

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?

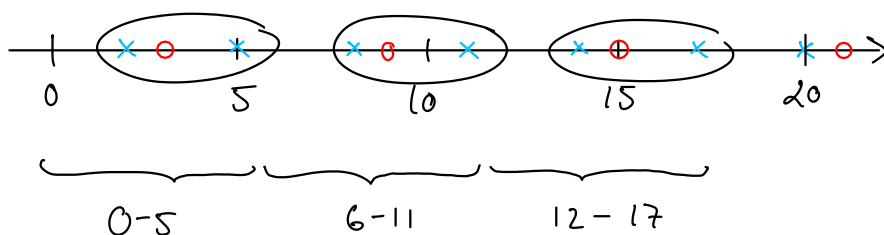
Nej:

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

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

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

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



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

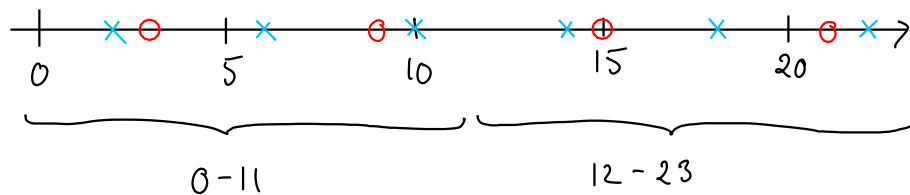
D.v.s.

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

Tilsvarende:

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

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



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

P.v.s.

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

Bemærk: $\text{lcm}(3, 6) = 6$ og $\text{lcm}(4, 6) = 12$

Generelt: n kongruenser med moduli $m_1, m_2, \dots, m_n$

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

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

$\text{lcm}(m_1, m_2, \dots, m_n)$ er størst muligt, hvis

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

(da er $\text{lcm}(m_1, m_2, \dots, m_n) = m_1 m_2 \dots m_n$)

Vi skal se, at i det tilfælde $\exists! \text{ løsning i } \mathbb{Z}_{m_1 m_2 \dots m_n}$ (Kinesiske Restklasse-løsning)

Howdan 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

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

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

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

Da er

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

Kan vi finde b_i 'erne?

$b_1 = 70$	$= 23 \cdot 3 + 1 = 14 \cdot 5 = 10 \cdot 7$
$b_2 = 21$	$= 7 \cdot 3 = 4 \cdot 5 + 1 = 3 \cdot 7$
$b_3 = 15$	$= 5 \cdot 3 = 3 \cdot 5 = 2 \cdot 7 + 1$

D.v.s.

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

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

Kinesiske Restklasse-Løsning (Sætning 2)

(Chinese Remainder Theorem)

Hvis

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

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

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

Da har

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

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

$\vdots$

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

er unik løsning modulo m

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

NB:

Der kan godt være en løsning, selvom m 'ene ikke er p.i.p.

Ekst:

$$x \equiv 1 \pmod{4}$$

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

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:

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

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.

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

(M_k har en mult. invers mod m_k)

D.v.s. vi kan vælge $b_k = M_k y_k$

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 4.4.21 og 4.4.22 $\square$

D.v.s. løsningsmetode:

o For $1 \leq k \leq n$

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

o For $1 \leq k \leq n$

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

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

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

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.

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

I DM534 kommer I til at se et bevis for, at RSA „virker“, d.v.s. $S(P(M)) = M$
Beviset bruger KRS og punkt (1) i

Fermats Lille Sætning (Sætning 3):

Lad $a, p \in \mathbb{Z}$, p primtal

$$(1) \quad p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

$$(2) \quad a^p \equiv a \pmod{p}$$

Bemærk, at $(2) \Rightarrow (1)$ p.g.a. Sætning 4.3.7
(men ikke omvendt).

Eks 9: Beregn $7^{222} \pmod{11}$

11 er et primtal og går ikke op i 7.

D.v.s. vi kan bruge Sætning 3(1) med $a=7, p=11$:

$$7^{10} \equiv 1 \pmod{11}$$

$$7^{222} = 7^{10 \cdot 22 + 2} = 7^{10 \cdot 22} \cdot 7^2 = (7^{10})^{22} \cdot 7^2$$

D.v.s.

$$7^{222} \pmod{11} = (7^{10})^{22} \cdot 7^2 \pmod{11}$$

$$= 1^{22} \cdot 7^2 \pmod{11}, \text{ ifølge Sætning 3(1) og Korollar 4.1.2}$$

$$= 49 \pmod{11}$$

$$= 5$$