

Sidste gang:

Primtal

Lad $n \in \mathbb{Z}$, $n \geq 2$

Hvis 1 og p er de eneste tal, der går op i n ,
er n et **primtal**.

Ellers er n et **sammensat** tal.

Øvelse 4.3.1 (Aritmetikkens Fundamentalsætning)

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

Eks: $2 = 2$ $15 = 3 \cdot 5$ $84 = 2 \cdot 2 \cdot 3 \cdot 7$

Største fælles divisor: $\gcd(a, b) = \max\{d \mid d \mid a \wedge d \mid b\}$
Mindste fælles multiplum: $\text{lcm}(a, b) = \min\{m \mid a \mid m \wedge b \mid m\}$

Eks:

$$\gcd(18, 24) = 6$$

$$18 = 2 \cdot 3 \cdot 3$$

$$24 = 2 \cdot 2 \cdot 2 \cdot 3$$

$$\gcd(12, 25) = 1 \Rightarrow 12 \text{ og } 25 \text{ er indbyrdes primiske}$$

$$\text{lcm}(18, 24) = 72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$$

$$18 = 2 \cdot 3 \cdot 3$$

$$24 = 2 \cdot 2 \cdot 2 \cdot 3$$

Bemærk:

$$\begin{aligned} \Leftrightarrow \text{lcm}(a,b) &= \text{gcd}(a,b) \cdot \frac{a}{\text{gcd}(a,b)} \cdot \frac{b}{\text{gcd}(a,b)} \\ a \cdot b &= \text{gcd}(a,b) \cdot \text{lcm}(a,b) \end{aligned}$$

1 dag:

Kongruenser (afsnit 4.3)

Kardinalitet af mængder (afsnit 2.5)

Først skal vi identificere nogle situationer, hvor man gerne må dividere på begge sider af $\equiv$.
(Vi så sidste gang, at man ikke altid må:
 $35 \equiv 55 \pmod{10}$, men $7 \not\equiv 11 \pmod{10}$)

Lemma 4.3.2

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

Bevisskitse:

a og b har ingen primtalsfaktorer til fælles.

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

Eks:

$$4 \mid 9 \cdot 12 \Rightarrow 4 \mid 12, \text{ da } \gcd(4,9)=1$$

$$4 \mid 2 \cdot 18 \not\Rightarrow 4 \mid 18$$

$$4 \mid 2 \cdot 20 \Rightarrow 4 \mid 20, \text{ selvom } \gcd(4,2)=2$$

Sætning 4.3.7

Hvis $a, b, c \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$, gælder

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

D.v.s. hvis c går op i både venstreside og højreside og ikke har nogen primtalsfaktorer til fælles med modulus, må man dividere med c på begge sider.

Beweis:

Lad $a, b, c \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ og antag, at $\gcd(c, m) = 1$.

$$\begin{aligned} & ac \equiv bc \pmod{m} \\ \Updownarrow & \\ & m \mid (ac - bc), \text{ ifølge Def 4.1.3} \\ \Updownarrow & \\ & m \mid (a-b)c \\ \Updownarrow & \\ & m \mid (a-b), \text{ ifølge Lemma 4.3.2, da } \gcd(c, m) = 1 \\ \Updownarrow & \\ & a \equiv b \pmod{m}, \text{ ifølge Def. 4.1.3} \end{aligned}$$

□

Eks:

$$\begin{aligned} & 25 \equiv 55 \pmod{6} \\ \Downarrow & \\ & 5 \equiv 11 \pmod{6}, \text{ da } \gcd(5, 6) = 1 \end{aligned}$$

Kardinalitet af mængder

(afsnit 2.5)

$|A|$: kardinaliteten af A
elementer i A , hvis A er endelig

Eks:

$$|\{2, 4, 6, 8\}| = 4 = |\{a, b, c, d\}|$$

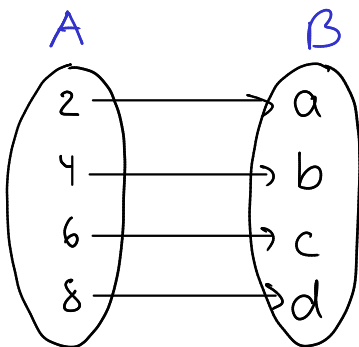
$$|\{2n \mid n \in \mathbb{Z}^+\}| = ?$$

$$|\mathbb{Z}^+| = ?$$

Def 2.5.1

$$\begin{aligned} &|A| = |B| \\ \Leftrightarrow &\exists \text{ bijektion } f: A \rightarrow B \end{aligned}$$

Eks:



$$\begin{array}{ccc} \mathbb{Z}^+ & & \mathbb{L}^+ \\ 1 & \longrightarrow & 2 \\ 2 & \longrightarrow & 4 \\ 3 & \longrightarrow & 6 \\ 4 & \longrightarrow & 8 \\ 5 & \longrightarrow & 10 \\ \vdots & & \vdots \end{array}$$

