Sidste gang

Delelighed $a \mid b$
- Def.
- Regler
- Divisionsalgoritmen

Kongruens $a \equiv b \pmod{n}$
- Def.
- Regneregler

Primtal
- Def.
- Aritmetikkens Fundamentalsætning
- Største fælles divisor (gcd)

I dag

gcd & lcm
- Euklids Alg.

Mere om kongruenser
- Dividere på begge sider ?
- Multiplikativ invers
- Kongruenssystemer

Delelighed

Def:

Def. 4.1.1:

For $a,b \in \mathbb{Z}$, $a \neq 0$, gælder:

$$a \mid b \iff \frac{b}{a} \in \mathbb{Z} \iff \exists k \in \mathbb{Z}: b = k \cdot a$$

"a går op i b"

"a er en faktor i b"

"b er et multiplum af a"

Regler:

Sætning 4.1.1:

For $a,b,c \in \mathbb{Z}$, $a \neq 0$, gælder

(i) $a \mid b \wedge a \mid c \Rightarrow a \mid (b+c)$

(ii) $a \mid b \Rightarrow \forall k \in \mathbb{Z}: a \mid kb$

(iii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

$\Rightarrow$

Korollar 4.1.1:

$a \mid b \wedge a \mid c \Rightarrow$
$\forall m,n \in \mathbb{Z}: a \mid (mb+nc)$

Divisionsalgoritmen:

Eks:

$16 = 3 \cdot 5 + 1$

$-16 = 3 \cdot (-6) + 2$

Kongruens

Def 4.1.3 / Sætning 4.1.3 / Sætning 4.1.4

$$a \equiv b \pmod{m} \quad \text{»} a \text{ og } b \text{ er kongruente modulo } m\text{«}$$

$$\Updownarrow$$

$$m \mid (a-b) \qquad (*)$$

$$\Updownarrow$$

$$a \bmod m = b \bmod m$$

$$\Updownarrow$$

$$\exists k \in \mathbb{Z} : \; a = b + km \qquad (**)$$

Sætning 4.1.5:

For $a,b,c,d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ gælder

$$\begin{cases} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{cases}$$

$$\Downarrow$$

$$\begin{cases} a+c \equiv b+d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{cases}$$

Primtal

Def:

Def. 4.3.1

Lad $p \in \mathbb{Z}^+ - \{1\}$.
Hvis 1 og p er de eneste tal, der går op i p, er p et primtal.
Ellers er p sammensat.

Aritmetikkens Fundamentalsætning:

Sætning 4.3.1 (Aritmetikkens Fundamentalsætning)

Ethvert heltal $n \geq 2$
kan skrives som et produkt af primtal på præcis én måde

(hvis man sorterer faktorerne efter str.)

Største fælles divisor:

Def. 4.3.2

Lad $a, b \in \mathbb{Z}$, $a \neq 0 \vee b \neq 0$

$\gcd(a,b) = \max\{d \mid d|a \wedge d|b\}$

kaldes **største fælles divisor** for a og b

(greatest common divisor)

Eks:

$\gcd(18,24) = 6$

$18 = \boxed{2 \cdot 3} \cdot 3$

$24 = 2 \cdot 2 \cdot \boxed{2 \cdot 3}$

$\gcd(12,24) = 12$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$24 = 2 \cdot \boxed{2 \cdot 2 \cdot 3}$

$\gcd(12,25) = 1 \Rightarrow$ 12 og 25 er indbyrdes primiske (relatively prime) — Def. 4.3.3

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

Def. 4.3.5

Lad $a, b \in \mathbb{Z}^+$

$\text{lcm}(a,b) = \min\{ m \mid a|m \wedge b|m \}$

kaldes mindste fælles multiplum af a og b

Eks:

$\text{lcm}(18,24) = 72 = 2 \cdot 2 \cdot \boxed{2 \cdot 3} \cdot 3$

$18 = \boxed{2 \cdot 3} \cdot 3$

$24 = 2 \cdot 2 \cdot \boxed{2 \cdot 3}$

$\text{lcm}(12,24) = 24 = 2 \cdot \boxed{2 \cdot 2 \cdot 3}$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$24 = 2 \cdot \boxed{2 \cdot 2 \cdot 3}$

