

Sidste gang:

Def. 4.3.1:

p er et **primtal**, hvis

- $p \geq 2$

- 1 og p er de eneste positive heltal, der går op i p

Ellers er p et **sammensat** tal

Sætning 4.3.1: (**Aritmetikens Fundamentalsætning**)

Hvis $n \geq 2$, kan n skrives som et produkt af primtal på præcis én måde.

Sætning 4.3.3

Der er uendeligt mange primtal

(Ikke-konstruktiv eksisterensbevis)

Sætning 4.3.4

„Men der bliver lægere og lægere mellem dem“

Illustration: Erathostnes' si

2 3 5

4 6 8 9 10 12 14 15 16 18 20 21 22 24 25 26 27 28 30 32 33 34 35 36

Jo flere primtal vi tilføjer, jo flere huller bliver fyldt.

Def. 4.3.2:

Største fælles divisor for a og b :

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

Def. 4.3.3:

a og b er indbyrdes primiske, hvis

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

Def. 4.3.5:

Mindste fælles multiplum af a og b :

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

Sætning 4.3.5:

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

Lemma 4.3.2:

Hvis $\gcd(a, b) = 1$, gælder:

$$a \mid bc \Rightarrow a \mid c$$

Lemma 4.3.3:

Hvis p er et primtal, gælder:

$$p \mid a_1 \cdot a_2 \cdot \dots \cdot a_n \Rightarrow \exists i : p \mid a_i$$

Sætning 4.3.7:

Hvis $\gcd(c, m) = 1$, gælder:

$$\begin{aligned} & ac \equiv bc \pmod{m} \\ \Downarrow & \\ & a \equiv b \pmod{m} \end{aligned}$$

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 :

x	0	1	2	3	4	...
$2x \pmod{4}$	0	2	0	2	0	...

← lige → så vi kan ikke få en ulige rest

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

$x=1$ er en løsning

Når vi løser en ligning som $4x=3$,

dividerer vi blot med 4 på begge sider.

hvis vi kunne gange med $s \in \mathbb{Z}$ på begge sider,
så $s \cdot 4x \equiv x \pmod{5}$, ville vi have en løsning.

til kongruensen $4x \equiv 3 \pmod{5}$

D.v.s. vi ønsker $s \cdot 4 \equiv 1 \pmod{5}$.

$$4 \cdot 4 = 16 = 3 \cdot 5 + \underline{1}$$

D.v.s. vi kan bruge $s=4$.

$$\uparrow \quad 4x \equiv 3 \pmod{5}$$

$$\uparrow \quad 4 \cdot 4x \equiv 4 \cdot 3 \pmod{5}$$

$$\uparrow \quad 16x \equiv 12 \pmod{5}$$

$$\uparrow \quad x \equiv 2 \pmod{5} \quad (\text{da } 12 = 5 \cdot 2 + \underline{2})$$

hvis $\gcd(a, m) = 1$, kan vi altid finde sådan et s
til kongruensen $ax \equiv b \pmod{m}$

Sætning 4.4.1:

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

$$\text{Op. 4.4.6} \quad \uparrow \downarrow \quad \gcd(a, m) = 1 \\ \exists! s \in \mathbb{Z}_m = \{0, 1, \dots, m-1\} : sa \equiv 1 \pmod{m}$$

s er multiplikativ invers til a modulo b

Basis:

Eksistens:

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

Unik:

Opgave 4.4.5