

Euklids Algoritme

(afsnit 4.3)

$$\gcd(287, 91) = ?$$

$$287 = 91 \cdot 3 + 14$$

$$91 = 14 \cdot 6 + \textcircled{7}$$

$$14 = 7 \cdot 2$$

$$\text{D.v.s. } \gcd(287, 91) = 7$$

$$\text{Check: } 287 = 7 \cdot 41$$

$$91 = 7 \cdot 13$$

Hvorfor virker det?

Lemma 4.3.1

$$\begin{aligned} a &= bq + r, \quad a, b, q, r \in \mathbb{Z} \\ \Downarrow \\ \gcd(a, b) &= \gcd(b, r) \end{aligned}$$

Bevis:

Vil vise, at $d|a \wedge d|b \Leftrightarrow d|b \wedge d|r$

(D.v.s. de divisorer, som er fælles for a og b ,
er de samme som for b og r .)

Dette er et stærkere udsagn end $\gcd(a, b) = \gcd(b, r)$

$$\Leftarrow: d|b \wedge d|r$$

$$\Downarrow \underbrace{d|(qb+r)}_{=a}, \text{ ifølge Korollar 4.1.1}$$

$$\Rightarrow: d|a \wedge d|b$$

$$\Downarrow \underbrace{d|(a-bq)}_{=r}, \text{ ifølge Kor. 4.1.1}$$



Ifølge Lemma 1 betyder udregningene ovenfor, at

$$\begin{aligned}\gcd(287, 91) &= \gcd(91, 14) = \gcd(14, 7) \\ &= \gcd(7, 0) = 7\end{aligned}$$

Ved at regne baglæns, kan man skrive $\gcd(a, b)$ som linearkombination af a og b (Sætning 4.3.6).

I eks. ovenfor:

$$\begin{aligned}7 &= 91 - 14 \cdot 6 \\ &= 91 - (287 - 3 \cdot 91) \cdot 6 \\ &= 91 - 6 \cdot 287 + 18 \cdot 91 \\ &= 19 \cdot 91 - 6 \cdot 287\end{aligned}$$

Hvornår kunne vi være interesserede i det?

Hvis vi f.eks. gerne vil finde en multiplikativ invers:

$$a\bar{a} \equiv 1 \pmod{m}$$

$\bar{a}$ eksisterer, hvis $\gcd(a, m) = 1$, fordi da kan 1 skrives som en linearkombination af a og m :

$$\begin{aligned}\Downarrow \quad 1 &= sa + tm, \quad s, t \in \mathbb{Z} \\ 1 &\equiv sa \pmod{m}\end{aligned}$$

Euklids Udvidede Algoritme beregner både $\gcd(a, b)$, s og t . Mere om det i DM534...

D.v.s. EUA er et konstruktivt bevis for Sætning 4.3.6.

Lineare kongruenser (afsnit 4.4)

Har $ax \equiv b \pmod{m}$ en løsning?

Hvis $\gcd(a, m) = 1$: ja

Ellers: Måske

Eks:

• $4x \equiv 3 \pmod{5}$ $\gcd(4, 5) = 1$

$x=2$ er en løsning

• $2x \equiv 3 \pmod{4}$ $\gcd(2, 4) = 2$

Ingen løsning:

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

↖ lige ↗, så vi kan ikke få en ulige rest.

• $2x \equiv 2 \pmod{4}$ $\gcd(2, 4) = 2$

$x=1$ er en løsning.

Bemærk:

For at løse ligningen $4x \equiv 3 \pmod{5}$ ganger vi blot med $\frac{1}{4}$ på begge sider, fordi $\frac{1}{4}$ er multiplikativt invers til 4:

$$4x \equiv 3 \pmod{5} \Leftrightarrow \frac{1}{4} \cdot 4x = \frac{1}{4} \cdot 3 \pmod{5} \Leftrightarrow x \equiv \frac{3}{4} \pmod{5}$$

Vi kan gøre det samme for kongruensen $4x \equiv 3 \pmod{5}$, hvis vi kan finde en multiplikativt invers til 4 modulo 5:

$$4x \equiv 3 \pmod{5} \Leftrightarrow 4 \cdot 4x \equiv 4 \cdot 3 \pmod{5} \Leftrightarrow x \equiv 2 \pmod{5}$$

↑
Sætning 4.3.7:
⇐

findes der altid en multiplikativ invers til a modulo m ?