$\text{lcm}(12,25) = 300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

Sætning 4.3.5

Lad $a, b \in \mathbb{Z}^+$. Da gælder

$a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

Euklids Algoritme

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

$$287 = 91 \cdot 3 + 14$$
$$91 = 14 \cdot 6 + 7$$
$$14 = 7 \cdot 2$$

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

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

$\Downarrow$

$d \mid \underbrace{(bq+r)}_{=a}$, 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

□

I eks. m. Euklids Alg. lavede vi disse udregninger:

$$287 = 91 \cdot 3 + 14 \quad (*)$$
$$91 = 14 \cdot 6 + 7 \quad (**)$$
$$14 = 7 \cdot 2$$

Ifølge Lemma 4.3.1 betyder de, 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 en linearkombination af a og b (Sætning 4.3.6):

$$\begin{aligned} 7 &= 91 - 14 \cdot 6, \text{ ifølge } (*) \\ &= 91 - (287 - 3 \cdot 91) \cdot 6, \text{ ifølge } (**) \\ &= 19 \cdot 91 - 6 \cdot 287 \end{aligned}$$

Sætning 4.3.6 kan bl.a. bruges til at bevise Lemma 4.3.2:

Lemma 4.3.2

$$a \mid bc \ \wedge \ \gcd(a,b) = 1 \Rightarrow a \mid c$$

Eks:

$4 \mid 9 \cdot 12 \Rightarrow 4 \mid 12$, da $\gcd(4,9) = 1$

$4 \mid 2 \cdot 18$, men $4 \nmid 18$ $(\gcd(4,2) = 2)$

$4 \mid 2 \cdot 20$, og $4 \mid 20$, selvom $\gcd(4,2) = 2$

Bevis for Lemma 4.3.2:

Antag, at $a \mid bc$ og $\gcd(a,b) = 1$.
Da gælder:

$\exists s,t \in \mathbb{Z}: sa + tb = \gcd(a,b)$, ifølge Sætning 4.3.6.
$\Updownarrow$
$\exists s,t \in \mathbb{Z}: sa + tb = 1$, da $\gcd(a,b) = 1$
$\Downarrow$
$\exists s,t \in \mathbb{Z}: sac + tbc = c$
$\Downarrow$
$a \mid c$, ifølge Kor. 4.1.1, da $a \mid tb$.

□

Af Lemma 4.3.2 følger Lemma 4.3.3, som kan bruges til at bevise unikheds-delen af Aritmetikkens Fundamentalsætning.

Sætning 4.3.7

Hvis $a, b, c \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$, gælder

$$ac \equiv bc \pmod{m} \;\wedge\; \gcd(c,m) = 1$$
$$\Downarrow$$
$$a \equiv b \pmod{m}$$

D.v.s. hvis c går op i både venstreside og højreside og ikke har nogen primtalsfaktorer til fælles med modulus, må man dividere med c på begge sider.

Bevis:

Lad $a, b, c \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$

Antag, at $\gcd(c,m) = 1$

Da gælder:

$$\begin{aligned}
&ac \equiv bc \pmod{m} \\
\Updownarrow\quad &m \mid (ac - bc), \text{ ifølge Def 4.1.3} \\
\Updownarrow\quad &m \mid (a-b)c \\
\Updownarrow\quad &m \mid (a-b), \text{ ifølge Lemma 4.3.2, da } \gcd(c,m) = 1 \\
\Updownarrow\quad &a \equiv b \pmod{m}, \text{ ifølge Def. 4.1.3}
\end{aligned}$$

□

Eks:

$9 \equiv 45 \pmod 4$

$\Downarrow$

$1 \equiv 5 \pmod 4$, da $\gcd(9,4) = 1$

$8 \equiv 20 \pmod 4$, men

$4 \not\equiv 10 \pmod 4$

$12 \equiv 20 \pmod 4$, og

$6 \equiv 10 \pmod 4$, selvom $\gcd(2,4) = 2$

Lineære kongruenser (Afsnit 4.4)

