

Sidste gang

$$0 \leq r \leq d-1$$

$$a = d \underset{\substack{\uparrow \\ a \text{ div } d \\ \text{kvotient}}}{q} + \underset{\substack{\uparrow \\ a \bmod d \\ \text{rest}}}{r}$$

(Def. 4.1.2)

Eks:

$$23 \text{ div } 5 = 4$$

$$23 \bmod 5 = 3$$

$$-23 \bmod 5 = -5$$

$$-23 \bmod 5 = 2$$

$$\begin{array}{lcl}
 \text{Def. 4.1.3} & \Updownarrow & a \equiv b \pmod{m} \\
 \text{Sætn. 4.1.3} & \Updownarrow & m \mid (a-b) \\
 \text{Sætn. 4.1.4} & \Updownarrow & a \bmod m = b \bmod m \\
 & \Updownarrow & a = b + km, \quad k \in \mathbb{Z}
 \end{array}$$

Eks:

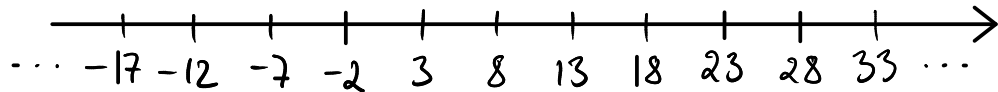
$$23 \equiv 8 \pmod{5}$$

$$5 \mid (23-8)$$

$$23 \bmod 5 = 8 \bmod 5$$

$$23 = 8 + 3 \cdot 5$$

8 og 23 er også kongruente med en masse andre tal:



Eks på Sætning 4.1.5:

Man må lægge det „samme“ tal til på begge sider:

$$\Downarrow \quad 23 \equiv 8 \pmod{5}$$

$$23 + 7 \equiv 8 + 27 \pmod{5}, \text{ da } 7 \equiv 27 \pmod{5}$$

$$\Updownarrow \quad 30 \equiv 35 \pmod{5}$$

Man må gange med det „samme“ tal på begge sider:

$$\Downarrow \quad 23 \equiv 8 \pmod{5}$$

$$23 \cdot 7 \equiv 8 \cdot 27 \pmod{5} \quad \text{—————} \text{—————}$$

$$\Updownarrow \quad 161 \equiv 216 \pmod{5}$$

Eks på Korollar 4.1.2:

$$(23 + 14) \bmod 5 = (3 + 4) \bmod 5 = 2$$

$$23 \cdot 14 \bmod 5 = 3 \cdot 4 \bmod 5 = 2$$

Def. 4.3.1:

Ethvert $p \in \{2, 3, 4, \dots\}$ er enten

- et primtal (hvis ingen andre tal end 1 og p går op i p) eller
- sammensat.

Aritmetikens Fundamentalsætning (Sætning 4.3.1):

Ethvert $n \in \{2, 3, 4, \dots\}$ kan skrives som et produkt af primtal på præcis en måde.

Eks: $2=2$, $3=3$, $4=2 \cdot 2$, $5=5$, $6=2 \cdot 3$, $7=7$
 $9=3 \cdot 3$, $10=2 \cdot 5$, $11=11$, $12=2 \cdot 2 \cdot 3$, ...

Eks: Største fælles divisor (Def. 4.3.2)

$$\gcd(18, 24) = 6 = 2 \cdot 3$$

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

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

Mindste fælles multiplum (Def. 4.3.5)

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

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

(Sætning 4.3.5)

1 dag

- Afslutning af primtal (Afsnit 4.3)
(hvornår må man dividere på begge sider?)
- Kardinalitet (Afsnit 2.5)

Eks:

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

$$12 = 2 \cdot 2 \cdot 3$$

$$25 = 5 \cdot 5$$

Ingen primtalsfaktorer til fælles

Def. 4.3.3

indbyrdes primiske
(relatively prime)

Lemma 4.3.2

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

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.

Bevis:

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

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

Da gælder:

$$\Updownarrow \quad ac \equiv bc \pmod{m}$$

$$\Updownarrow \quad m \mid (ac - bc), \quad \text{ifølge Def 4.1.3}$$

$$\Updownarrow \quad m \mid (a-b)c$$

$$\Updownarrow \quad m \mid (a-b), \quad \text{ifølge Lemma 4.3.2, da } \gcd(c, m) = 1$$

$$\Updownarrow \quad a \equiv b \pmod{m}, \quad \text{ifølge Def. 4.1.3}$$

□

Eks:

$$\Downarrow \begin{array}{l} 9 \equiv 45 \pmod{4} \\ 1 \equiv 5 \pmod{4}, \text{ da } \gcd(9, 4) = 1 \end{array}$$

$$\begin{array}{l} 8 \equiv 20 \pmod{4}, \text{ men} \\ 4 \not\equiv 10 \pmod{4} \end{array}$$

$$\begin{array}{l} 12 \equiv 20 \pmod{4}, \text{ og} \\ 6 \equiv 10 \pmod{4}, \text{ selvom } \gcd(2, 4) = 2 \end{array}$$

