

Sidste gang

Euklids Algoritme

Eks:

$$\gcd(20, 67) = 1;$$

$$(*) \quad 67 = 20 \cdot 3 + 7$$

$$(**) \quad 20 = 7 \cdot 2 + 6$$

$$(***) \quad 7 = 6 \cdot 1 + \textcircled{1}$$

$$6 = 1 \cdot 6$$

$$\left. \begin{array}{l} (*) \\ (**) \\ (***) \end{array} \right\} \Rightarrow \begin{array}{l} \textcircled{1} = 7 - 6 \\ = 7 - (20 - 7 \cdot 2) = 7 \cdot 3 - 20 \\ = (67 - 20 \cdot 3) \cdot 3 - 20 = 67 \cdot 3 - 20 \cdot 10 \end{array}$$

D.v.s.

$$67 \cdot 3 \equiv 1 \pmod{20} \quad \text{og}$$

$$20 \cdot (-10) \equiv 1 \pmod{67}$$

Har $ax \equiv b \pmod{m}$ en løsning?

Hvis $\gcd(a, m) = 1$: ja (for da $\exists \bar{a} \in \mathbb{Z}: a\bar{a} \equiv 1 \pmod{m}$)

Ellers: Måske

$\uparrow$
multiplikativ invers til a modulo m

Kongruenssystemer

Eks:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

Har ifølge KRS præcis en løsning modulo $3 \cdot 5 \cdot 7$,
da $\gcd(3, 5) = \gcd(3, 7) = \gcd(5, 7) = 1$.

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

$$M_1 = 35, \quad M_2 = 21, \quad M_3 = 15$$

$$2 \cdot 35 \equiv 1 \pmod{3}$$

$$1 \cdot 21 \equiv 1 \pmod{5}$$

$$1 \cdot 15 \equiv 1 \pmod{7}$$

$$x = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233 = 23 + 2 \cdot 105$$

Løsningsmængde: $\{23 + 105k \mid k \in \mathbb{Z}\}$

NB: Der kan godt være en løsning, selvom moduli ikke er parvis indbyrdes primiske, men da kan ovenstående løsningsmetode ikke anvendes.

Fermats lille Sætning (1) kan, sammen med KRS, bruges til at bevise, at RSA virker

Fermats Lille Sætning (Sætning 4.4.3)

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

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

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

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

11 er et primtal og går ikke op i 7.

D.v.s. vi kan bruge Sætning 3(1) med $a=7, p=11$:

$$7^{10} \equiv 1 \pmod{11} \quad (*)$$

$$7^{222} = 7^{10 \cdot 22 + 2} = 7^{10 \cdot 22} \cdot 7^2 = (7^{10})^{22} \cdot 7^2$$

D.v.s.

$$7^{222} \pmod{11} = (7^{10})^{22} \cdot 7^2 \pmod{11}$$

$$\stackrel{(*)}{=} 1^{22} \cdot 7^2 \pmod{11}, \text{ ifølge Sætning 3(1) og Korollar 4.1.2}$$

$$= 49 \pmod{11}$$

$$= 5$$

Følger og rækker (afsnit 2.4)

Følge (sequence/progression)

Ordnet mængde /
funktion fra (en delmængde af) $\mathbb{N}$

Eks: Fibonacci-tallene (uendelig følge)

0, 1, 1, 2, 3, 5, 8, 13, ...

$$f_0 = 0$$

$$f_1 = 1$$

$$f_n = f_{n-2} + f_{n-1}, \text{ for } n \geq 2$$

ingen dør
Hvert par, som var der allerede for to måneder siden, får et par unger.

Modellerer # kaniner på en ø:

- Et par sættes på øen ved starten af første måned
- Fra et par er to måneder, får de et par unger hver måned
- Ingen kaniner dør

Eks: $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$ (uendelig følge)

$$f(n): \mathbb{N}^+ \rightarrow \mathbb{Q}^+, \quad f(n) = \frac{1}{n}$$

$$a_n = \frac{1}{n}, \quad n \in \mathbb{N}^+ \quad (n\text{'te led})$$

$$\{a_n\} = 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots \quad (\text{helt sekvensen})$$

konflikt med mængdenotation

Eks: $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots$

(uendelig følge)

$$a_n = \left(\frac{1}{2}\right)^n, \quad n \in \mathbb{N}$$

Eller rekursiv def:

$$a_0 = 1$$

$$a_n = \frac{1}{2} \cdot a_{n-1}, \quad \text{for } n \geq 1$$

Eks på:

Geometrisk følge

$a, ar, ar^2, \dots$

$$a_n = a \cdot r^n, \quad n \in \mathbb{N}$$

begyndelsesled $\nwarrow$ $\swarrow$ fælles faktor

Eksempel fra før: $a=1, r=\frac{1}{2}$

Aritmetrisk følge

$a, a+d, a+2d, \dots$

$$a_n = a + nd, \quad n \in \mathbb{N}$$

begyndelsesled $\nwarrow$ $\swarrow$ fælles forskel

Eks: $1, 3, 5, 7, \dots$

$$a=1, d=2$$

Eks: Mandibrot - følge

Defineret for hvert $c \in \mathbb{C}$:

$$X_0 = 0$$

$$X_n = X_{n-1}^2 + c, \quad n \geq 1$$

c tilhører Mandibrot-mængden,
hvis $\{X_n\}$ er begrænset

i tilhører Mandibrot-mængden:

$$X_1 = 0^2 + i = i$$

$$X_2 = i^2 + i = i - 1$$

$$X_3 = (i-1)^2 + i = -1 + 1 - 2i + i = -i$$

$$X_4 = (-i)^2 + i = i - 1 = \underline{X_2}$$

$$X_5 = X_3$$

$$X_6 = X_4 = X_2$$

$\vdots$

D.v.s.

$\{X_n\}$ er begrænset

Escape condition: $|X_n| > 2$

Jo hurtigere escape, jo lysere farve.

Man kan også lægge ledene i en følge sammen:

Række (summation / series)

Sum af et uendeligt (eller endeligt) # led

Eks: $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots$

Geometrisk række: $\sum_{i=0}^n ar^i$

$a=1, r=\frac{1}{2}$

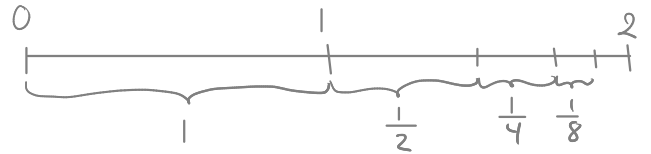
$n=1: 1 + \frac{1}{2} = 2 - \frac{1}{2}$

$n=2: 1 + \frac{1}{2} + \frac{1}{4} = 2 - \frac{1}{4}$

$n=3: 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} = 2 - \frac{1}{8}$

$\sum_{i=0}^n \left(\frac{1}{2}\right)^i = 2 - \left(\frac{1}{2}\right)^n$

$\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i = 2$



Mer generelt:

Tabel 2, linie 1:

$\sum_{i=0}^n r^i = \frac{r^{n+1} - 1}{r - 1}, \quad \text{for } r \neq 1 \quad (= n+1, \text{ for } r=1)$

D.v.s.

$\sum_{i=0}^n 2^i = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1$

Illustration: (binære tal)

$i=0$	1
$i=1$	10
$i=2$	100
$i=3$	1000
	1111

$= 10000 - 1$

$r=3$:

Ternære tal:

$2 \cdot 3^0:$	2
$2 \cdot 3^1:$	20
$2 \cdot 3^2:$	200
$2 \cdot 3^3:$	2000
	2222

$= 10000 - 1$