

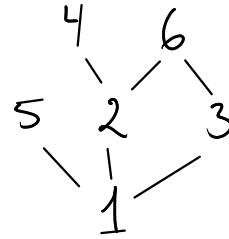
Sidste gang:

Partiel ordning:

Relation, som er reflektiv, antisymmetrisk og transitiv

Eks: $A = \{1, 2, 3, 4, 5, 6\}$
 $R = \{(a, b) \in A \times A \mid a \mid b\}$

Hasse-diagram for R :



$$S = \{(a, b) \in A \times A \mid a \leq b\}$$

Hasse diagram for S :



S er en total ordning, da
 $\forall a, b \in A: a \leq b \vee b \leq a$

R er ikke en total ordning, da f.eks.
 $3 \nmid 5 \wedge 5 \nmid 3$ (3 og 5 er ikke sammenlignelige)

Talteori

Delbarhed

$$a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z} : b = ka$$

a går op i b

a er en faktor i b

b er et multiplum af a

Sætning 4.1.1:

$$(i) a|b \wedge a|c \Rightarrow a|(b+c)$$

$$(ii) a|b \Rightarrow \forall k \in \mathbb{Z} : a|kb$$

$$(iii) a|b \wedge b|c \Rightarrow a|c$$

Af Sætning 4.1.1 (i)+(ii) følger:

Korollar 4.1.1:

$$a|b \wedge a|c \Rightarrow \forall k, l \in \mathbb{Z} : a|(kb+lc)$$

Sætning 4.1.2:

For $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ gælder

$$\exists! q, r \in \mathbb{Z} : (a = d \cdot q + r \wedge 0 \leq r < d)$$

$$q = a \operatorname{div} d = \left\lfloor \frac{a}{d} \right\rfloor$$

$$r = a \bmod d = a - dq = a - d \left\lfloor \frac{a}{d} \right\rfloor$$

„ a modulo d “

Eks: $16 = 3 \cdot 5 + 1$

$$16 \text{ div } 3 = 5 = \lfloor \frac{16}{3} \rfloor$$

$$16 \bmod 3 = 1 = 16 - 3 \cdot 5$$

$$-16 = 3 \cdot (-6) + 2$$

$$-16 \text{ div } 3 = -6 = \lfloor \frac{-16}{3} \rfloor$$

$$-16 \bmod 3 = 2 = -16 - 3 \cdot (-6)$$

Kongruens

a er kongruent med b modulo m

$$\Leftrightarrow a \equiv b \pmod{m}$$

Def. 1 $\Leftrightarrow m \mid (a-b)$

Sætning 3 $\Leftrightarrow a \bmod m = b \bmod m$

Sætning 4 $\Leftrightarrow \exists k \in \mathbb{Z}: a = b + km$

$a \equiv b \pmod{m}$ kaldes en kongruens
 $\uparrow$
 modulus

Eks: $7 \equiv 16 \pmod{3}$, da $3 \mid (16-7)$
 (og $7 \bmod 3 = 1 = 16 \bmod 3$
 og $7 = 16 + (-3) \cdot 3$)

$11 \equiv 11 \pmod{4}$, da $4 \mid 0$
 (og $11 \bmod 4 = 11 \bmod 4$
 og $11 = 11 + 0 \cdot 4$)

Ætning 4.1.5:

Hvis $c \equiv d \pmod{m}$, gælder:

$$a \equiv b \pmod{m} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases}$$

Gælder der også, at $a-c \equiv b-d \pmod{m}$?
 $a/c \equiv b/d \pmod{m}$?

Man må gerne **subtrahere** det "samme" tal på begge sider, for det er det samme som at addere:
 $c \equiv d \pmod{m} \Leftrightarrow -c \equiv -d \pmod{m}$

Man kan ikke altid **dividere** med det samme tal på begge sider (selvom divisionen går op):

$$20 \equiv 30 \pmod{5}, \text{ men}$$

$$4 \not\equiv 6 \pmod{5}$$

Nedenstående resultat kan spare os for at regne med meget store tal:

Korollar 4.1.2:

For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

- $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
- $a \cdot b = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

Beweis:

$$\begin{cases} a \equiv a \bmod m \pmod{m}, & \text{ifølge Sætning 4.1.3} \\ b \equiv b \bmod m \pmod{m}, & \text{ifølge Sætning 4.1.3} \end{cases}$$

$\Downarrow$

$$a+b \equiv (a \bmod m) + (b \bmod m) \pmod{m},$$

ifølge Sætning 4.1.5

$\Uparrow$

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m,$$

ifølge Sætning 4.1.3

Tilsvarende fås:

$$\begin{aligned} \Uparrow \quad ab &\equiv (a \bmod m)(b \bmod m) \pmod{m}, && \text{ifølge Sætning 4.1.5} \\ \Uparrow \quad ab \bmod m &= ((a \bmod m)(b \bmod m)) \bmod m, && \text{ifølge Sætning 4.1.3} \end{aligned}$$

□

D.v.s. man kan nøjes med at regne med tallene i

$$\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$$

Printal (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, 13, 17

Sammensat: 4, 6, 8, 9, 10, 12, 14, 15, 16

Sætning 4.3.1 (Aritmetikkens Fundamentalsætning)

Enhvert heltal $n \geq 2$

kan skrives som et produkt af printal
på præcis én måde

(hvis man sorterer faktorerne efter størrelse)

Eks:

$$2 = 2$$

$$10 = 2 \cdot 5$$

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

$$3 = 3$$

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

$$4 = 2 \cdot 2$$

$$30 = 2 \cdot 3 \cdot 5$$

Def. 4.3.2

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

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

kaldes *største fælles divisor* for a og b

(greatest common divisor)

Eks:

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

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

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

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

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

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

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

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

$$25 = 5 \cdot 5$$

Def. 4.3.3
(relatively prime)

Def. 4.3.5

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

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

kaldes *mindste fælles multiplum* af a og b

Eks:

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

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

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

$$\text{lcm}(12, 24) = 24 = 2 \cdot \boxed{2 \cdot 2 \cdot 3}$$

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

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

$$\text{lcm}(12, 25) = 300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$$

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

$$25 = 5 \cdot 5$$

Sætning 4.3.5

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

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