Forelesning 11
INTRO TIL TALLTEORI

- Deling og delbarhet $a|b \Leftrightarrow b = q\cdot a,\ q\in\mathbb{Z}$
- Heltallsdivisjon $b = a\cdot q + r$

  Primtall $1|p$ og $p|p$ men $n\nmid p$ for $n \neq 1, p$
- Største felles divisor, gcd(a,b) "største heltall d.s.a $d|a$ og $d|b$"
- Diofantiske ligninger $ax + by = c$

Deling og delbarhet

Vi skal se på heltallene $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ og hva som skjer når vi deler heltall på andre heltall

Eks: $\frac{14}{2} = 7$ med rest lik 0

$\frac{15}{6} = 2$ med rest lik 3

Vi skriver $2|14$ og $6\nmid 15$

"2 deler 14" "6 deler ikke 15"

Definisjon

La a og b være heltall, $b\neq 0$. Hvis det finnes et heltall q slik at $a = q\cdot b$ sier vi at b deler a, og vi skriver $b|a$.

Vi kaller b en divisor av a og sier at a er delelig med b.

Hvis b ikke deler a skriver vi $b\nmid a$.

Eksempel

$8 \mid 32$ fordi $32 = 4 \cdot 8$ ($a = 32$, $q = 4$, $b = 8$)

$8 \nmid 33$ fordi det ikke finnes $q \in \mathbb{Z}$ s.a. $33 = q \cdot 8$

Vi merker oss følgende:

① $1 \mid a$, $a \mid a$ og $a \mid 0$ $\forall a \in \mathbb{Z} \setminus \{0\}$

② Delbarhet er transitivt:
Hvis $c \mid b$ og $b \mid a$ så vil $c \mid a$

Hvorfor?
Hvis $c \mid b$ så er $b = q \cdot c$ for en $q \in \mathbb{Z}$
Hvis $b \mid a$ så er $a = r \cdot b$ for $r \in \mathbb{Z}$
$= r(q \cdot c)$
$= (r \cdot q) \cdot c$, så $c \mid a$
($r \cdot q$: heltall)

③ Hvis $b \mid a$ og $d \mid c$ så vil $(b \cdot d) \mid (a \cdot c)$ (heltall)
$a = q \cdot b$ $\quad c = r \cdot d$, så $ac = (q \cdot b) \cdot (r \cdot d) = (q \cdot r) \cdot (b \cdot d)$

Heltallsdivisjon

Vi kan prøve å dele a på b selv om $b \nmid a$,
men da vil vi få en rest.

$\frac{a}{b}$ = kvotient + $\frac{\text{rest}}{b}$ $\longleftrightarrow$ a = (kvotient)b + rest

Definisjon

La a og b være heltall slik at $b > 0$. Dersom vi finner heltall q og r slik at $a = q \cdot b + r$ og $0 \leq r < b$, kaller vi q en kvotient og r for en rest.

Resten kalles også "a modulo b" og skrives ofte som $r = a \bmod b$

Eksempel

$15 \bmod 4 = 3$ fordi $15 = 3 \cdot 4 + 3$ ($a = 15$, $q = 3$, $b = 4$, $r = 3$) og $21 \bmod 7 = 0$ fordi $21 = 3 \cdot 7 + 0$

(Dette skrives som $15 \,\%\, 4$ i f.eks Python)
($a \,\%\, b$)

Noen tall er ekstra viktige/spesielle: primtallene

Definisjon

> Et naturlig tall $p>1$ er et primtall hvis det ikke har noen andre positive divisorer enn 1 og p.
>
> Et naturlig tall $n>1$ som ikke er primtall kalles et sammensatt tall

Så for primtall p vil $1 \mid p$ og $p \mid p$ men for alle andre $n \in \mathbb{N}, n>0$ vil $n \nmid p$

Eks: $2, 3, 5, 7, 11, 13, \ldots$

Hvor mange primtall finnes det?

Svar: uendelig mange!

