Sidste gang:

Primtal (afsnit 4.3)

Sætning 1: (Aritmetikkens Fundamentalsætning)
Ethvert heltal $n \geq 2$ har en unik primtalsfaktorisering.

Største fælles divisor (greatest common divisor):
$$\gcd(a,b) = \max\{ d \mid d|a \wedge d|b \}$$
Mindste fælles multiplum (least common multiple)
$$\operatorname{lcm}(a,b) = \min\{ m \mid a|m \wedge b|m \}$$

Sætning 5: $a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$

Eks: $18 = \boxed{2\cdot 3}\cdot 3$ $\quad \gcd = 2\cdot 3 = 6$

$24 = \boxed{2\cdot 2}\cdot\boxed{2\cdot 3}$ $\quad \operatorname{lcm} = 2\cdot 3\cdot 3\cdot 2\cdot 2 = 72$

$18\cdot 24 = \underbrace{2\cdot 3}_{\gcd}\cdot\underbrace{3\cdot 2\cdot 2\cdot 2\cdot 3}_{\operatorname{lcm}}$

Def. 3: Lad $a,b \in \mathbb{Z}$.
Hvis $\gcd(a,b) = 1$, er a og b indbyrdes primiske

Lemma 2:

$$a \mid bc \;\wedge\; \gcd(a,b) = 1$$
$$\Downarrow$$
$$a \mid c$$

Bevisskitse:

a og b har ingen primtalsfaktorer til fælles.
D.v.s. alle a's primtalsfaktorer må findes i c. □

Nogle gange må man gerne dividere med det samme tal på begge sider:

Sætning 7: Lad $a,b,c \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$.

$$ac \equiv bc \pmod{m} \;\wedge\; \gcd(c,m) = 1$$
$$\Downarrow$$
$$a \equiv b \pmod{m}$$

D.v.s. hvis et tal c går op i både h.s. og v.s., og c er indbyrdes primisk med m, da må vi dividere med c på begge sider.

Bevis: Antag, at $\gcd(c,m) = 1$.

$$ac \equiv bc \pmod{m}$$
$$\Updownarrow$$
$$m \mid (a-b)c, \text{ ifølge Def. 4.1.1}$$
$$\Updownarrow$$
$$m \mid (a-b), \text{ ifølge Lemma 2}$$
$$\Updownarrow$$
$$a \equiv b \pmod{m}, \text{ ifølge Def. 4.1.1}$$

□

Skal det være præcis samme tal, man dividere med på begge sider? (Eller er det igen tilstrækkeligt, at de er kongruente, ligesom i Sætning 4.1.5?)

Lineære kongruenser (afsnit 4.4)

Har $ax \equiv b \pmod m$ en løsning?

Hvis $\gcd(a,m) = 1$: ja

Ellers: Måske

Eks:

- $4x \equiv 3 \pmod 5$ $\quad \gcd(4,5) = 1$

  $x = 2$ er en løsning

- $2x \equiv 3 \pmod 4$ $\quad \gcd(2,4) = 2$

  Ingen løsning:

x	1	2	3	4	...
$2x \bmod 4$	2	0	2	0	...

↖ Lige, så vi kan ikke få en ulige rest.

- $2x \equiv 2 \pmod 4$ $\quad \gcd(2,4) = 2$

  $x = 1$ er en løsning.

Bemærk:

For at løse ligningen $4x = 3$ ganger vi blot med $\frac{1}{4}$ på begge sider, fordi $\frac{1}{4}$ er multiplikativ invers til 4:

$$4x = 3 \iff \tfrac{1}{4} \cdot 4x = \tfrac{1}{4} \cdot 3 \iff x = \tfrac{3}{4}$$

Vi kan gøre det samme for kongruensen $4x \equiv 3 \pmod 5$, hvis vi kan finde en multiplikativ invers til 4 modulo 5:

$$4x \equiv 3 \pmod 5 \iff 4 \cdot 4x \equiv 4 \cdot 3 \pmod 5 \iff x = 2 \pmod 5$$

$\iff$: Sætning 7: $\Leftarrow$

Findes der altid en multiplikativ invers til a modulo m?