Hvis $\gcd(a, m) = 1$: Ja, der findes præcis én i $\mathbb{Z}_m$ (Sætning 1)

Ellers: Nej (Opgave 6)

Sætning 4.4.1

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

$$\begin{array}{c} \text{Opg. 8} \\ \uparrow \downarrow \end{array} \quad \begin{array}{l} \gcd(a, m) = 1 \\ \exists! s \in \mathbb{Z}_m : sa \equiv 1 \pmod{m} \end{array}$$

s er multiplikativ invers til a modulo m

Basis:

Eksistens:

Kan findes v.h.s. den udvidede Euklids Alg. (afsnit 4.3)

Unik:

Opgave 7

Bemærk, at $ax \equiv b \pmod{m}$ godt kan have en løsning, selvom a ikke har en multiplikativ invers modulo m (jof. ovenstående eks.).

Kongruenssystemer

Eks:

$$x \equiv 2 \pmod{3} \quad 2, 5, \textcircled{8}, 11, 14, 17, 20, \textcircled{23} \dots$$

$$x \equiv 3 \pmod{5} \quad 3, \textcircled{8}, 13, 18, \textcircled{23}$$

$$x \equiv 2 \pmod{7} \quad 2, 9, 16, \textcircled{23}$$

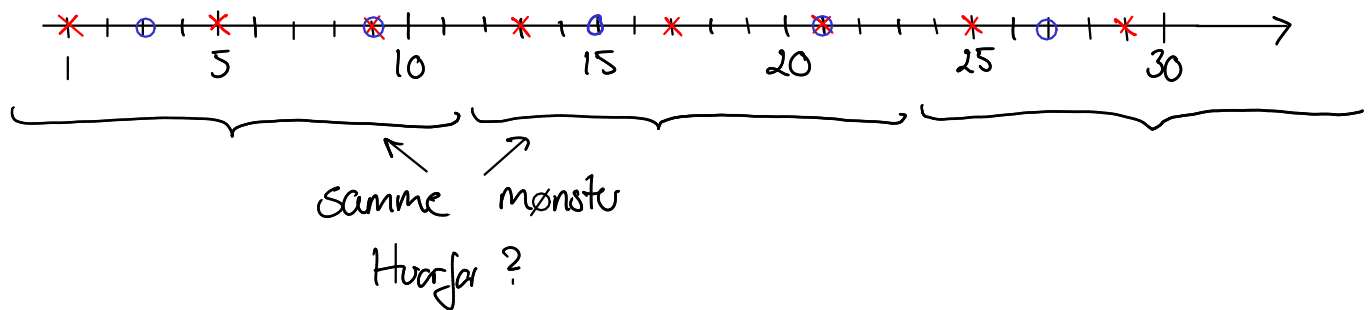
$x = \textcircled{23}$ er en løsning

Vi vender tilbage til dette eks...

Eks:

$$x \equiv 1 \pmod{4} \quad 1, 5, \textcircled{9}, 13, 17, \textcircled{21}, 25, 29, \dots \quad \times$$

$$x \equiv 3 \pmod{6} \quad 3, \textcircled{9}, 15, \textcircled{21}, 27, \dots \quad \circ$$



Hvis man lægger (et multiplum af) 12 til x ,
er begge kongruenser uændrede, da 12 er et
multiplum af begge moduli.

D.v.s.