Minder om lineære (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 en kongruens, 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

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

↑ multiplikativ invers til a modulo m

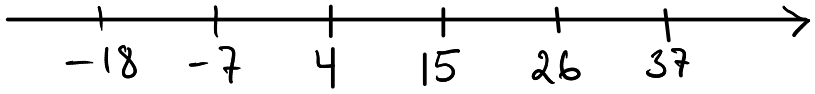
Eks: $4x \equiv 5 \pmod{11}$

$\Uparrow$ følger af Sætning 4.3.7

$\Updownarrow$ $3 \cdot 4x \equiv 3 \cdot 5 \pmod{11}$

$\Updownarrow$ $12x \equiv 15 \pmod{11}$

$\Updownarrow$ $x \equiv 4 \pmod{11}$



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, da et multiplum af 4 divideret med 10 giver en lige rest:

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

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:

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

Heraf fås:

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

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 inverse, jvf. ovenstående eks.

Kongruenssystemer

Eks:

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

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

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

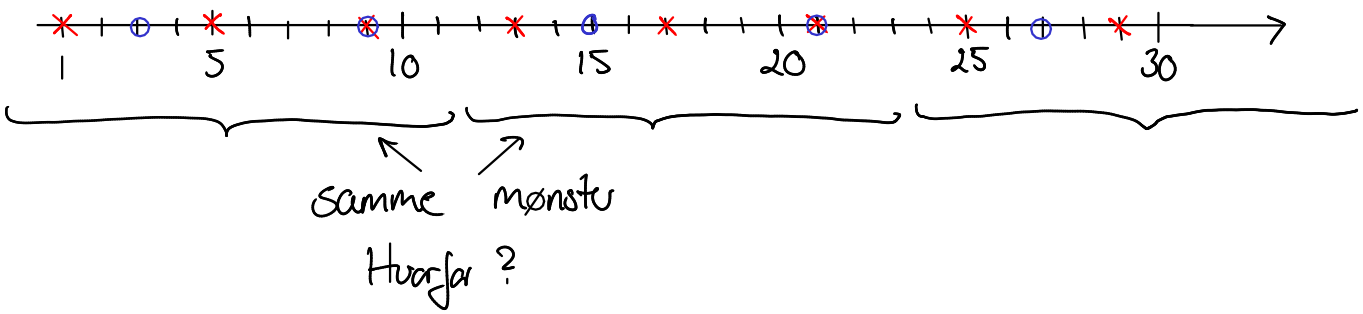
$x = (23)$ er en løsning

Vi vender tilbage til dette eks...

Eks:

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

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



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:

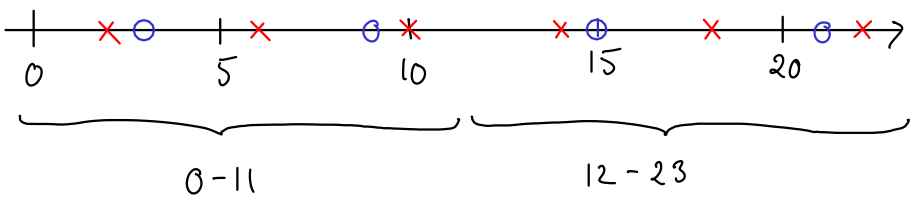
x er en løsning $\Rightarrow$ $\forall k \in \mathbb{Z}: x + 12k$ er en løsning

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 inger løsning.

Bemærk: $\text{lcm}(4,6) = 12$

Generelt:
For n kongruenser med moduli $m_1, m_2, \dots, m_n$
og $l = \text{lcm}(m_1, m_2, \dots, m_n)$ gælder:

$\Updownarrow$ $\exists$ løsning
$\exists$ løsning $\in \mathbb{Z}_l$
$\Updownarrow$ $\exists!$ løsning $\in \mathbb{Z}_l$

$\text{lcm}(m_1, m_2, \dots, m_n)$ 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?