Notater til forelesning 6-9; gcd osv.

Dagens tema er *største felles divisor*.

Definisjon 0.1. La a og b være hele tall, med minst ett av dem forskjellig fra null. Da vil det bare finnes endelig mange tall som deler begge, og vi kan plukke ut det største tallet med denne egenskapen; det tallet skriver vi $d = gcd(a, b)$ (forkortet fra greatest common divisor), og vi kaller det den største felles divisoren til a og b. I symboler er definisjonen som følger: $d = gcd(a, b)$ er definert ved

a) $d|a$ og $d|b$
b) Om $c|a$ og $c|b$, vil $c \leq d$.

I det tilfellet at $gcd(a, b) = 1$ sier vi at a og b er *relativt primiske* (eller koprimiske).

Jeg minner om at symbolet | markerer delelighet, så $d|a$ leses d deler a, og betyr at brøken $\frac{a}{d}$ er et heltall. En annen måte å si det på, er å si at resten vi får når a deles på d er null. Den motsatte relasjonen, altså d deler ikke a, skriver vi $d \not| a$. Dette er et vanlig fenomen i matematisk notasjon; en skråstrek over et symbol viser negasjon. Vi skriver f.eks. $2 \in \{x|x > 0\}$ for å vise at 2 er et positivt tall, $\in$ betyr "er element i", mens $-2 \notin \{x|x > 0\}$ viser at det samme ikke holder for -2. $\notin$ betyr altså "er ikke element i".

En banal måte å beregne *gcd* på, er å skrive opp alle divisorene til a og b, og så plukke ut den største som står på begge listene. F.eks. ser vi at $gcd(35, 20) = 5$ siden divisorene til 35 er $\pm 1, \pm 5, \pm 7, \pm 35$ og divisorene til 20 er $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$. Fra nå av vil vi alltid droppe de negative divisorene, siden vi er interessert i den *største* divisoren.

Eksempler:

$$gcd(4, 6) = 2 \qquad gcd(1000, -50) = 50 \qquad gcd(-2, -3) = 1$$
$$gcd(42, 18) = 6 \qquad gcd(0, a) = |a| \qquad gcd(a, b) = gcd(b, a)$$

Det første resultatet vi trenger om *gcd* er

Teorem 0.2. *La a og b være heltall, ikke begge null (slik at gcd er definert). Da finnes hele tall x og y slik at*

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

Det står et bevis i boken (side 22), men vi venter med beviset for dette resultatet til fredag, da vi vil finne det som et korollar av Euklids algoritme.

Eksempler:

$gcd(4, 6) = 4.(-1)+6.1$, $gcd(1000, -50) = 1000.0+(-50).(-1)$, $gcd(42, 18) = 42.1+18.(-2)$

Her kommer noen resultater om *gcd*, sakset fra boken (side 23-24), mye av dette blir bevist på forelesning. Bevisene vil følge boken, som presenterer disse utsagnene på en god måte.

Teorem 0.3. *La a og b være heltall, ikke begge null, og la $d = gcd(a, b)$.*

i. *Mengden $T = \{ax+by|x, y \text{ heltall}\}$ er nøyaktig mengden av heltallige multipler av d.*
ii. *a og b er relativit primiske (altså $d = 1$) hvis og bare hvis det finnes heltall x, y slik at $1 = ax + by$.*
iii. *$gcd(\frac{a}{d}, \frac{b}{d}) = 1$*
iv. *Om $a|c$ og $b|c$, der $d = gcd(a, b) = 1$, så vil $ab|c$ (produktet deler altså c)*
v. *Om $a|bc$ og $d = gcd(a, b) = 1$, så $a|c$.*
vi. *Hvis $c|a$ og $c|b$, så vil også $c|d = gcd(a, b)$.*

Merknad 0.4. Hvis $gcd(a, b) \neq 1$ holder ikke punktene iv. og v. Med $a = b = c$ har vi $a|c$ og $b|c$ men ikke $ab|c$, så betingelsen er nødvendig i iv. Med $a = 6, b = 3, c = 4$ ser vi at betingelsen også er nødvendig i v.

Foreløpig har vi ikke noen praktiske måter å beregne *gcd* på (å skrive opp alle divisorene er ikke noen *praktisk* fremgangsmåte), men på fredag skal vi lære Euklids algoritme. Den viser hvordan vi beregner *gcd* for vilkårlige tall (uten at vi trenger å kjenne divisorene deres) på en rask og effektiv måte. Vi vil også få beviset for Teorem 0.2 gratis fra denne algoritmen.

Jon Eivind Vatne