

Sidste gang:

Def. 4.1.1:

$$a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z} \Leftrightarrow b = k \cdot a, k \in \mathbb{Z}$$

Lemma 4.1.1:

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

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

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

Korollar 4.1.1: (opsummerer (i) og (ii))

$$\Downarrow \begin{array}{l} a|b \wedge a|c \\ \forall k_1, k_2 \in \mathbb{Z}: a|(k_1 b + k_2 c) \end{array}$$

$$47 \text{ div } 5 = 9, \quad 47 \bmod \underline{5} = \underline{2} \Leftrightarrow$$

$$47 = 5 \cdot 9 + 2$$

$$-47 \text{ div } 5 = -10, \quad -47 \bmod 5 = 3 \Leftrightarrow$$

$$-47 = 5 \cdot (-10) + 3$$

$$32 \text{ div } 5 = 6, \quad 32 \bmod \underline{5} = \underline{2}$$

$$47 - 32 = 5 \cdot 3 \Rightarrow 47 \equiv 32 \pmod{5}$$

$$a \equiv b \pmod{m}$$

OK at addere (gange med) c på den ene side og d på den anden side, hvis $c \equiv d \pmod{m}$.

(Også OK at trække fra, men ikke altid OK at dividere - heller ikke selvom div. går op.)

Afsnit 4.3 : Primtal

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.

Eks :

Primtal : 2, 3, 5, 7, 11, ...

Sammensat : 4, 6, 8, 9, 10, ...

Sætning 4.3.1 (Aritmetikens Fundamentalsætning) :

Enhvert heltal $n \geq 2$

kan skrives som et produkt af primtal,
og det kan kun gøres på én måde (hvis man
sorterer faktorerne efter størrelse).

Eks :

$$2 = 2$$

$$3 = 3$$

$$4 = 2 \cdot 2$$

$$10 = 2 \cdot 5$$

$$12 = 2 \cdot 2 \cdot 3$$

$$45 = 3 \cdot 3 \cdot 5$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5$$

Basis:

- Eksisterer: (afsnit 5.2, Eks 2)

Stærk induktion:

Basis: $n=2$ er et primtal - OK (produkt med 1 faktor)

Ind. ant.: Alle tal n , $2 \leq n \leq n-1$ kan skrives som et produkt af primtal.

Ind. Skridt: $n \geq 3$

Hvis n er et primtal: OK

Hvis n er sammensat:

$$n = p \cdot q, \quad 1 < p, q < n$$

Ifølge ind. ant. kan p og q skrives som produkter af primtal:

$$p = p_1 p_2 \dots p_k$$

$$q = q_1 q_2 \dots q_l$$

Dermed kan n skrives som et produkt af primtal:

$$n = p_1 p_2 \dots p_k q_1 q_2 \dots q_l$$

- Unik: (sidst i afsnit 4.3)

Øøthning 4.3.2:

Hvis n er sammensat, har n en divisor $\leq \sqrt{n}$.

Beris:

Antag til **modstrid**, at n ikke har en divisor $\leq \sqrt{n}$.

Da n er sammensat, er $n = a \cdot b$, hvor $1 < a, b < n$.

Ifølge antagelsen er $a, b > \sqrt{n}$. D.v.s. $n > \sqrt{n} \cdot \sqrt{n} = n$ ⚡

D.v.s. hvis vi skal teste, om et tal n er et primtal, behøver vi kun at teste faktorer op til $\sqrt{n}$.

Eratosthenes' si (de sammensatte tal drysser igennem - først de sorte, så de røde, og så de blå...)

2 3 5

Sammensatte:

4 6 8 9 10 12 14 15 16 18 20 21 22 24 25

Primtal:

2 3 5 7 11 13 17 19 23

Øøthning 4.3.3: Der er uendeligt mange primtal

Beris: Antag til **modstrid**, kun n primtal $p_1, p_2, \dots, p_n$.

Lad $Q = p_1 p_2 \dots p_n + 1$.

To muligheder:

- Q primtal. Da er der $n+1$ forskellige primtal ⚡
- Q sammensat.

$\exists$ primtal q , så $q \mid Q$.

Bemærk, at $p_i \mid (Q-1)$, for $1 \leq i \leq n$.

q kan ikke gå op i både Q og $Q-1$.

D.v.s. $q \neq p_1, p_2, \dots, p_n$

D.v.s. $n+1$ forskellige primtal. ⚡

} Ikke-konstruktiv eksisterensberis

Men der bliver lægges og lægges imellem dem:

Sætning 4.3.4:

Lad $P(n)$ være # primtal blandt $2, 3, \dots, n$.

$$\lim_{n \rightarrow \infty} \frac{P(n)}{n/\ln n} = 1$$

Største fælles divisor og mindste fælles multiplum
(kender datalogene fra DM534, inkl. Euklids Alg.):

Def 4.3.2:

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

$\gcd(a, b) = \max \{ d \mid d \mid a \wedge d \mid b \}$ kaldes
største fælles divisor for a og b

Eks :

$$\gcd(18, 24) = 6$$

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

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

$$\gcd(12, 24) = 12$$

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

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

$$\gcd(12, 25) = 1 \Rightarrow 12 \text{ og } 25 \text{ er } \underline{\text{indbyrdes primiske}} \\ (\text{Def 4.3.3})$$

$$12 = 2 \cdot 2 \cdot 3$$

$$25 = 5 \cdot 5$$

Def. 4.3.5:

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

$\text{lcm}(a, b) = \min \{ m \mid a \mid m \wedge b \mid m \}$ kaldes
mindste fælles multiplum af a og b

Eks:

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

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

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

$$\text{lcm}(12, 24) = 24$$

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

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

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

$$12 = 2 \cdot 2 \cdot 3$$

$$25 = 5 \cdot 5$$

Sætning 4.3.5:

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

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

Lemma 4.3.2:

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

Bevisstrategi:

a og b har ingen primtalsfaktorer til fælles.
D.v.s. alle a 's primtalsfaktorer må findes i c .

Lemma 4.3.3:

p primtal

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

$$p|a_1 a_2 \dots a_n \Rightarrow \exists i: p|a_i$$

Bevis: Opgave 5.1.52

Hvis p ikke er et primtal, gælder impl. ikke nødvendigvis.
Eks: $4|6 \cdot 10$, men $4 \nmid 6$ og $4 \nmid 10$.

Sætning 4.3.7:

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

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

D.v.s. hvis c går op i både h.s. og v.s. og c ikke har nogen primtalsfaktorer fælles med m , må vi dividere med c på begge sider.