3/10 - 2013

MAT 1140

Tallteori

Vi skal nå studere de hele tallene

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

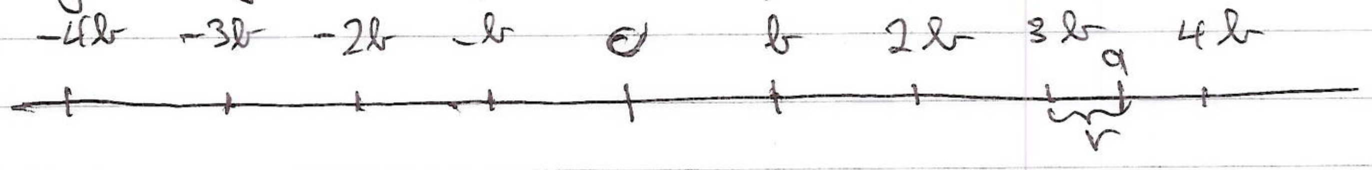
med spesiell vekt på delelighet. Et viktig hjelpemiddel vil være mengden

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

av naturlige tall

Anta at $a, b \in \mathbb{Z}$, $b \neq 0$. Vi sier at a er <u>delelig</u> <u>med</u> b dersom det finnes en $q \in \mathbb{Z}$ slik at $a = qb$. Med symboler skriver vi $b|a$.

Tallene som er delelig med b, ligger jevnt fordelt på tallinjen



Siden ethvert helt tall a ligger i et av intervallene $[qb, (q+1)b)$, finnes det en q og en r, $0 \leq r < b$, slik at

$$a = qb + r.$$

q kalles den (ufullstendige) kvotienten og r kalles resten.

Praktisk divisjonsalgoritme:

$$\begin{array}{l} 243 : 7 = 34 \\ \underline{21} \\ \;\;33 \\ \;\;\underline{28} \\ \;\;\;\;5 \end{array}$$

Da er 34 kvotienten og 5 resten.

$243 = 34 \cdot 7 + 5$

En felles divisor for m og n er et tall som går opp i både m og n. Dersom ikke både m og n er null, lar vi (m,n) være den største felles divisoren til m og n. Hvis både m og n er null, setter vi (m,n) = 0.

Skolemetoden for å finne største felles divisor: Faktorisér begge tallene, og gang sammen de felles primfaktorene

$$\left.\begin{array}{l} m = 24 = 2 \cdot 2 \cdot 2 \cdot 3 \\ n = 54 = 2 \cdot 3 \cdot 3 \cdot 3 \end{array}\right\} \text{felles } 2 \cdot 3 = \underline{6}$$

Denne metoden er effektiv for små tall, men ineffektiv for store tall siden faktorisering er arbeidskrevende.

Vi skal arbeide oss frem til en mer effektiv metode.

Anta $a, b \in \mathbb{Z}$. Vi sier at $c \in \mathbb{Z}$ er en lineærkombinasjon av a og b dersom det finnes tall $s, t \in \mathbb{Z}$ slik at

$$c = sa + tb$$

Mengden av alle lineærkombinasjoner av a, b betegnes med $I(a,b)$.

Lemma: Anta at $d \mid a$ og $d \mid b$. Da deler d alle elementene i $I(a,b)$

Bevis: Vi har $a = q_1 d$ og $b = q_2 d$. Hvis $c \in I(a,b)$, har vi da

$$c = sa + tb = sq_1 d + tq_2 d = (sq_1 + tq_2)d$$

som viser at c er delelig med d

Lemma: Anta at a, b ikke begge er null. Da består $I(a,b)$ nøyaktig av de tallene som er delelig med d, der d er det minste positive tallet i $I(a,b)$.

~~Bevis:~~

Bevis: Anta $d \mid c$. Da finnes det tall q, s, t slik at $c = qd$ og $d = sa + tb$. Dermed er

$$c = (sq)a + (tq)b \in I(a,b)$$

Anta c ikke er delelig med d, og anta for motsigelse at $c \in I(a,b)$. Da er

$$c = sa + tb$$

og $c = qd + r$. Vi vet også at $d = s'a + t'b$. Dermed er

$$r = c - qd = (s - qs')a + (t - qt')b$$

som viser at $r \in I(a,b)$. Det er umulig siden $r < d$ og d er det minste positive elementet i $I(a,b)$

Teorem: La $a, b \in \mathbb{Z}$. Da består $I(a,b)$ av nøyaktig de hele tallene som kan deles med (a,b)

Bevis: Hvis både a og b er 0, er påstanden opplagt riktig. Hvis a, b ikke begge er null er det nok å vise at $(a,b) = d$, det minste positive tallet i $I(a,b)$.

~~Vi vet at alle elementene i $I(a,b)$~~ er ~~delelig~~ med d, så $d \mid (a,b)$

Siden d deler alle elementene i $I(a,b)$, deler d både a og b, og er dermed en felles divisor. På den annen side er d delelig med alle felles divisorer, og må dermed være største felles divisor.

<u>Korollar:</u> Største felles divisor av to tall er delelig med alle andre felles divisorer.

<u>Korollar:</u> Ethvert helt tall kan skrives som en lineær kombinasjon av a og b hvis og bare hvis a og b er innbyrdes primisk, dvs største felles faktor er 1.

—

Mer generelt ser vi at ligningen

$$ax + by = c$$

har heltallige løsninger x, y hvis og bare hvis c er delelig med (a, b).

—

For å finne løsningene bruker vi en metode som kalles Euklids algoritme.

Vi demonstrerer metoden på et eksempel.

La $a = 208$, $b = 18$. Vi deler det største tallet på det minste

$$208 = 11 \cdot 18 + 10$$ flytter opp

$$18 = 1 \cdot 10 + 8$$

$$10 = 1 \cdot 8 + 2$$ — siste rest er største felles divisor.

$$8 = 4 \cdot 2$$

Arbeider oppover igjen

$$2 = 10 - 1\cdot 8 = 10 - (18 - 1\cdot 10)$$

$$= -18 + 2\cdot 10 = -18 + 2(208 - 11\cdot 18)$$

$$= \underline{2\cdot 208 - 23\cdot 18}$$

Generelt:

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$
$$r_n = q_{n+2} r_{n+1}$$

$\Downarrow$ felles faktor deler alle r'ene

$\Uparrow$ Hvis noe deler r_{n+1} deler det også alle r'ene og a og b

Altså er r_{n+1} største felles divisor