Lineære kongruenser: $ax \equiv b \pmod{n}$ løsbar $\iff$ $\gcd(a,n)$ deler b. Hvis x_0 er en løsn, vil

$$x \equiv x_0, x_0 + n/d, x_0 + 2n/d, \dots, x_0 + (d-1)n/d \pmod{n}$$

gi alle de d løsningene modulo n. For å finne en x_0: løs

$$ax + ny = b$$

for eksempel m/ Euklids algoritme.

Systemer: Hvordan løse systemer av lineære kongruenser?

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_t x &\equiv b_t \pmod{n_t} \end{aligned}$$

Altså finne alle $x \in \mathbb{Z}$ som passer inn i alle kongruensene. Kan ofte redusere til systemer på form

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_t \pmod{n_t} \end{aligned}$$

Teorem 4.8 (Det kinesiske restteorem)

La

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_t \pmod{n_t} \end{aligned}$$

være et system av lin. kongr. Hvis $\gcd(n_i, n_j) = 1$ når $i \neq j$, så har systemet en unik løsning modulo $n_1 n_2 \cdots n_t$.

Bevis/algoritme:

(1) Sett

$$\begin{aligned} N_1 &= n_2 n_3 \cdots n_t \\ N_2 &= n_1 n_3 \cdots n_t \\ &\vdots \\ N_t &= n_1 n_2 \cdots n_{t-1} \end{aligned}$$

dvs $N_k = \prod_{\substack{i=1 \\ i \neq k}}^{t} n_i$

(2) Løs følgende t kongruenser hver for seg:

$$\begin{aligned} N_1 x &\equiv 1 \pmod{n_1} \longrightarrow x_1 \text{ en løsning} \\ N_2 x &\equiv 1 \pmod{n_2} \longrightarrow x_2 \text{ en løsning} \\ &\vdots \\ N_t x &\equiv 1 \pmod{n_t} \longrightarrow x_t \text{ en løsning.} \end{aligned}$$

(3) Dann tallet

$$x_0 = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_t N_t x_t$$

(4) Løsningen av systemet:

$$x \equiv x_0 \pmod{n_1 n_2 \cdots n_t}$$

Se på en kongruens $N_k x \equiv 1 \pmod{n_k}$ i punkt (2). Siden $N_k = \prod_{\substack{i=1 \\ i \neq k}}^{t} n_i$ er $\gcd(N_i, n_i) = 1$, så den er løsbar, og vi kan finne en x_i som passer inn. Da vil

$$x_0 = a_1 N_1 x_1 + \cdots + a_t N_t x_t$$

være en løsn. av det opprinnelige systemet. For se på $x \equiv a_i \pmod{n_i}$. Siden $n_i \mid N_k$ når $i \neq k$ er $N_k \equiv 0 \pmod{n_i}$ for $i \neq k$, som gir $a_k N_k x_k \equiv 0 \pmod{n_i}$ for $k \neq i$. Det gir

$$x_0 = a_1 N_1 x_1 + \cdots + a_t N_t x_t \equiv a_i N_i x_i \pmod{n_i}.$$

Videre er x_i valgt slik at $N_i x_i \equiv 1 \pmod{n_i}$, som gir $a_i N_i x_i \equiv a_i \pmod{n_i}$. Derfor er

$$x_0 \equiv a_i N_i x_i \equiv a_i \pmod{n_i}$$

så x_0 løser systemet.

Anta $y \equiv x_0 \pmod{n_1 n_2 \cdots n_t}$. Da vil $n_1 n_2 \cdots n_t$ dele $y - x_0$, så n_i deler $y - x_0$ $\forall i$, dvs $y \equiv x_0 \pmod{n_i}$. Det gir $y \equiv x_0 \equiv a_i \pmod{n_i}$ $\forall i$, så y er en løsn av systemet. Motsatt, anta y er en løsn av systemet. Da er $y \equiv a_i \equiv x_0 \pmod{n_i}$ $\forall i$, så $n_i \mid (y - x_0)$ $\forall i$. Siden $\gcd(n_i, n_j) = 1$ for $i \neq j$, vil da $n_1 n_2 \cdots n_t$ dele $y - x_0$, dvs $y \equiv x_0 \pmod{n_1 n_2 \cdots n_t}$. □

