

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

Def. 3.5.1 :

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 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).

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

Def 3.4.2:

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

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

Eks :

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

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

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

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

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

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

$$\gcd(12, 25) = 1 \Rightarrow 12 \text{ og } 25 \text{ er } \underline{\text{indhyrdes primiske}} \quad (\text{Def. 3.5.3})$$

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

$$25 = 5 \cdot 5$$

Def. 3.5.4:

$a_1, a_2, \dots, a_n$ er parvis indhyrdes primiske, hvis
 $\gcd(a_i, a_j) = 1$ for alle $1 \leq i < j \leq n$.

Eks 13 : 10, 17 og 21 er parvis indhyrdes primiske

10, 19 og 24 er ikke parvis indhyrdes primiske

Def. 3.4.5:

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

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

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

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

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

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

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

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

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

$$25 = 5 \cdot 5$$

Sætning 3.5.5:

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

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

↑
fælles
primtalsfaktorer

↑
alle primtalsfaktorer,
men fælles faktorer kun én gang.

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 3.7.3:

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 b

Basis:

Eksistens:

Kan findes v.h.a. den udvide 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.

Kongruenssystemer

Eks:

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

$$2, 5, 8, 11, 14, 17, 20, 23, \dots$$

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

$$3, 8, 13, 18, 23$$

$$x \equiv 2 \pmod{7}$$

$$2, 9, 16, 23$$

$x = 23$ er en løsning

Er der altid en løsning?

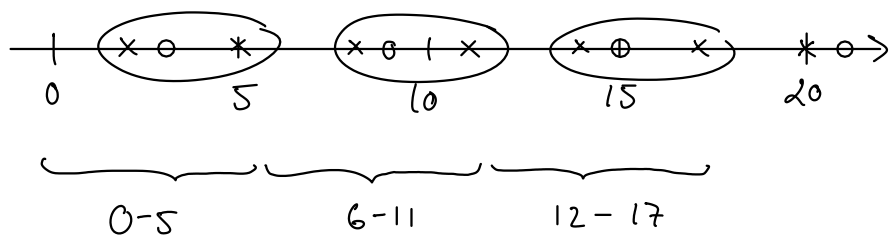
Nej:

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

$$x \equiv 3 \pmod{6}$$

$$2, 5, 8, 11, 14, 17, 20, \dots \quad x$$

$$3, 9, 15, 21, \dots \quad 0$$



hvis vi lægger (et multiplum af 6) til x ,
er begge kongruenser uændede

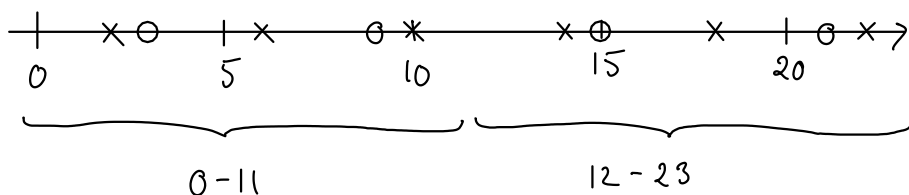
D.v.s.

$$\exists \text{ løsning} \Leftrightarrow \exists \text{ løsning i } \underbrace{\{0, 1, 2, 3, 4, 5\}}_{\mathbb{Z}_6}$$

Tilsvarende:

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

$$x \equiv 3 \pmod{6}$$



Hvis vi lægger 12 til x , er begge
kongruenser uændede.

D.v.s.

$$\exists \text{ løsning} \Leftrightarrow \exists \text{ løsning i } \underbrace{\{0, 1, 2, \dots, 11\}}_{\mathbb{Z}_{12}}$$

Hvis $m_1, m_2, \dots, m_n$ er parvis indbyrdes primiske,

har vi $\{0, 1, \dots, m_1 m_2 \dots m_n\}$ at gøre godt med

- og så er der præcis én løsning i det interval

Hvordan finder vi den løsning?

Tilbage til eksemplet, som kunne løses:

Lad $x = 2 \cdot b_1 + 3 \cdot b_2 + 2 \cdot b_3$, hvor

$$b_1 = \begin{cases} 1 & (\text{mod } 3) \\ 0 & (\text{mod } 5) \\ 0 & (\text{mod } 7) \end{cases}$$

$$b_2 = \begin{cases} 0 & (\text{mod } 3) \\ 1 & (\text{mod } 5) \\ 0 & (\text{mod } 7) \end{cases}$$

$$b_3 = \begin{cases} 0 & (\text{mod } 3) \\ 0 & (\text{mod } 5) \\ 1 & (\text{mod } 7) \end{cases}$$

