

Sidste gang:

$a|b$ „a går op i b “

Eks: $3|6 \wedge 3|9 \xRightarrow{\text{Korollar 1}} 3|(2 \cdot 6 + 5 \cdot 9)$
 $3|6 \wedge 6|30 \xRightarrow{\text{Sætning 1 (iii)}} 3|30$

Eks: $17 \text{ div } 5 = \lfloor \frac{17}{5} \rfloor = 3, \quad 17 \text{ mod } 5 = 17 - 5 \cdot 3 = 2$

$-17 \text{ div } 5 = \lfloor \frac{-17}{5} \rfloor = -4, \quad -17 \text{ mod } 5 = -17 - 5 \cdot (-4) = 3$

„a er kongruent med b modulo m“:

$$\begin{array}{lcl} \text{Def. 3} & \Updownarrow & a \equiv b \pmod{m} \\ & \Updownarrow & m | (a-b) \\ \text{Sætning 3} & \Updownarrow & a \text{ mod } m = b \text{ mod } m \\ \text{Sætning 4} & \Updownarrow & \exists k \in \mathbb{Z}: a = b + km \end{array}$$

Eks:

$$17 \equiv 2 \pmod{5}$$

Sætning 5 $\Downarrow$

$$\left\{ \begin{array}{l} 17 + 6 \equiv 2 + 26, \text{ since } 6 \equiv 26 \pmod{5} \\ 17 \cdot 6 \equiv 2 \cdot 26 \\ 17 - 6 \equiv 2 - 26, \text{ since } -6 \equiv -26 \pmod{5} \end{array} \right.$$

Eks: Ifølge Korollar 2:

$$(104 + 252) \text{ mod } 5 = (4 + 2) \text{ mod } 5 = 1$$

$$(104 \cdot 252) \text{ mod } 5 = 4 \cdot 2 \text{ mod } 5 = 3$$

1 dag:

Primtal

Aritmetikens fundamental - Sætning

gcd, lcd

Indbyrdes primiske

Primtal (afsnit 4.3)

Def. 1:

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

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

Ellers er p **sammensat**.

D.v.s.:

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

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

Sætning 1: (Aritmetikens Fundamentalsætning):

Enhvert heltal $n \geq 2$

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

Eks:

$$2 = 2$$

$$3 = 3$$

$$4 = 2 \cdot 2$$

$$10 = 2 \cdot 5$$

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

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

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

Def. 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:

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

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

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

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

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

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

$$\gcd(12, 25) = 1 \Rightarrow 12 \text{ og } 25 \text{ er indbyrdes primiske (Def. 3)}$$

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

$$25 = 5 \cdot 5$$

Def. 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

Exs:

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

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

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

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

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

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

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

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

$$25 = 5 \cdot 5$$

Soetning 5:

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

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