Kongruenssystemer

Eks:

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

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

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

$x = \underline{23}$ er en løsning

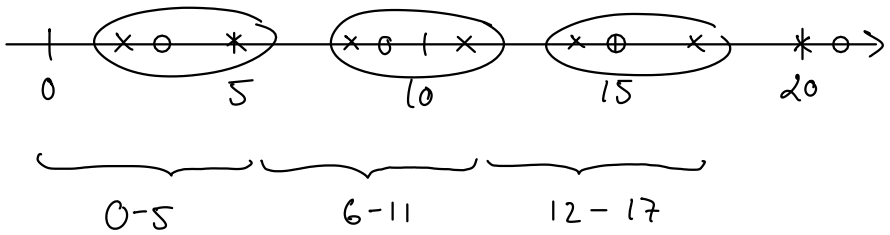
.

Er der altid en løsning ?

Nej:

$x \equiv 2 \pmod 3$ $\quad 2, 5, 8, 11, 14, 17, 20, \ldots$ $\quad x$

$x \equiv 3 \pmod 6$ $\quad 3, 9, 15, 21, \ldots$ $\quad o$



Hvis vi lægger (et multiplum af) 6 til x, er begge kongruenser overholdt

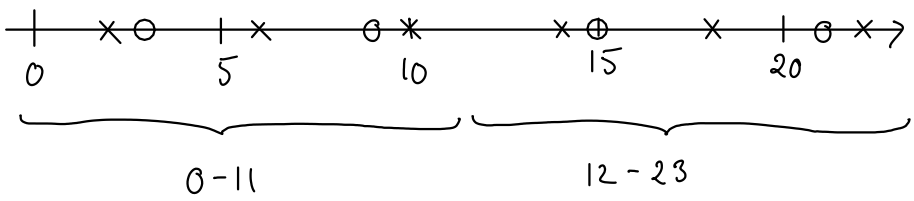
D.v.s.

$\exists$ løsning $\Leftrightarrow$ $\exists$ 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 vandrede.

D.U.S.

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

Hvis $m_1, m_2, \ldots, m_n$ er parvis indbyrdes primiske, har vi $\{0,1,\ldots,m_1 m_2 \cdots m_n - 1\}$ 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 $\boxed{x = 2\cdot b_1 + 3\cdot b_2 + 2\cdot b_3}$, 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?

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

D.u.s.

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

Def. 4.3.4:

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

Eks 13: 10, 17 og 21 er parvis indbyrdes primiske
10, 19 og 24 er ikke parvis indbyrdes primiske

Kinesiske Restklasse-Sætning (Sætning 4.4.2)

(Chinese Remainder Theorem)

Hvis

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

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

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 $m = m_1 m_2 \cdots m_n$.

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

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

Eks:

$$x \equiv 1 \pmod{4}$$
$$x \equiv 3 \pmod{6}$$

Bevis:

Eksisterer: 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 $M_k = \frac{m}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_n$

Da gælder:

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

D.u.s.

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

(M_k har en mult. invers mod m_k)

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

D.u.s. vi kan vælge $b_k = M_k y_k$

D.u.s.

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

D.u.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

Unik modulo m: Opgave 4.4.21 og 4.4.22 □

D.U.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:

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

$M_1 = 5 \cdot 7 = 35$
$M_2 = 3 \cdot 7 = 21$
$M_3 = 3 \cdot 5 = 15$

$M_1 y_1 \equiv 1 \pmod{m_1}$
$\Leftrightarrow \; 35 y_1 \equiv 1 \pmod{3}$
$\Leftarrow \; y_1 = 2$

$M_2 y_2 \equiv 1 \pmod{m_2}$
$\Leftrightarrow \; 21 y_2 \equiv 1 \pmod{5}$
$\Leftarrow \; y_2 = 1$

$M_3 y_3 \equiv 1 \pmod{m_3}$
$\Leftrightarrow \; 15 y_3 \equiv 1 \pmod{7}$
$\Leftarrow \; y_3 = 1$

D.u.s.

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

D.u.s.

Løsningsmengde: $\{ 23 + 105 \cdot k \mid k \in \mathbb{Z} \} =$
$\{ \ldots, -187, -82, 23, 128, 233, \ldots \}$

Næste gang skal vi vise, at RSA „virker".
Beviset bruger KRS og punkt (1) i

Fermats Lille Sætning (Sætning 4.4.3):

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

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

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

Bevis:

(2): Opgave 4.4.13

(1) følger af (2):

p primtal og $p \nmid a$

$\Downarrow$

$\gcd(a,p) = 1$

$\Downarrow$

$\exists \bar{a} \in \mathbb{Z} : \bar{a}a \equiv 1 \pmod{p}$, ifølge Sætning 4.4.1.

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

$\Downarrow$

$a^{p-1} a \equiv a \pmod{p}$

$\Downarrow$

$a^{p-1} a\bar{a} \equiv a\bar{a} \pmod{p}$

$\Downarrow$

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

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

11 er et primtal og går ikke op i 7.

D.v.s. vi kan bruge Sætning 4.4.3 (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.

$$\begin{aligned} 7^{222} \bmod 11 &= (7^{10})^{22} \cdot 7^2 \bmod 11 \\ &= 1^{22} \cdot 7^2 \bmod 11, \quad \text{iflg. Sætning 4.4.3(1)} \\ &= 49 \bmod 11 \\ &= 5 \end{aligned}$$