Først: alle naturlige tall større enn 1 har en primtallsfaktorisering (ØFS)

Anta at det finnes k primtall $p_1, p_2, \ldots p_k$

La $q = p_1 \cdot p_2 \cdot \ldots p_k + 1$

$c = p_0 \cdot p_k$

Da vil $p_1 \nmid q$ fordi $q = c \cdot p_1 + 1$

Rest lik 1

Generelt: $p_i \nmid q$ for alle $i = 1, 2, \ldots, k$

Men! q har en primtallsfaktorisering, så q må ha en primtallsfaktor p som ikke er blant $p_1, p_2, \ldots, p_k$.

Så det kan ikke finnes bare endelig mange primtall. ■

Største felles divisor (gcd)

← "greatest common divisor"

Primtallsfaktoriseringen av 20 er $2 \cdot 2 \cdot 5$
og av 24 er $2 \cdot 2 \cdot 2 \cdot 3$

Største felles divisor av 20 og 24 er $2^2 = 4$,
og da sier vi at $\gcd(20,24) = 4$

Definisjon

La $a, b \in \mathbb{Z}$ slik at ikke begge er null.

Den største felles divisoren til a og b er tallet d som oppfyller

1. $d \mid a$ og $d \mid b$ (d deler både a og b)
2. Ethvert tall som deler både a og b er mindre enn eller lik d.

Vi skriver da $\gcd(a,b) = d$

gcd kan brukes til å forkorte brøker

$$\frac{20}{24} : \gcd(20,24) = \frac{5}{6}$$

← Garantert ferdig forkortet

Andre bruksområder: Kryptografi (om to uker)

Diofantiske ligninger

Eksempel

$36 = 6 \cdot 6 = 2 \cdot 2 \cdot 3 \cdot 3$
$60 = 6 \cdot 10 = 2 \cdot 2 \cdot 3 \cdot 5$
} $\gcd(36,60) = 2 \cdot 2 \cdot 3 = 12$

Men $24 = 2^3 \cdot 3$
$35 = 5 \cdot 7$
} Ingen felles faktorer!
Da er $\gcd(24,35) = 1$

Definisjon

Hvis $\gcd(a,b)=1$, sier vi at a og b er relativt primiske (coprime) til hverandre og vi skriver $a \perp b$

Eksempel

$24 \perp 35$ og $10 \perp 27$ ($2\cdot 5$, 3^3) men $8 \not\perp 14$ fordi $\gcd(8,14)=2 \neq 1$

Noen flere egenskaper (?) med delbarhet

① Hvis $m \mid (a \cdot b)$ vil da $m \mid a$ eller $m \mid b$?
Nei! Motseksempel: $9 \mid 180$ men $9 \nmid 12$ og $9 \nmid 15$ ($12 \cdot 15$)

② Hvis $m \mid (a \cdot b)$ og $m \perp a$, vil da $m \mid b$?
Ja!

③ Hvis $(m \cdot n) \mid a$, vil da $m \mid a$ og $n \mid a$?
Ja!

④ Hvis $m \mid a$ og $n \mid a$, vil da $(m \cdot n) \mid a$?
Nei! Motseksempel: $2 \mid 12$ og $4 \mid 12$ men $8 \nmid 12$

⑤ Hvis $m \mid a$ og $n \mid a$ og $m \perp n$, vil $(m \cdot n) \mid a$?
Ja!

Bevis for "ja"-ene er i notatene på wiki

Diofantiske ligninger

Eksempel

Prøv å finne heltall x og y slik at
$20x + 24y = 14$

Vi her at $\gcd(20,24) = 4$, så vi prøver å skrive

$$20x + 24y = 14$$
$$4(5x + 6y) = 14$$

Venstresiden er på formen $4 \cdot c$

Kan vi skrive høyresiden som $4 \cdot (noe)$?

Nei, fordi $4 \nmid 14$, så $20x + 24y = 14$ har ingen heltallsløsninger