

Afsnit 4.3, s. 266: Euklids Algoritme

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

$$287 = 91 \cdot 3 + 14$$

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

$$14 = 7 \cdot 2 + 0$$

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

Check: $91 = 7 \cdot 13$

$$287 = 7 \cdot 41$$

Hvorfør virker det?

Lemma 1:

Hvis $a = bq + r$, hvor $a, b, q, r \in \mathbb{Z}$,
da er $\gcd(a, b) = \gcd(b, r)$.

Bevis:

Vil vise, at $\gcd(a, b) = \gcd(b, r)$.

(dvs a og b har de samme divisorer til fælles
som b og r)

$$\gcd(b, r) \leq \gcd(a, b):$$

$$d \mid b \wedge d \mid r \Rightarrow d \mid (qb + r), \text{ ifølge Kor. 4.1.1} \\ \Leftrightarrow d \mid a$$

$$\gcd(a, b) \leq \gcd(b, r):$$

$$d \mid a \wedge d \mid b \Rightarrow d \mid (a - qb), \text{ ————— " —————} \\ \Leftrightarrow d \mid r \quad \square$$

Ifølge Lemma 1 betyder udregningene ovenfor, 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 linear-kombination af a og b . (Sætning 6)

I eks. ovenfor:

$$\begin{aligned}7 &= 91 - 14 \cdot 6 \\ &= 91 - (287 - 3 \cdot 91) \cdot 6 \\ &= 91 - 6 \cdot 287 + 18 \cdot 91 \\ &= 19 \cdot 91 - 6 \cdot 287\end{aligned}$$

Hvornår kunne vi være interesserede i det?

Hvis vi f.eks. gerne vil finde en multiplikativ invers:

$$a\bar{a} \equiv 1 \pmod{m}$$

$\bar{a}$ eksisterer, hvis $\gcd(a, m) = 1$

$$1 = sa + tm, \quad s, t \in \mathbb{Z} \quad \Rightarrow$$

$$1 \equiv sa \pmod{m}$$

Euklids Udvidede Algoritme beregner s og t nemmere end ved at regne baglæns.

Mer om det i DM534...

Følger & rækker (afsnit 2.4)

Følge: (Sequence/progression)

Ordnet mængde/

Funktion fra (delmængde af) $\mathbb{N}$

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

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

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

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

↑ konflikt med mængdenotation

Eks: Fibonacci-tallene (uendelig følge)

$$1, 1, 2, 3, 5, 8, 13, \dots$$

$$f_0 = f_1 = 1$$

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

hver par, som var der allerede for to måneder siden, får et par unger.
Modeller # 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: $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots$ (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: $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$ (endelig følge)

Eks på:

Geometrisk følge:

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

$$a_n = ar^n, \quad n \in \mathbb{N}$$

begyndelsesled

følles 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

følles 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 endeligt eller uendeligt # led.

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

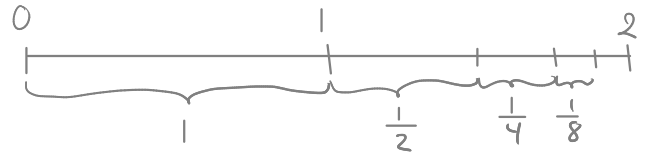
Geometrisk række: $\sum_{i=0}^n ar^i$

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

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

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

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



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

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

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.U.S.

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

Illustration: (binære tal)

$$\begin{array}{r} i=0 \\ i=1 \\ i=2 \\ i=3 \\ \hline \end{array} \begin{array}{r} 1 \\ 10 \\ 100 \\ 1000 \\ \hline \end{array} = 10000 - 1$$

r=3:

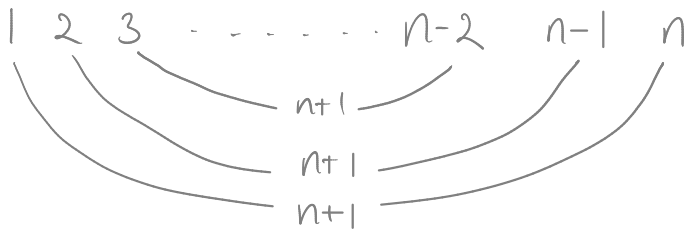
Ternære tal:

$$\begin{array}{r} 2 \cdot 3^0: \\ 2 \cdot 3^1: \\ 2 \cdot 3^2: \\ 2 \cdot 3^3: \\ \hline \end{array} \begin{array}{r} 2 \\ 20 \\ 200 \\ 2000 \\ \hline \end{array} = 10000 - 1$$

Aritmetrisk række:

$$\begin{aligned}\sum_{i=0}^n (a+id) &= (n+1)a + d \sum_{i=0}^n i \\ &= (n+1)a + d \frac{n(n+1)}{2}\end{aligned}$$

Tabel 2, s. 166
2. linie



Bevis tidligere i
kurset v.h.a. induktion

n lige:

$\frac{n}{2}$ par med sum $n+1$

n ulige:

$\frac{n-1}{2}$ par med sum $n+1$

Midtvorte tal: $\frac{n+1}{2}$

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

Eks:

$$\begin{aligned}1 + 3 + 5 + 7 + \dots + 2n+1 &= \sum_{i=0}^n (1+2i) \\ &= (n+1) \cdot 1 + 2 \cdot \frac{n(n+1)}{2} \\ &= n+1 + n(n+1) \\ &= (n+1)(n+1) \\ &= n^2 + 2n + 1\end{aligned}$$

Summer dukker f.eks. op, når vi skal beregne #gennemløb af et loop (for at analysere køretid af en algoritme):

for $i := 1$ to 10

 for $j := 1$ to 20

 ...

$$\# \text{gennemløb} = 10 \cdot 20 \left(= \sum_{i=1}^{10} 20 \right) = 200$$

for $i := 1$ to 10

 for $j := 1$ to i

 ...

$$\# \text{gennemløb} = \sum_{i=1}^{10} i = \frac{10 \cdot 11}{2} = 55$$

for $i := 5$ to 10

 for $j := 1$ to i

 ...

$$\# \text{gennemløb} = \sum_{i=1}^{10} i - \sum_{i=1}^4 i = 55 - \frac{4 \cdot 5}{2} = 45$$

For $i:=1$ to 3

For $j:=1$ to i

For $k:=1$ to j

...

$$\# \text{ gemmed } = \sum_{i=1}^3 \sum_{j=1}^i j = \sum_{i=1}^3 \frac{i(i+1)}{2}$$

$$= \sum_{i=1}^3 \frac{i^2 + i}{2} = \frac{1}{2} \sum_{i=1}^3 i^2 + \frac{1}{2} \sum_{i=1}^3 i$$

Table 2, Line 2 of 3

$$= \frac{1}{2} \left(\frac{3 \cdot 4 \cdot 7}{6} \right) + \frac{1}{2} \frac{3 \cdot 4}{2}$$

$$= 7 + 3 = 10$$

Notation:

$$\sum_{i=1}^5 i = \sum_{1 \leq i \leq 5} i = \sum_{i \in A} i, \text{ hvor } A = \{1, 2, 3, 4, 5\}$$