Kardinalitet af mængder

(afsnit 2.5)

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

Eks:

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

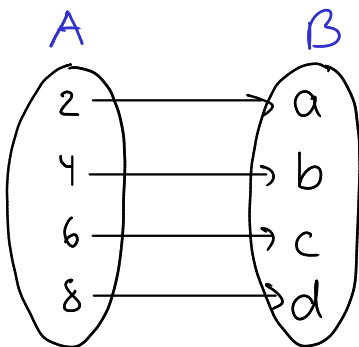
$$|\{2n \mid n \in \mathbb{Z}^+\}| = ?$$

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

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.
 $|\mathbb{Z}^+| = |\mathbb{L}^+|$

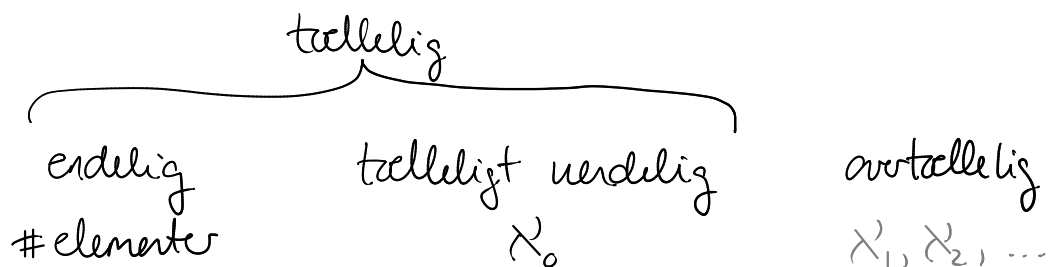
Def. 2.5.3

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 ovrtællelig.



Eks 3: $\mathbb{Z}$ har samme kardinalitet som $\mathbb{Z}^+$:

$0, -1, 1, -2, 2, -3, 3, \dots$ (uendelig opremsning af $\mathbb{Z}$)

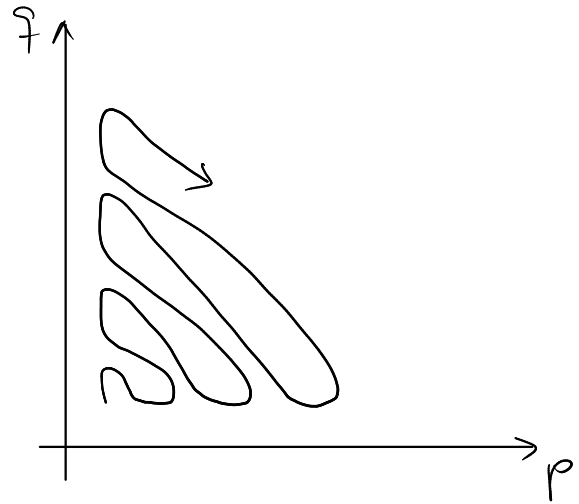
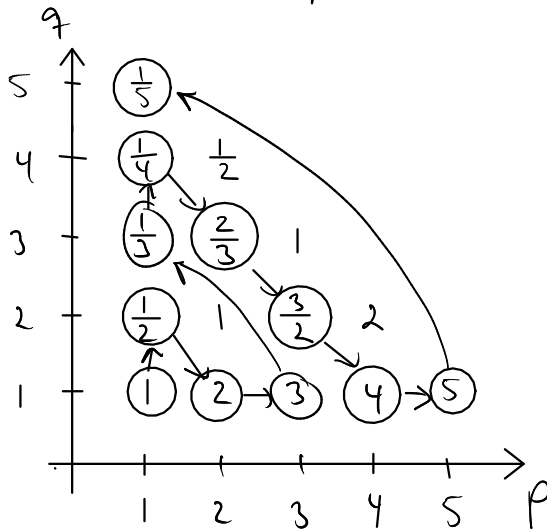
Eller:

$f: \mathbb{Z}^+ \rightarrow \mathbb{Z}, f(n) = (-1)^{n-1} \lfloor \frac{n}{2} \rfloor$
(bijektion mellem $\mathbb{Z}^+$ og $\mathbb{Z}$)

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

Eks: $\mathbb{Q}^+$ er også tællelig:

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



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

$\mathbb{Q}$ 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** (opgave 16)



Lad R_0 bestå af de tal i R , hvis decimaler er udelukkende 0'er og/eller 1-taller.

D.v.s. $R_0 = \{0,1, 0,01, 0,11, 0,001, \dots\}$

R_0 er også tællig, da $R_0 \subseteq R$.

D.v.s. elementene i R_0 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:

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

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

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

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

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

$\vdots$

$$S = 0,00111\dots$$