Hvis $\gcd(a,m)=1$: Ja, der findes præcis én i $\mathbb{Z}_m$ (Sætning 1)

Ellers: Nej (Opgave 6)

Sætning 1:

Lad $a, m \in \mathbb{Z}$, $m \geq 2$. Da gælder

$$\gcd(a,m) = 1$$

Opg. 6 $\Uparrow \Downarrow$

$$\exists!\ s \in \mathbb{Z}_m : sa \equiv 1 \pmod{m}$$

s er multiplikativ invers til a modulo m

Bevis:

Eksistens:

Kan findes v.h.a. den udvidede Euklids Alg. (afsnit 4.3)

Unik:

Opgave 5

Bemærk, at $ax \equiv b \pmod{m}$ godt kan have en løsning, selvom a ikke har en multiplikativ invers modulo m (jvf. ovenstående eks.).

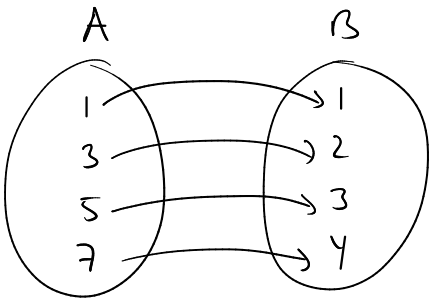
Kardinalitet af mængder (afsnit 2.5)

$|A|$: kardinaliteten af A.
Hvis A er endelig, er $|A| = \#$ elementer i A.

Def. 2.5.2:

A og B har samme kardinalitet
$\Leftrightarrow$ $\exists$ bijektion $f : A \rightarrow B$

Eks:



$|A| = |B| = 4$

Eks:

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$

$L^+ = \{2n \mid n \in \mathbb{Z}^+\} = \{2, 4, 6, \ldots\}$

$\mathbb{Z}^+$		L^+
1	$\longrightarrow$	2
2	$\longrightarrow$	4
3	$\longrightarrow$	6
4	$\longrightarrow$	8
$\vdots$		$\vdots$

$f : \mathbb{Z}^+ \rightarrow L^+$, $f(n) = 2n$ er en bijektion

Eller

Elementerne i L^+ kan stilles op i en uendelig række, som indeholder dem alle.

D.v.s.

L^+ og $\mathbb{Z}^+$ har samme kardinalitet.

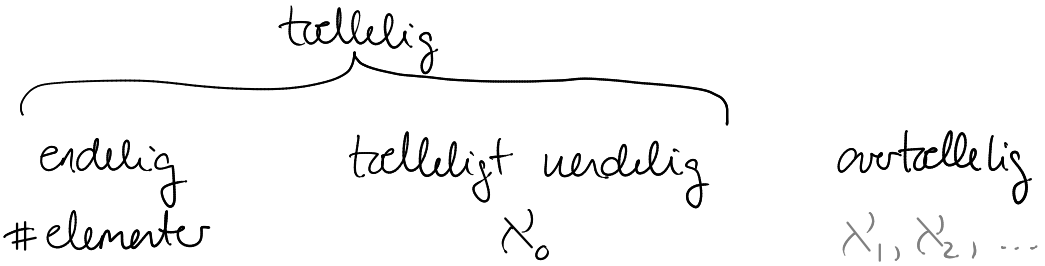
Def. 2.5.4:

Kardinaliteten af $\mathbb{Z}^+$ kaldes $\aleph_0$ (aleph 0)

En mængde, som er endelig eller har kardinalitet $\aleph_0$, kaldes tællelig.

En mængde med kardinalitet $\aleph_0$ kaldes tælleligt uendelig.

En mængde, som ikke er tællelig, kaldes overtællelig.



Eks 3: $\mathbb{Z}$ er tællelig:

