

Printal, største fælles divisor og mindste fælles mult. (Afsnit 4.3)

Def. 4.3.1 :

Lad $p \in \mathbb{Z}^+ - \{1\}$.

Hvis 1 og p er de eneste tal, der går op i p ,
er p et printal.

Ellers er p sammensat.

Eks :

Printal : 2, 3, 5, 7, 11, ...

Sammensat : 4, 6, 8, 9, 10, ...

Sætning 4.3.1 (Aritmetikens Fundamentalsætning) :

Enhvert heltal $n \geq 2$

kan skrives som et produkt af printal,
og det kan kun gøres på én måde (hvis man
sorterer faktorerne efter størrelse).

Bevis :

- Eksisterer : afsnit 5.2 (Eks. 2)
- Unik : sidst i afsnit 4.3

Eks :

$$2 = 2$$

$$3 = 3$$

$$4 = 2 \cdot 2$$

$$10 = 2 \cdot 5$$

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

$$45 = 3 \cdot 3 \cdot 5$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5$$

Største fælles divisor og mindste fælles multiplum
(kender datalogene fra DM539, inkl. Euklids Alg.):

Def 4.3.2:

Lad $a, b \in \mathbb{Z}$, $a \neq 0 \vee b \neq 0$.

$\gcd(a, b) = \max \{ d \mid d \mid a \wedge d \mid b \}$ kaldes
største fælles divisor for a og b

Ek:

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

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

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

$$\gcd(12, 24) = 12$$

$$12 = \boxed{2 \cdot 2 \cdot 3}$$

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

$$\gcd(12, 25) = 1 \Rightarrow 12 \text{ og } 25 \text{ er } \underline{\text{indbyrdes primiske}} \\ (\text{Def 4.3.3})$$

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

$$25 = 5 \cdot 5$$

Def. 4.3.5:

Lad $a, b \in \mathbb{Z}^+$.

$\text{lcm}(a, b) = \min \{ m \mid a \mid m \wedge b \mid m \}$ kaldes
mindste fælles multiplum af a og b

Eks:

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

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

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

$$\text{lcm}(12, 24) = 24$$

$$12 = \boxed{2 \cdot 2 \cdot 3}$$

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

$$\text{lcm}(12, 25) = 300 = 12 \cdot 25$$

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

$$25 = 5 \cdot 5$$

Sætning 4.3.5:

Lad $a, b \in \mathbb{Z}^+$. Da gælder

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

Afsnit 4.4:

Lineære

kongruenser og
kongruenssystemer

~

ligninger og
ligningssystemer

Lineære kongruenser

$$ax \equiv b \pmod{m}$$

Løsning ?

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

Ja

Ellers :

Måske

Eks:

$$\underline{4}x \equiv 3 \pmod{\underline{5}}$$

$x=2$ er en løsning

$$\underline{2}x \equiv 3 \pmod{\underline{4}}$$

Ingen løsning

$$\underline{2}x \equiv 2 \pmod{\underline{4}}$$

$x=1$ er en løsning

Sætning 4.4.1:

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

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

$$\Downarrow \exists! s \in \mathbb{Z}_m = \{0, 1, \dots, m-1\} : sa \equiv 1 \pmod{m}$$

s er multiplikativ invers til a modulo m

Basis:

Eksistens:

Kan findes v.h.a. den udvidede Euklids Alg.

Unik:

Opgave 4.4.5

Og hvad har det så med lineære kongruenser at gøre?

$$ax \equiv b \pmod{m}$$

$$\gcd(a, m) = 1 \Rightarrow \exists s \in \mathbb{Z} : as \equiv 1 \pmod{m}$$

$$\Rightarrow \exists s \in \mathbb{Z} : \underbrace{as}_{x} b \equiv b \pmod{m}$$

D.v.s. $x = sb$ er en løsning til $ax \equiv b \pmod{m}$

Så påstanden, at kongruensen har en løsning, hvis $\gcd(a, m) = 1$, var korrekt.

Kardinalitet af mængder (afsnit 2.5)

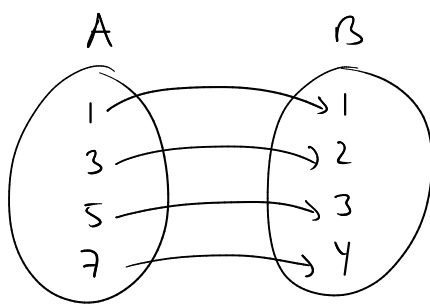
$|A|$: kardinaliteten af A .

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:

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

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

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

$$1 \longrightarrow 2$$

$$2 \longrightarrow 4$$

$$3 \longrightarrow 6$$

$$4 \longrightarrow 8$$

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

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

er en bijektion

Eller

Elementerne i A kan stilles op i en uendelig række, som indeholder dem alle.

D.v.s.

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

Def. 2.5.4:

Kardinaliteten af $\mathbb{N}^+$ kaldes $\aleph_0$ (alef 0)

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

En mængde, som ikke er tællelig, kaldes avortællelig.

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

Eks 3: $\mathbb{Z}$ er tællelig

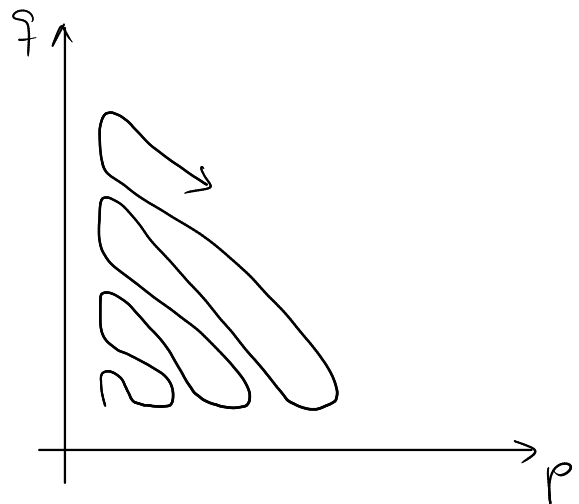
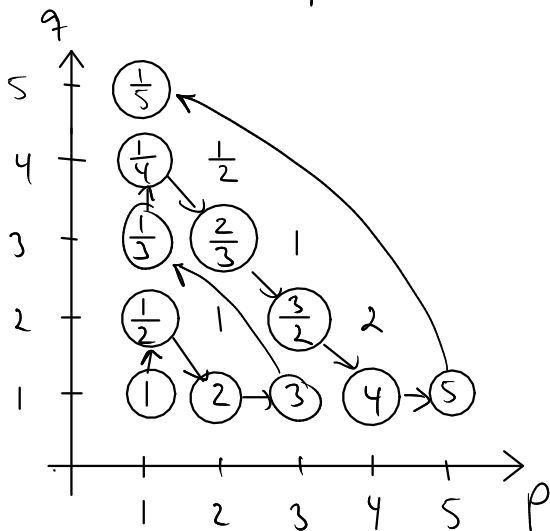
$0, -1, 1, -2, 2, \dots$

Eller

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

Eks 4: $\mathbb{Q}^+$ er tællelig

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



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

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 uædtællelig

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:

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

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

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

$\vdots$

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:

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

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

⚡ $\square$

Eks: $r_1 = 0, 410 \dots$

$$r_2 = 0, 420 \dots$$

$$r_3 = 0, 430 \dots$$

$$0, 544 \dots$$