

Sidste gang:

Modulær aritmetik (afsnit 4.1)

Kongruens: "modulo" (mod m) ← modulus

Def. 1 $\iff a \equiv b$

$$m \mid (a-b)$$

Sætn. 3 $\iff$

$$a \bmod m = b \bmod m$$

Sætn. 4 $\iff$

$$\exists k \in \mathbb{Z} : a = b + km$$

Sætning 5: Man må **addere** og **gange** med (og **subtrahere**) det „samme“ tal på hver side af $\equiv$.

Primtal (afsnit 4.3)

Sætning 1: (Aritmetikens Fundamentalsætning)

Enhvert heltal $n \geq 2$ har en unik primtalsfaktorisering.

Største fælles divisor (greatest common divisor):

$$\gcd(a, b) = \max \{ d \mid d \mid a \wedge d \mid b \}$$

Mindste fælles multiplum (least common multiple)

$$\text{lcm}(a, b) = \min \{ m \mid a \mid m \wedge b \mid m \}$$

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

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

$$24 = \boxed{2 \cdot 2} \cdot \boxed{2 \cdot 3}$$

$$\gcd = 2 \cdot 3 = 6$$

$$\text{lcm} = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 = 72$$

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

Def. 3: Lad $a, b \in \mathbb{Z}$.

Hvis $\gcd(a, b) = 1$, er a og b **indbyrdes primiske**

Lemma 2:

$$\Downarrow \begin{array}{l} a|bc \wedge \gcd(a,b)=1 \\ a|c \end{array}$$

Bevisstrøktse:

a og b har ingen primtalsfaktorer til fælles.

D.v.s. alle a 's primtalsfaktorer må findes i c . $\square$

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

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

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

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 $\gcd(c, m) = 1$.

$$\begin{array}{l} \Updownarrow ac \equiv bc \pmod{m} \\ \Updownarrow m | (a-b)c, \text{ ifølge Def. 4.1.1} \\ \Updownarrow m | (a-b), \text{ ifølge Lemma 2} \\ \Updownarrow a \equiv b \pmod{m}, \text{ ifølge Def. 4.1.1} \end{array} \quad \square$$

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

Lineare kongruenser (afsnit 4.4)

Har $ax \equiv b \pmod{m}$ en løsning?

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

Ellers: Måske

Eks:

• $4x \equiv 3 \pmod{5}$ $\gcd(4, 5) = 1$

$x=2$ er en løsning

• $2x \equiv 3 \pmod{4}$ $\gcd(2, 4) = 2$

Ingen løsning:

x	1	2	3	4	...
$2x \pmod{4}$	2	0	2	0	...

↖ lige ↗, så vi kan ikke få en ulige rest.

• $2x \equiv 2 \pmod{4}$ $\gcd(2, 4) = 2$

$x=1$ er en løsning.

Bemærk:

For at løse ligningen $4x \equiv 3 \pmod{5}$ ganger vi blot med $\frac{1}{4}$ på begge sider, fordi $\frac{1}{4}$ er multiplikativt invers til 4:

$$4x \equiv 3 \pmod{5} \Leftrightarrow \frac{1}{4} \cdot 4x = \frac{1}{4} \cdot 3 \pmod{5} \Leftrightarrow x \equiv \frac{3}{4} \pmod{5}$$

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

$$4x \equiv 3 \pmod{5} \Leftrightarrow 4 \cdot 4x \equiv 4 \cdot 3 \pmod{5} \Leftrightarrow x \equiv 2 \pmod{5}$$

↑
Sætning 7:
⇐

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

$$\begin{array}{c} \text{Opg. 6} \\ \uparrow \downarrow \end{array} \quad \begin{array}{l} \gcd(a, m) = 1 \\ \exists! s \in \mathbb{Z}_m : sa \equiv 1 \pmod{m} \end{array}$$

s er multiplikativ invers til a modulo m

Bevis:

Eksistens:

Kan findes v.h.s. 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 (jof. ovenstående eks.).

Kardinalitet af mængder (afsnit 2.5)

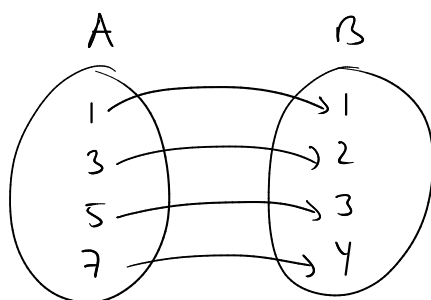
$|A|$: kardinaliteten af A .

Hvis A er endelig, er $|A| = \# \text{ elementer i } A$.

Def. 2.5.2:

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

Eks:



$$|A| = |B| = 4$$

Eks:

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

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

$$\mathbb{Z}^+ \quad \mathbb{L}^+$$

$$1 \longrightarrow 2$$

$$2 \longrightarrow 4$$

$$3 \longrightarrow 6$$

$$4 \longrightarrow 8$$

$$\vdots \quad \quad \quad \vdots$$

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

er en bijektion

Eller

Elementerne i $\mathbb{L}^+$ kan stilles op i en uendelig række, som indeholder dem alle.