$0, -1, 1, -2, 2, \ldots$

Eller

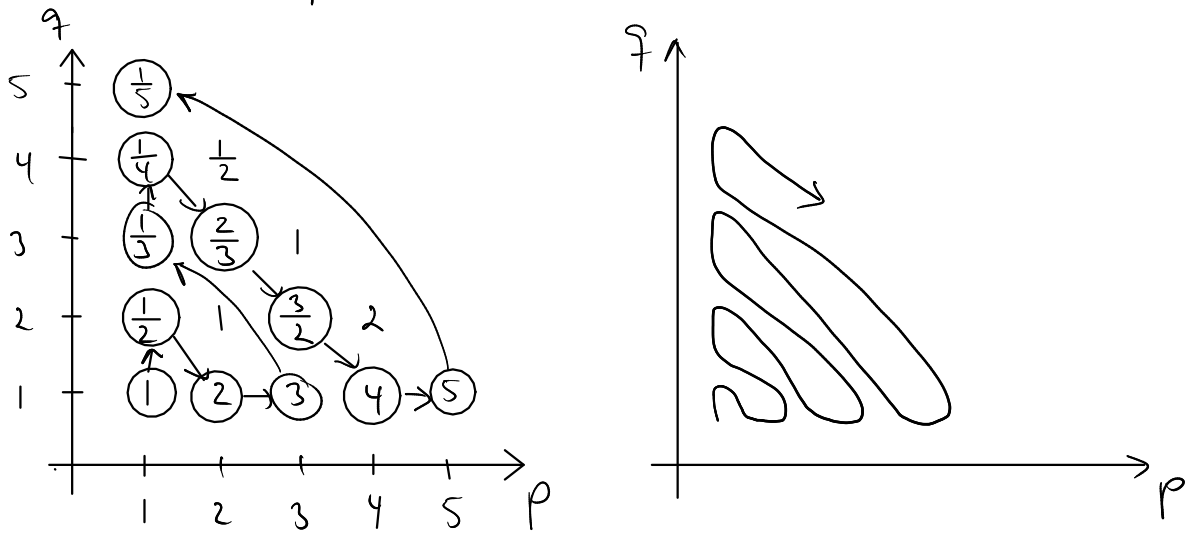
$$f: \mathbb{Z}^+ \to \mathbb{Z}, \quad f(n) = (-1)^{n-1} \left\lfloor \frac{n}{2} \right\rfloor$$

Desuden er $\mathbb{Z}$ uendelig.

D.v.s. $\mathbb{Z}$ har kardinalitet $\aleph_0$.

Eks 4: $\mathbb{Q}^+$ er tællelig:

$$\mathbb{Q}^+ = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}^+ \right\}$$



$$1, \frac{1}{2}, 2, 3, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, 4, 5, \frac{1}{5}, \frac{1}{6}, \ldots$$

Desuden er $\mathbb{Q}^+$ uendelig, da $\mathbb{Z}^+ \subseteq \mathbb{Q}^+$.
D.v.s. $\mathbb{Q}^+$ har kardinalitet $\aleph_0$.

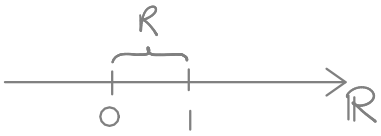
$\mathbb{Q}$ er også tællelig:

Gør det samme med $\mathbb{Q}^-$
Start med 0, og find så $\mathbb{Q}^-$ og $\mathbb{Q}^+$, som vi gjorde det med $\mathbb{Z}^-$ og $\mathbb{Z}^+$.

Eks 5: $\mathbb{R}$ er overtællelig

Diagonalisering:

Antag til modstrid, at $\mathbb{R}$ er tællelig.
Da er $R = \{ r \in \mathbb{R} \mid 0 < r < 1 \}$ tællelig.
D.v.s. elementerne i R kan opremses:



$$r_1 = 0, d_{11} d_{12} d_{13} \ldots$$
$$r_2 = 0, d_{21} d_{22} d_{23} \ldots$$
$$r_3 = 0, d_{31} d_{32} d_{33} \ldots$$
$$\vdots$$

Hvis vi ikke tillader en uendelig følge af 9-taller, kan hvert tal i R skrives på præcis én måde.

Vi kan konstruere et tal i R, som ikke er med i opremsningen:

$s = 0, d_1 d_2 d_3 \ldots$, hvor

$$d_i = \begin{cases} 5, & \text{hvis } d_{ii} = 4 \\ 4, & \text{ellers} \end{cases}$$

↯ □

Eks:
$r_1 = 0,100100\ldots$ $\quad s = 0,4445\ldots \neq r_1$
$r_2 = 0,100200\ldots$ $\quad s \neq r_2$
$r_3 = 0,100300\ldots$ $\quad s \neq r_3$
$r_4 = 0,100400\ldots$ $\quad s \neq r_4$
$\vdots$ $\quad \vdots$