I dag:

Afsnit 4.3: Euklids Algoritme til at beregne gcd
Afsnit 4.4: Lineære kongruenser og kongruenssystemer

Vi så sidste gang, at vi kan finde gcd(a,b) ved at faktorisere a og b.
Eks:

gcd(18,24) = 6:

$18 = 2 \cdot 3 \cdot 3$

$24 = 2 \cdot 2 \cdot 2 \cdot 3$

Hvis a og b er store, tager det for lang tid at faktorisere dem.
(Der er mange krypteringsprotokoller, som afhænger af, at det tager for lang tid at faktorisere meget store tal.)
Derfor har vi brug for en mere effektiv algoritme til at beregne gcd.

Euklids Algoritme (afsnit 4.3)

$\gcd(287, 91) = ?$

$287 = 91 \cdot 3 + 14$

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

$14 = 7 \cdot 2$

D.v.s. $\gcd(287, 91) = 7$ Check: $287 = 7 \cdot 41$

$91 = 7 \cdot 13$

Hvorfor virker det?

Lemma 4.3.1

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

Bevis:

Vil vise, at $d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$

(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 $\gcd(a,b) = \gcd(b,r)$

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

$\Downarrow$

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

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

$\Downarrow$

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

□

Ifølge Lemma 1 betyder udregningerne ovenfor, at

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7)$$
$$= \gcd(7, 0) = 7$$

Ved at regne baglæns, kan man skrive $\gcd(a,b)$ som linear-kombination af a og b (Sætning 4.3.6).
I eks. ovenfor:

$$7 = 91 - 14 \cdot 6$$
$$= 91 - (287 - 3 \cdot 91) \cdot 6$$
$$= 91 - 6 \cdot 287 + 18 \cdot 91$$
$$= 19 \cdot 91 - 6 \cdot 287$$

Sætning 4.3.6 kan bl.a. bruges til at bevise Aritmetikkens Fundamentalsætning.
Om lidt skal vi se en anden anvendelse...

Lineære kongruenser (Afsnit 4.4)

Minder om lineær (d.v.s. 1. grads) ligninger.
Eks: $4x = 5 \iff x = 5/4$

Eks: $4x \equiv 5 \pmod{11}$ $(\gcd(4,11)=1)$
$x = 4$ er en løsning, da $16 \equiv 5 \pmod{11}$

$4x \equiv 5 \pmod{10}$ $(\gcd(4,10)=2)$
Hvis vi dividerer med 10, giver $4x$ en lige rest, og 5 giver en ulige rest. Dvs:
Ingen løsning

$4x \equiv 2 \pmod{10}$ $(\gcd(4,10)=2)$
$x = 3$ er en løsning.

Hvornår har $ax \equiv b \pmod{m}$ en løsning?
- Hvis $\gcd(a,m)=1$: Altid
- Ellers: Nogle gange

En lineær ligning har altid en løsning.
Vi finder den ved at gange med $\frac{1}{a}$ på begge sider:

$$ax = b \iff \frac{1}{a} \cdot ax = \frac{1}{a} b \iff x = \frac{b}{a}$$

Kan vi tilsvarende gange noget på begge sider af kongruensen, så venstre-siden bliver x?
D.v.s. findes der et $\bar{a}$, så $\bar{a} \cdot a \equiv 1 \pmod{m}$?
Så ville vi få

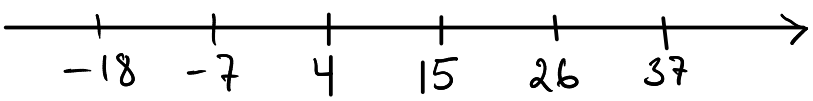
$\bar{a}$: multiplikativ invers til a modulo m

$$\begin{aligned} & ax \equiv b \pmod{m} \\ \Downarrow\Uparrow\ & \bar{a} \cdot ax \equiv \bar{a}b \pmod{m} \\ & x \equiv \bar{a}b \pmod{m} \end{aligned}$$

Eks: $4x \equiv 5 \pmod{11}$

$$\begin{aligned} \Updownarrow\ & 3 \cdot 4x \equiv 3 \cdot 5 \pmod{11} \\ \Updownarrow\ & 12x \equiv 15 \pmod{11} \\ \Updownarrow\ & x \equiv 4 \pmod{11} \end{aligned}$$

$\Updownarrow$ følger af Sætning 4.3.7



Løsningsmængden er

$$\{4 + 11k \mid k \in \mathbb{Z}\} = \{\ldots, -7, 4, 15, \ldots\}$$

$4x \equiv 5 \pmod{10}$

4 har ikke nogen multiplikativ invers modulo 10:

$$\begin{aligned} 1 \cdot 4 &\equiv 4 \pmod{10} \\ 2 \cdot 4 &\equiv 8 \pmod{10} \\ 3 \cdot 4 &\equiv 2 \pmod{10} \\ 4 \cdot 4 &\equiv 6 \pmod{10} \\ 5 \cdot 4 &\equiv 0 \pmod{10} \\ &\vdots \end{aligned}$$

Hvordan afgør vi, om a har en multiplikativ invers modulo m?

