempel: $I(4,6)$ 2 deler både 4 og 6,
så 2 deler alle elementene i $I(4,6)$,
F.eks. $1 \notin I(4,6)$

Lemma: Anta at ikke både a og b er null, og la d være det minste positive elementet i $I(a,b)$. Da er alle tallene i $I(a,b)$ delelig med d.



Bevis: Anta d det finnes et tall $c \in I(a,b)$ som ikke er delelig med d. Da $c = qd + r$ der $0 < r < d$. Dermed er

$$r = \underbrace{c}_{sa+tb} - q\underbrace{cd}_{sa+t'b} = sa+tb - q(sa+t'b) = (s-qs')a + (t-qt')b \in I(a,b)$$

Dette er en selvmotsigelse siden d var det minste positive tallet i $I(a,b)$ og $0 < r < d$. Altså er alle tallene i $I(a,b)$ delelig med d.

Teorem: $I(a,b)$ består nøyaktig av det tallene som er delelig med største felles faktor (a,b) til a og b.

Bevis: La d være det minste positive tallet i $I(a,b)$. Da vil ifølge lemmaet alle tallene i $I(a,b)$ være delelig med d.
Spesielt er a og b delelig med d siden

$$a = 1 \cdot a + 0 \cdot b \in I(a,b)$$
$$b = 0 \cdot a + 1 \cdot b \in I(a,b)$$

Følgelig er d en felles faktor i a og b.
Videre vet vi at siden $d \in I(a,b)$, så går alle felles faktorer til a og b opp i d. Dette betyr at $d = (a,b)$.
Det gjenstår å vise at $I(a,b) = \{nd : n \in \mathbb{Z}\}$.
Siden alle elementer i $I(a,b)$ er delelig med d, så
$I(a,b) \subseteq \{nd : n \in \mathbb{Z}\}$.
På den andre siden, siden $d \in I(a,b)$, så er $d = sa+tb$ for $s,t \in \mathbb{Z}$. Dermed er

$$nd = n(sa+tb) = (ns)a + (nt)b \in I(a,b),$$

dvs $\{nd : n \in \mathbb{Z}\} \subseteq I(a,b)$
Dermed er $I(a,b) = \{nd : n \in \mathbb{Z}\}$ der $d = (a,b)$.

Oppsummering

1 c er en lin.komb av a og b (dvs $c = sa+tb$ for $s,t \in \mathbb{Z}$) hvis og bare hvis $(a,b) \mid c$

2 Ligning $ax+by=c$ har en løsning $x,y \in \mathbb{Z}$ hvis og bare hvis $(a,b) \mid c$.

Korollar: Hvis d er største felles faktor til a,b $(a,b \neq 0)$, så er vil alle andre felles faktorer dele d.

Bevis: Vi vet $d \in I(a,b)$ og at hvis c er en felles faktor for a og b, så deler c alle elementene i $I(a,b)$. Spesielt vil c dele d.

Setning: Hvis a og b er innbyrdes primiske (dvs. at de ikke har felles faktorer) og $b \mid ac$, så vil $b \mid c$.

Bevis: Siden a og b er innbyrdes primiske, er den største felles faktoren 1. Altså finnes det $s,t \in \mathbb{Z}$ slik at

$$1 = sa + tb \quad | \cdot c$$

dvs

$$c = sac + tbc \qquad (\text{Vet at } ac = nb \text{ for } n \in \mathbb{Z})$$

$$= snb + tbc = (sn+tc)b$$

som viser at $b \mid c$.

Praktisk innledning: Hvordan finner vi en løsning av ligningen

$$c = ax + by \quad \text{der } x,y \in \mathbb{Z}.$$

Vet at ligningen kun har en løsning når $(a,b) \mid c$.

Euklids algoritme for å finne (a,b)

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n \quad \text{delelig med } r_{n+1}$$
$$r_{n-1} = q_{n+1} r_n + r_{n+1} \quad \text{delelig med } r_{n+1}$$
$$r_n = q_{n+1} r_{n+1} \quad \text{slutt ved som ikke er null.}$$

$r_{n+1} \mid r_n$

Påstand: Den siste ikke-null verdien r_{n+1} er største felles faktor til a og b.

Bevis: La oss først kunne at r_{n+1} er en felles faktor i a og b. Begynner nedre for:

$$r_{n-1} = q_{n+1} q_n r_{n+1} + r_{n+1}$$
$$= (q_{n+1} q_n + 1) r_{n+1}$$

$r_{n+1} \mid r_{n-1}$

Hvis i forsetter oppover denne veien, får i fort at alle r'ene er delelig med r_{n+1} og dermed at b og a er delelig med r_{n+1}.

For å vise at r_{n+1} er den største fellesfaktoren, viser vi at enhver felles faktor c for a og b nødvendigvis deler r_{n+1}.

Gjør nedover

$$a = q_1 b + r_1 \Rightarrow r_1 = a - q_1 b \qquad c \mid r_1$$
$$b = q_2 r_1 + r_2 \Rightarrow r_2 = b - q_2 r_1 \qquad c \mid r_2$$
$$r_1 = q_3 r_2 + r_3 \Rightarrow r_3 = r_1 - q_3 r_2 \qquad c \mid r_3$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$r_{n-1} = q_{n+1} r_n + r_{n+1} \qquad c \mid r_{n+1}$$

Altså er r_{n+1} en felles faktor som er delelig med alle andre felles faktorer, dvs r_{n+1} må være største felles faktor.

Eksempel: Finn største felles faktor til 210 og 32 ved hjelp av Euklids algoritme

Kladd:

$210 : 32 = 6$
192
18

$210 = 6 \cdot 32 + 18$
$32 = 1 \cdot 18 + 14$
$18 = 1 \cdot 14 + 4$
$14 = 3 \cdot 4 + 2$ — siste felles faktor.
$4 = 2 \cdot 2$

Dette betyr at 2 er en lin.komb $2 = s \cdot 210 + t \cdot 32$ av 210 og 32. Hvordan finner vi s og t? $s = -7$ $t = 46$

Bruker Euklids algoritme bakfra:

$2 = 14 - 3 \cdot 4 = 14 - 3(18 - 1 \cdot 14) = 4 \cdot 14 - 3 \cdot 18$
$= 4 \cdot (32 - 1 \cdot 18) - 3 \cdot 18 = 4 \cdot 32 - 7 \cdot 18$
$= 4 \cdot 32 - 7 \cdot (210 - 6 \cdot 32)$
$= 46 \cdot 32 - 7 \cdot 210 = (-7) \cdot 210 + 46 \cdot 32$

Dette viser hvordan vi kan skrive siste felles faktor som en lin. komb. av a og b. Hva med andre elementer i $I(a,b)$. Hvordan skrive fx 28 som en lin komb?

$28 = 14 \cdot 2 = 14 \cdot ((-7) \cdot 210 + 46 \cdot 32) = (-98) \cdot 210 + 644 \cdot 32$