Eksempler: (1) Midtsem H2013, oppg 3:

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$

Får $N_1 = 5 \cdot 7 = 35$, $N_2 = 3 \cdot 7 = 21$, $N_3 = 3 \cdot 5 = 15$, og må løse disse individuelt:

$$35x \equiv 1 \pmod 3 \longrightarrow x_1 = -1 \text{ passer inn}$$
$$21x \equiv 1 \pmod 5 \longrightarrow x_2 = 1 \text{ passer inn}$$
$$15x \equiv 1 \pmod 7 \longrightarrow x_3 = 1 \text{ passer inn}$$

(tips: let etter små verdier for løsninger av disse, som 1, -1, 2, -2 etc).
Får nå

$$x_0 = 1 \cdot 35 \cdot (-1) + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 52$$

Så løsningen av systemet er

$$x \equiv 52 \pmod{3 \cdot 5 \cdot 7}$$

dvs

$$x \equiv 52 \pmod{105}$$

(2) Eksamen H2011, oppg 2:

$$8x \equiv 6 \pmod 7$$
$$x \equiv -3 \pmod 9$$
$$4x \equiv -1 \pmod{13}$$

Her må vi få fjernet koeffisientene 8 og 4. Siden $6 \equiv -8 \pmod 7$ er $8x \equiv -8 \pmod 7$, og siden $\gcd(7,8)=1$ kan vi dele ut og få $x \equiv -1 \pmod 7$. Videre, siden $-1 \equiv 12 \pmod{13}$ er $4x \equiv 12 \pmod{13}$, og $\gcd(4,13)=1$ gir da $x \equiv 3 \pmod{13}$. Så systemet er ekvivalent med systemet

$$x \equiv -1 \pmod 7$$
$$x \equiv -3 \pmod 9$$
$$x \equiv 3 \pmod{13}$$

Setter $N_1 = 9\cdot 13 = 117$, $N_2 = 7\cdot 13 = 91$, $N_3 = 7\cdot 9 = 63$, og må løse disse individuelt:

$$117x \equiv 1 \pmod 7 \longrightarrow x_1 = 3 \text{ passer inn}$$
$$91x \equiv 1 \pmod 9 \longrightarrow x_2 = 1 \text{ passer inn}$$
$$63x \equiv 1 \pmod{13}$$

For å finne x_1 prøvde jeg $1, -1, 2, -2$ og så 3. For x_2 ser vi at $91 \equiv 1 \pmod 9$, så $x_2 = 1$ passer. For x_3 prøvde jeg $1, -1, 2, -2, 3, -3$ uten hell. Euklids alg gir

$$63 = 4\cdot 13 + 11$$
$$13 = 1\cdot 11 + 2$$
$$11 = 5\cdot 2 + 1$$

$$\Rightarrow 1 = 63\cdot 6 + 13(-29)$$

Så $13 \mid (63\cdot 6 - 1)$, dvs $x_3 = 6$ er en løsning. Får da

$$x_0 = (-1)\cdot 117\cdot 3 + (-3)\cdot 91\cdot 1 + 3\cdot 63\cdot 6 = 510$$

Så løsn på systemet er

$$x \equiv 510 \pmod{7\cdot 9\cdot 13}$$

dvs

$$x \equiv 510 \pmod{819}$$

Merk: Hvis vi har $ax \equiv b \pmod n$ og $\gcd(a,n)=1$, finnes alltid en $c \in \mathbb{Z}$ med $a|c$ og $b \equiv c \pmod n$. Da er $ax \equiv c \pmod n$, og siden $a|c$ er $c = am$ for en m. Da er $ax \equiv am \pmod n$, og vi kan dele ut siden $\gcd(a,n)=1$:

$$x \equiv m \pmod n$$

Dette gjorde vi med $8x \equiv 6 \pmod 7$ og $4x \equiv -1 \pmod{13}$ over.