$f: \mathbb{Z}^+ \rightarrow \mathbb{L}^+$
 $f(n) = 2n$
er en bijektion
D.v.s.
 $|\mathbb{Z}^+| = |\mathbb{L}^+|$

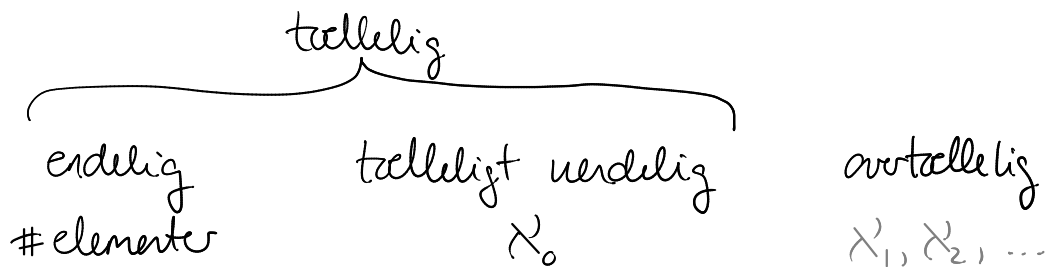
Def. 2.5.3

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 uvællelig.



Eks 3: $\mathbb{Z}$ er tællelig:

$0, -1, 1, -2, 2, \dots$

Eller

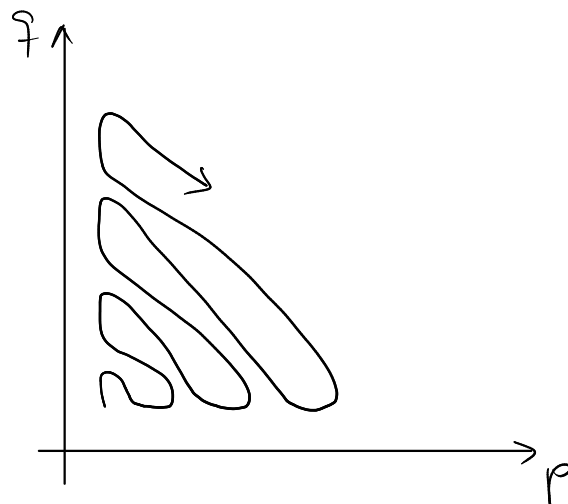
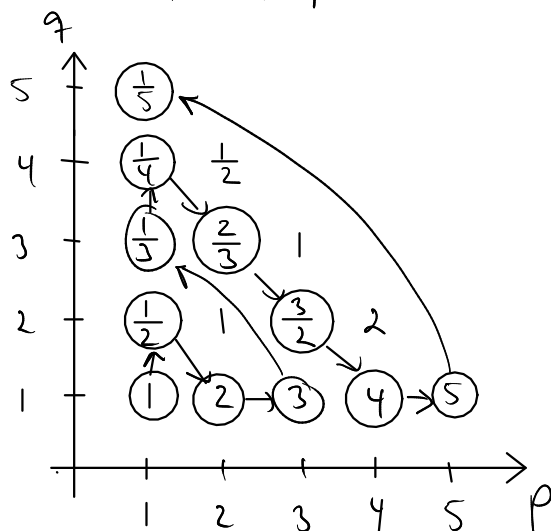
$$f: \mathbb{Z}^+ \rightarrow \mathbb{Z}, \quad f(n) = (-1)^{n-1} \left\lfloor \frac{n}{2} \right\rfloor$$

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 overtællelig

Diagonalisering:

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

Da er $R = \{r \in \mathbb{R} \mid 0 < r < 1\}$ **tællelig** (opgave 16)



Lad R_{01} bestå af de tal i R , hvis decimaler er udelukkende 0'er og/eller 1-taller.

D.v.s. $R_{01} = \{0,1, 0,01, 0,11, 0,001, \dots\}$

R_{01} er også tællelig, da $R_{01} \subseteq R$.

D.v.s. elementene i R_{01} kan opremses:

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

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

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

$\vdots$

Men uanset, hvilken rækkefølge vi remser tallene op i, kan man altid **konstruere et tal s , som ikke har en plads i opremsningen**:

$$s = 0, d_1 d_2 d_3 \dots, \text{ hvor}$$

$$d_i = \begin{cases} 0, & \text{hvis } d_{ii} = 1 \\ 1, & \text{ellers} \end{cases}$$



□

Eks:

$$r_1 = 0,100000\dots \neq S$$

$$r_2 = 0,010000\dots \neq S$$

$$r_3 = 0,110000\dots \neq S$$

$$r_4 = 0,001000\dots \neq S$$

$$r_5 = 0,011000\dots \neq S$$

$\vdots$

$$S = 0,00111\dots$$