- Hvis $\gcd(a,m)=1$: Ja (Sætning 1)
- Ellers: Nej (Opgave 8)

Hvis $\gcd(a,m)=1$, kan vi finde $\bar{a}$ v.h.a. Euklids Udvidede Algoritme.

Eks:

$$11 = 4\cdot 2 + 3 \quad (i)$$
$$4 = 3\cdot 1 + 1 \quad (ii)$$

Heraf fås:

$$1 \overset{(ii)}{=} 4 - 3 \overset{(i)}{=} 4 - (11 - 4\cdot 2) = 4\cdot 3 - 11$$
$$\Downarrow$$
$$4\cdot 3 = 1 + 11$$
$$\Downarrow$$
$$4\cdot 3 \equiv 1 \pmod{11}$$

D.v.s. 3 er en multiplikativ invers til 4 modulo 11. Og der er ikke andre tal i $\mathbb{Z}_{11}$, som er multiplikativ invers til 4 modulo 11 (opgave 7):

Sætning 4.4.1

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

$$\gcd(a,m)=1$$
$$\Downarrow$$
$$\exists!\, \bar{a} \in \mathbb{Z}_m : \bar{a}a \equiv 1 \pmod{m}$$

Bemærk, at $ax \equiv b \pmod{m}$ godt kan have en løsning, selvom a ikke har nogen invers, jvf. ovenstående eks.

Kongruenssystemer

Eks:

$x \equiv 2 \pmod 3$: $2, 5, (8), 11, 14, 17, 20, (23) \ldots$

$x \equiv 3 \pmod 5$: $3, (8), 13, 18, (23)$

$x \equiv 2 \pmod 7$: $2, 9, 16, (23)$

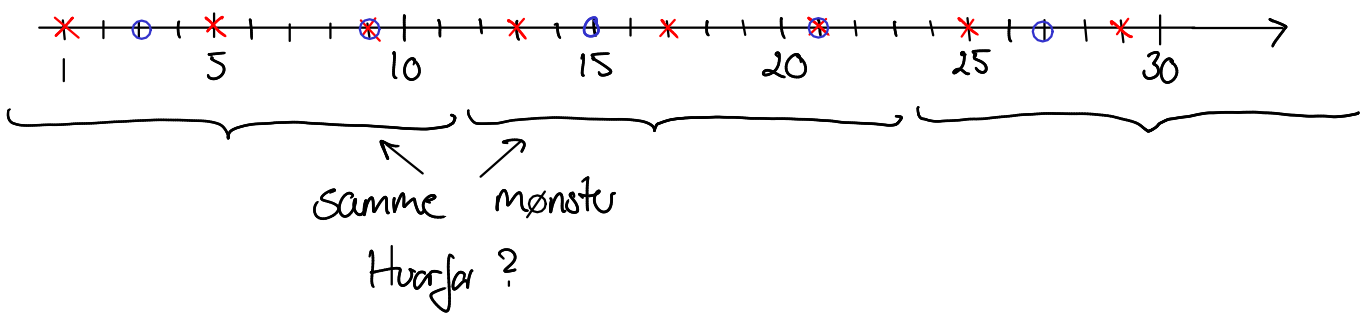
$x = (23)$ er en løsning

Vi vender tilbage til dette eks...

Eks:

$x \equiv 1 \pmod 4$: $1, 5, (9), 13, 17, (21), 25, 29, \ldots$ x

$x \equiv 3 \pmod 6$: $3, (9), 15, (21), 27, \ldots$ o



Hvorfor ?

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

D.v.s.

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

Desuden:

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

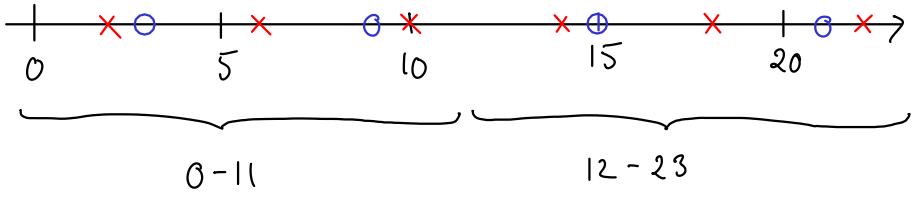
D.v.s. x er en løsning, hvis

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

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

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

Hvordan finder vi den løsning?

Tilbage til dit første eksempel:

Lad $\boxed{x = 2\cdot b_1 + 3\cdot b_2 + 2\cdot b_3}$, 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

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

Men findes der sådanne b_i'er? Ja:

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

D.v.s. $x = 2\cdot 70 + 3\cdot 21 + 2\cdot 15 = 233$

$\equiv 23 \pmod{105}$

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

Kan man altid finde sådanne b_i'er?

Ja. Det fremgår af beviset for den Kinesiske Restklasse-Sætning.