D.v.s.

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

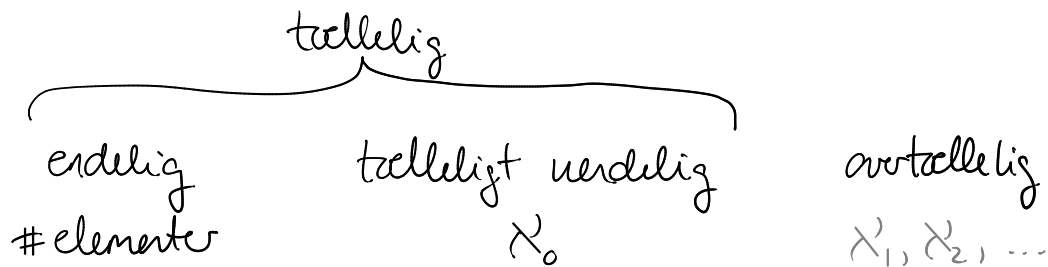
Def. 2.5.4:

Kardinaliteten af $\mathbb{Z}^+$ kaldes $\aleph_0$ (alef 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 avtællelig.



Eks 3: $\mathbb{Z}$ er tællelig:

0, -1, 1, -2, 2, ...

Eller

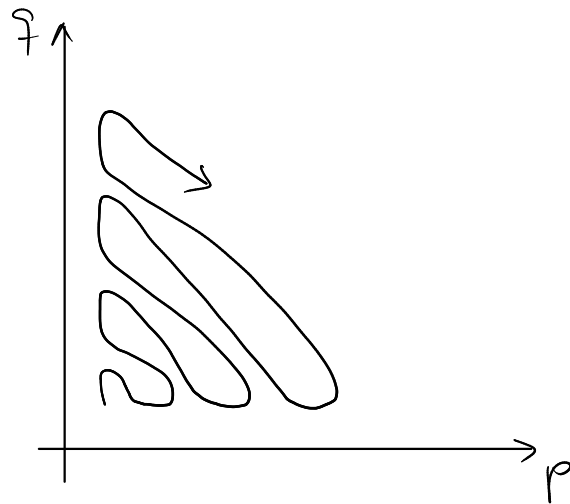
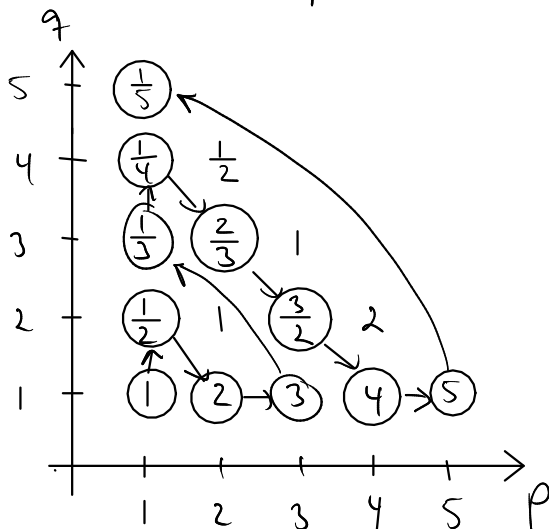
$$f: \mathbb{Z}^+ \rightarrow \mathbb{Z}, \quad f(n) = (-1)^{n-1} \left\lfloor \frac{n}{2} \right\rfloor$$

Desuden er $\mathbb{Z}$ uendelig.

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

Eks 4: $\mathbb{Q}^+$ er tællelig:

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



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

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 flet så $\mathbb{Q}^-$ og $\mathbb{Q}^+$, som vi gjorde
det med $\mathbb{Z}^-$ og $\mathbb{Z}^+$.

Eks 5: $\mathbb{R}$ er overtællig

Diagonalisering:

Antag til modstrid, at $\mathbb{R}$ er tællig.

Da er $R = \{r \in \mathbb{R} \mid 0 < r < 1\}$ tællig.

D.v.s. elementerne i R kan opremses:



$$r_1 = 0, d_{11}d_{12}d_{13}\dots$$

$$r_2 = 0, d_{21}d_{22}d_{23}\dots$$

$$r_3 = 0, d_{31}d_{32}d_{33}\dots$$

$\vdots$

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:

$$s = 0, d_1d_2d_3\dots, \text{ hvor}$$

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



Eks: $r_1 = 0, 100100\dots$

$$r_2 = 0, 100200\dots$$

$$r_3 = 0, 100300\dots$$

$$r_4 = 0, 100400\dots$$

$\vdots$

$$s = 0, 4445\dots \neq r_1$$

$$s \neq r_2$$

$$s \neq r_3$$

$$s \neq r_4$$

$\vdots$