Da er

$$x \equiv \begin{cases} 2 \cdot 1 + 0 + 0 & (\text{mod } 3) \\ 0 + 3 \cdot 1 + 0 & (\text{mod } 5) \\ 0 + 0 + 2 \cdot 1 & (\text{mod } 7) \end{cases}$$

Kan vi finde b_i 'erne?

$$\begin{array}{lcl} b_1 = 70 & = & 23 \cdot \underbrace{3} + 1 = 14 \cdot \underbrace{5} = 10 \cdot \underbrace{7} \\ b_2 = 21 & = & 7 \cdot \underbrace{3} = 4 \cdot \underbrace{5} + 1 = 3 \cdot \underbrace{7} \\ b_3 = 15 & = & 5 \cdot \underbrace{3} = 3 \cdot \underbrace{5} = 2 \cdot \underbrace{7} + 1 \end{array}$$

D.v.s.

$$\begin{aligned} x &= 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 \\ &\equiv 23 \pmod{105} \end{aligned}$$

Kinesiske Restklasse - Sætning (Sætning 4.4.2)

(Chinese Remainder Theorem)

Hvis

$m_1, m_2, \dots, m_n$: parvis indbyrdes primiske heltal

$a_1, a_2, \dots, a_n \in \mathbb{Z}$

Da gælder, at

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$\vdots$

$$x \equiv a_n \pmod{m_n}$$

har en unik løsning modulo $m = m_1 m_2 \dots m_n$

(D.v.s. $\exists!$ løsning i $\mathbb{Z}_m$)

Bevis:

Ekisterer : Konstruktivt bevis

Idé: Lad $x = \sum_{k=1}^n b_k a_k$, hvor

$$b_k \equiv \begin{cases} 0 & \pmod{m_i}, \text{ for } i \neq k \\ 1 & \pmod{m_i}, \text{ for } i = k \end{cases}$$

Lad $M_k = \frac{m}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_n$

Da gælder:

- $\gcd(M_k, m_k) = 1$,
da m_k ikke har nogen primtalsfaktorer fælles med de andre m_i 'er.

D.v.s.

$$\exists y_k \in \mathbb{Z} : \underline{M_k y_k \equiv 1 \pmod{m_k}} \quad (\text{Sætning 3.7.3})$$

(M_k har en mult. invers mod. m_k)

- $M_k \equiv 0 \pmod{m_i}$, for $i \neq k$

D.v.s.

$$\underline{M_k y_k \equiv 0 \pmod{m_i}}, \text{ for } i \neq k$$

D.v.s.,

$$x = \sum_{k=1}^n M_k y_k a_k, \quad \text{hvor } M_k y_k \equiv 1 \pmod{m_k},$$

er en løsning

Unit modulo m : Opgave 4.4.22

□

D.v.s. løsningsmetode:

- For $1 \leq k \leq n$

Beregn $M_k = \frac{m}{m_k}$

- For $1 \leq k \leq n$

Find y_k , så $M_k y_k \equiv 1 \pmod{m_k}$

- Beregn $x = \sum_{k=1}^n M_k y_k a_k$

Eks fra før:

$$m = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = 5 \cdot 7 = 35$$

$$M_2 = 3 \cdot 7 = 21$$

$$M_3 = 3 \cdot 5 = 15$$

$$\begin{aligned} & \Updownarrow M_1 y_1 \equiv 1 \pmod{m_1} \\ & \Updownarrow 35 y_1 \equiv 1 \pmod{3} \\ & \Updownarrow y_1 = 2 \end{aligned}$$

$$\begin{aligned} & \Updownarrow M_2 y_2 \equiv 1 \pmod{m_2} \\ & \Updownarrow 21 y_2 \equiv 1 \pmod{5} \\ & \Updownarrow y_2 = 1 \end{aligned}$$

$$\begin{aligned} & \Updownarrow M_3 y_3 \equiv 1 \pmod{m_3} \\ & \Updownarrow 15 y_3 \equiv 1 \pmod{7} \\ & \Updownarrow y_3 = 1 \end{aligned}$$

D.v.s.

$$\begin{aligned} x &= M_1 y_1 a_1 + M_2 y_2 a_2 + M_3 y_3 a_3 \\ &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \\ &= 233 \\ &= 2 \cdot 105 + 23 \\ &\equiv 23 \pmod{105} \end{aligned}$$

D.v.s.

$$\begin{aligned} \text{Løsningsmængde: } \{ 23 + 105 \cdot k \mid k \in \mathbb{Z} \} &= \\ \{ \dots, -187, -82, 23, 128, 233, \dots \} \end{aligned}$$