

Foreløbig eksamensplan tilgængelig.
Endelig plan senest 28/10.

Sidste gang

Rotationer

Sætning 9.5.2:

Ækv. rel $\rightarrow$ partitionering

Partitionering $\rightarrow$ ækv. rel.

Partiel ordning

Partielt ordnet mængde

Hasse-diagram

Sammenlignelig

Total ordning

Leksikografisk ordning

Talteori (division)

Def. 4.1.1:

$$a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z} \Leftrightarrow b = k \cdot a, k \in \mathbb{Z}$$

Sætning 4.1.1:

(i) ...

(ii) ...

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

Korollar 4.1.1:

$$\left. \begin{array}{l} (i) \dots \\ (ii) \dots \end{array} \right\} \Rightarrow \left(\begin{array}{l} a|b \wedge a|c \Rightarrow \\ \forall n, m \in \mathbb{Z}: a|(bn+cm) \end{array} \right)$$

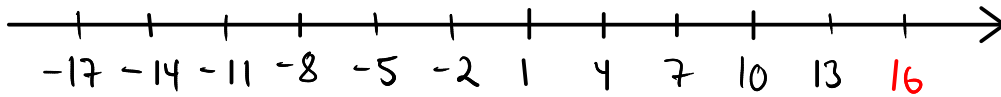
Hvis en division ikke går op, bliver der en rest:

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

Der bliver en rest på 1, når man dividerer 16 med 3.

$$16 \text{ div } 3 = 5$$

$$16 \bmod 3 = 1$$



Sætning 4.1.2 (Divisionsalgoritmen):

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

$$\exists! q, r : (a = d \cdot q + r \wedge 0 \leq r < d)$$

dividend

divisor

køotient

rest

Def. 4.1.2

$$q = a \text{ div } d$$

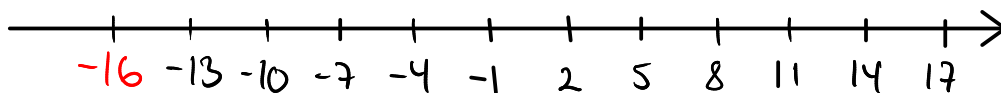
$$r = a \bmod d \quad \text{„a modulo d“}$$

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

Der bliver en rest på 2, når man dividerer -16 med 3.

$$-16 \text{ div } 3 = -6$$

$$-16 \bmod 3 = 2$$



Modulær aritmetik

Def 4.1.3

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

» a og b er
kongruente modulo m"
(*)

$\Leftrightarrow$

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

Sætning 4.1.3

$\Leftrightarrow$

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

Sætning 4.1.4

$\Leftrightarrow$

$$\exists k \in \mathbb{Z} : a = b + km \quad (**)$$

Eks:

$$16 \equiv 7 \pmod{3}, \text{ da } 3 \mid 9$$

$$-16 \not\equiv 16 \pmod{3}, \text{ da } 3 \nmid 32$$

$$4 \equiv 4 \pmod{10}, \text{ da } 10 \mid 0$$

Bevis for Sætning 4.1.3: Opgave 21-22

Bevis for Sætning 4.1.4:

(**) er en simpel omskrivning af (*):

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

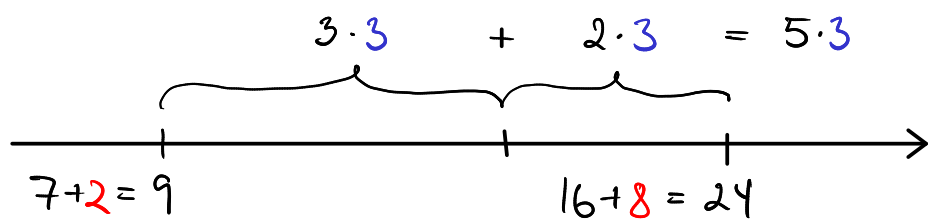
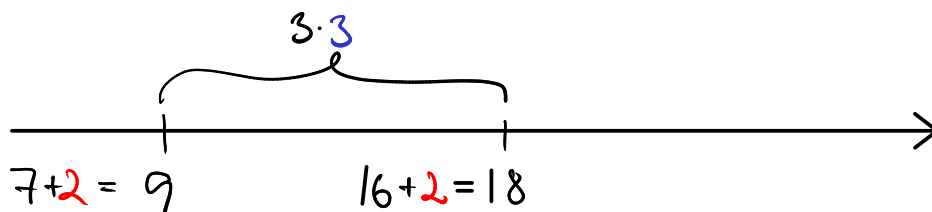
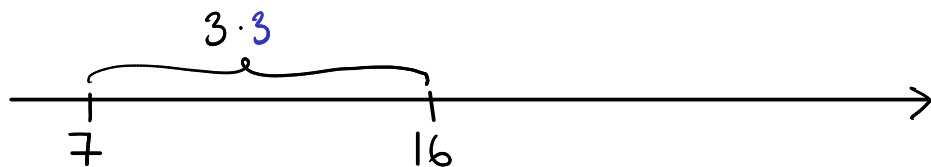
$$\Leftrightarrow a-b = km, \quad k \in \mathbb{Z}, \quad \text{ifølge Def. 4.1.3}$$