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

Desuden:

$$x \text{ er en løsning} \Rightarrow \forall k \in \mathbb{Z}: x + 12k \text{ er en løsning}$$

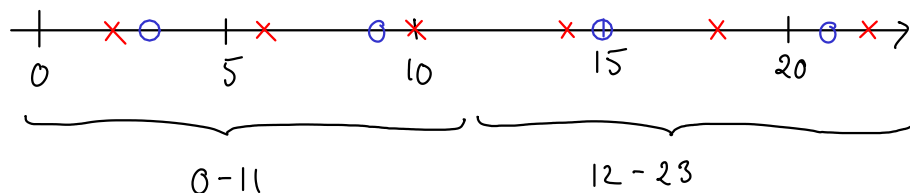
D.v.s. x er en løsning, hvis

$$x \in \{9 + 12k \mid k \in \mathbb{Z}\} = \{\dots, -15, -3, 9, 21, 33, \dots\}$$

Eks:

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

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



$\exists$ løsning $\Leftrightarrow \exists$ løsning i $\mathbb{Z}_{12}$

D.v.s. der er ingen løsning.

Bemærk: $\text{lcm}(4,6) = 12$

Generelt:

For n kongruenser med moduli $m_1, m_2, \dots, m_n$ gælder

$\Updownarrow \exists$ løsning

$\Updownarrow \exists$ løsning $\in \mathbb{Z}_{\text{lcm}(m_1, m_2, \dots, m_n)}$

$\Updownarrow \exists!$ løsning $\in \mathbb{Z}_{\text{lcm}(m_1, m_2, \dots, m_n)}$

$\text{lcm}(m_1, m_2, \dots, m_n)$ er størst mulig, hvis $m_1, m_2, \dots, m_n$ er parvis indbyrdes primiske. (Da er

$$\text{lcm}(m_1, m_2, \dots, m_n) = m_1 \cdot m_2 \cdot \dots \cdot m_n.)$$

Vi skal se, at i det tilfælde er der altid en løsning (Kinesiske Restklasse-Løsning).

Hvordan finder vi den løsning?

Tilbage til eksemplet, som kunne løses:

Lad $X = 2 \cdot b_1 + 3 \cdot b_2 + 2 \cdot b_3$, hier

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

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

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

Da er

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

Mer findes der sådanne b_i 'er? Ja:

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

$$\begin{aligned} \text{D.O.S. } X &= 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 \\ &\equiv 23 \pmod{105} \end{aligned}$$

$\nwarrow 3 \cdot 5 \cdot 7 = \text{lcm}(3, 5, 7)$

Kan man altid finde sådanne b_i 'er?

Ja. Det fremgår af beviset for:

Sætning 4.4.2 (Kinesiske Restklasse-Sætning)

Hvis

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

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

$m = m_1 \cdot m_2 \cdot \dots \cdot m_n$

Da har

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

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

$\vdots$

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

en unik løsning modulo m (d.v.s. $\exists!$ løsning i $\mathbb{Z}_m$)

NB: Der kan godt være en løsning, selvom m_i 'erne ikke er parvis indbyrdes primiske, jvf. vores andet eksempel.

Basis:

Ekisterer: Konstruktivt bevis:

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

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

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

Da gælder:

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

D.v.s. for ethvert $y_k \in \mathbb{Z}$ gælder:

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

Så skal vi bare vælge y_k sådan, at

$$M_k y_k \equiv 1 \pmod{m_k}:$$

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

D.v.s.

$$\exists y_k \in \mathbb{Z} : M_k y_k \equiv 1 \pmod{m_k} \quad (\text{Sætning 4.4.1})$$

(M_k har en mult. invers mod m_k)

D.v.s. vi kan vælge $b_k = M_k y_k$, hvor y_k er en multiplikativ invers til M_k modulo m_k .

D.v.s.,

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

er en løsning til kongruenssystemet

Unik modulo m : Opgave 4.4.29 og 4.4.30 $\square$

D.v.s. løsningsmetode:

• For $1 \leq k \leq n$

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

• For $1 \leq k \leq n$

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

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

$$\text{Løsningsmængde: } \{x + cm \mid c \in \mathbb{Z}\}$$

OBS: Hvis $m_1, \dots, m_n$ ikke er parvis indbyrdes primiske, kan der godt være en løsning, men ovenstående metode kan ikke bruges til at finde den. (Hvorfor ikke?)

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.

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