Divisjonsalgoritmen

Anta at $a \in \mathbb{Z}$ og $b \in \mathbb{N}$. Da finnes det entydig bestemte tall $q, r \in \mathbb{Z}$ slik at

$$a = qb + r \quad , \quad 0 \leq r < b$$

Delelighet

For hele tall a og b sier vi at *a er delelig med b* dersom det finnes et helt tall q slik at

$$a = qb$$

Vi sier også at *b går opp i a* og at *b deler a*. Med symboler skriver vi

$$b|a$$

Dersom a deler b og b deler c, så vil a dele c.

Dersom $a|b$ og $a|c$, så har vi $a|(nb + mc)$

SFF og MFM

$SFF(n, m)$: Største felles faktor for to hele positive tall n og m.

$MFM(n, m)$: Minste felles multiplum av to hele positive tall n og m.

Dersom n og m ikke har noen felles faktor (annet enn 1), så vil $SFF(n, m) = 1$ og $MFM(n, m) = n \cdot m$.

Dersom vil tilfører en felles faktor q, dvs. vi ser på tallene qn og qm, så har vi at $SFF(qn, qm) = q$, og $MFM(qn, qm) = q \cdot MFM(n, m) = qnm$. Det gir

$$SFF(qn, qm) \cdot MFM(qn, qm) = q \cdot qnm = qn \cdot qm$$

Euklids algoritme

Gitt to positive hele tall, a og b. Vi skal finne største felles faktor $SFF(a, b)$. Vi starter med å dele det største av tallene (la oss si det er a) med det minste:

$$a = q_1 b + r_1$$

Hvis divisjonen ikke går opp, deler vi nå b med resten r_1:

$$b = q_2 r_1 + r_2.$$

Deretter deler vi den første resten med den andre:

$$r_1 = q_3 r_2 + r_3$$

Så deler vi r_2 med r_3:

$$r_2 = q_4 r_3 + r_4$$

Vi fortsetter på denne måten inntil divisjonen går opp (siden hver rest er mindre enn den foregående, må vi til slutt få en rest som er null).

Dersom r_n er den siste resten som ikke er null, har vi nå utført følgende divisjoner

$$
\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
r_2 &= q_4 r_3 + r_4 \\
\vdots \quad & \vdots \quad \vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}
$$

Påstanden er nå at den siste ikke-null resten r_n er den største felles divisoren til a og b.

La oss først vise at r_n deler både a og b. Starter vi nedenfra i ligningene våre, ser vi at $r_n|r_{n-1}$. Fra den nest nederste ligningen følger det at $r_n|r_{n-2}$. Men hvis $r_n|r_{n-1}$ og $r_n|r_{n-2}$, så følger det fra den tredje nederste ligningen at $r_n|r_{n-3}$. Fortsetter vi oppover i systemet på denne måten, ser vi at r_n må dele alle venstresidene i ligningene, og til slutt får vi at $r_n|b$ og $r_n|a$.
Dermed vet vi at r_n er en felles divisor.

For å vise at det er den *største* felles divisoren, er det nok å vise at ethvert tall c som deler både a og b også deler r_n. Denne gang begynner vi ovenfra - den øverste ligningen forteller oss at $c|r_1$. Men hvis $c|b$ og $c|r_1$, så forteller den andre linjen oss at $c|r_2$. Fortsetter vi på samme måte, ser vi at $c|r_3$ osv. Til slutt får vi at $c|r_n$, og dermed har vi vist at r_n er den største felles divisoren til a og b.

Eksempel på bruk av Euklids algoritme

Finn største felles divisor til 222 og 84. Vi får

$$\begin{aligned} 222 &= 2 \cdot 84 + 54 \\ 84 &= 1 \cdot 54 + 30 \\ 54 &= 1 \cdot 30 + 24 \\ 30 &= 1 \cdot 24 + 6 \\ 24 &= 4 \cdot 6 \end{aligned}$$

som viser at største felles divisor er 6.

Vi skal skrive 6 som en lineær kombinasjon av 222 og 84.
Starter vi med den nest nederste ligningen ser vi at

$$6 = 30 - 1 \cdot 24.$$

Fra den tredje nederste ligningen ser vi at $24 = 54 - 1 \cdot 30$, og setter vi dette inn i uttrykket ovenfor, får vi

$$6 = 30 - 1 \cdot 24 = 30 - 1(54 - 1 \cdot 30) = 2 \cdot 30 - 54$$

(legg merke til at vi bare samler sammen leddene uten å gange ut).
Nå ser vi fra den nest øverste ligningen at $30 = 84 - 1 \cdot 54$, og setter vi dette inn i det siste uttrykket ovenfor, får vi

$$6 = 2 \cdot 30 - 54 = 2(84 - 1 \cdot 54) - 54 = 2 \cdot 84 - 3 \cdot 54.$$

Til slutt ser vi fra den øverste ligningen at $54 = 222 - 2 \cdot 84$, så

$$6 = 2 \cdot 84 - 3(222 - 2 \cdot 84) = 8 \cdot 84 - 3 \cdot 222$$

Dermed har vi skrevet 6 som en lineær kombinasjon av 84 og 222;

$$6 = 8 \cdot 84 + (-3) \cdot 222$$

Oppgave

En rikmann sendte sin slave til markedet for å kjøpe sauer og geiter, og sendte med ham 170 drakmer. Slaven kom tilbake med innkjøpte dyr. “Hva var prisene?” spurte rikmannen. “En sau kostet 30 drakmer og en geit 18 drakmer,” svarte slaven. “Har du noen penger igjen?” spurte rikmannen. “Nei, jeg handlet for alle sammen,” svarte slaven. “Du lyver,” sa rikmannen. Og ganske riktig, da de ransaket slaven, fant de 8 drakmer.

a) Hvordan kunne rikmannen vite at slaven løy?
b) Hvor mange sauer og hvor mange geiter hadde slaven kjøpt?