$$\Leftrightarrow a = b + km, \quad k \in \mathbb{Z}$$

□

Eks:

$$\begin{aligned} & 16 \equiv 7 \pmod{3}, \text{ da } 3 \mid (16-7) \\ \Downarrow & 16+2 \equiv 7+2 \pmod{3}, \text{ da } (16+2)-(7+2) = 16-7 \\ \Downarrow & 16+8 \equiv 7+2 \pmod{3}, \text{ da } (16+8)-(7+2) = 16-7+2 \cdot 3 \end{aligned}$$



OK at addere 2 på den ene side og 8 på den anden side, fordi $2 \equiv 8 \pmod{3}$

Eks:

$$\begin{aligned} & 16 \equiv 7 \pmod{3}, \text{ da } 3 \mid (16-7) \\ \Downarrow & 16 \cdot 2 \equiv 7 \cdot 2 \pmod{3}, \text{ da } 16 \cdot 2 - 7 \cdot 2 = (16-7) \cdot 2 \\ \Downarrow & 16 \cdot 2 \equiv 7 \cdot 8 \pmod{3}, \text{ da } 16 \cdot 2 - 7 \cdot 8 = (16-7) \cdot 2 - 7 \cdot 6 \\ & \quad \quad \quad = (16-7) \cdot 2 - 7 \cdot 2 \cdot 3 \end{aligned}$$

OK at gange med 2 på den ene side og med 8 på den anden side, da $2 \equiv 8 \pmod{3}$.

For = må man addere og multiplicere med det samme tal på begge sider.

For $\equiv$ må man også *addere* og *multiplicere* med det "samme" tal på begge sider:

Sætning 4.1.5:

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

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

Beweis:

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & \\ & a = b + km \wedge c = d + lm, \quad k, l \in \mathbb{Z}, \quad \text{ifølge Sætning 4.1.4} \\ \Downarrow & \\ & a + c = (b + km) + (d + lm), \quad k, l \in \mathbb{Z} \\ \Updownarrow & \\ & a + c = b + d + (k+l)m, \quad k+l \in \mathbb{Z} \\ \Updownarrow & \\ & a + c \equiv b + d \pmod{m}, \quad \text{ifølge Sætning 4.1.4} \end{aligned}$$

Tilsvarende:

$$\begin{aligned} & a \equiv b \pmod{m} \wedge c \equiv d \pmod{m} \\ \Downarrow & \\ & a = b + km \wedge c = d + lm, \quad k, l \in \mathbb{Z}, \quad \text{ifølge Sætning 4.1.4} \\ \Downarrow & \\ & ac = (b + km)(d + lm), \quad k, l \in \mathbb{Z} \\ \Downarrow & \\ & ac = bd + blm + kmd + kmlm, \quad k, l \in \mathbb{Z} \\ \Updownarrow & \\ & ac = bd + (bl + kd + kml)m, \quad bl + kd + kml \in \mathbb{Z} \\ \Updownarrow & \\ & ac \equiv bd \pmod{m}, \quad \text{ifølge Sætning 4.1.4} \end{aligned}$$

□

Må man også subtrahere det "samme" tal på begge sider?

Ja, for det er det samme som at addere:

$$c \equiv d \pmod{m} \Leftrightarrow -c \equiv -d \pmod{m}$$

Må man dividere med det samme tal på begge sider?

Nej, ikke generelt:

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

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

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:

$$\Uparrow ab \equiv (a \bmod m)(b \bmod m) \pmod{m}, \text{ ifølge Sætning 4.1.5}$$

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

ifølge Sætning 4.1.3

□

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

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