Euklids algoritme:

$37 = 5 \cdot \underline{7} + \underline{2}$

$7 = 2 \cdot \underline{3} + \underline{1} \leftarrow$

$1 = 7 - 3 \cdot 2$

$1 = 7 - 3 \cdot (37 - 5 \cdot 7)$

$1 = 16 \cdot 7 - 3 \cdot 37$

Fermat's lille Teorem

p = primtall og a = heltall

Da er: $a^p \equiv a \pmod p$

Hvis p = primtall og $a \in \{1, 2, \ldots, p-1\}$

Da er: $a^{p-1} \equiv 1 \pmod p$

Eksempel: Finn a i $2^{50} \equiv a \pmod{17}$

$2^{50} = 2^{16 \cdot 3 + 2} = (2^{16})^3 \cdot 2^2$

$2^{50} \equiv (2^{16})^3 \cdot 2^2 \mod 17$ (vi vet at $2^{17-1} \equiv 1 \mod 17$)

$2^{50} \equiv (1)^3 \cdot 4 \equiv \underline{\underline{4}} \mod 17$

Relasjoner

Snakker om relasjonen R

Refleksivitet: $(a,a) \in R$ for alle $a \in A$

Symetrisk: $(b,a) \in R \iff (a,b) \in R$

Transitiv: $(a,b) \in R$ og $(b,c) \in R$ medfører $(a,c) \in R$

Ekvivalensrelasjon: R er Refleksiv, Symmetrisk og transitiv

Ant. Symmetrisk: $(a,b) \in R$ og $(b,a) \in R$, så $a = b$

Irrefleksiv: en relasjon hvor ingenting er relatert til seg selv

Ordninger

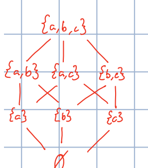
Partiell Ordninger:

En binær relasjon på mengden S er en partiell ordning hvis den er refleksiv, transitiv og anti-symmetrisk.

Total ordning:

En partiell ordning R på en mengde S kalles en total ordning hvis det for alle x og y i S er slik at xRy eller yRx.

Hasse diagram



De Morgan's Law

$\neg(A \land B) \iff (\neg A \lor \neg B)$

$\neg(A \lor B) \iff (\neg A \land \neg B)$

$\neg(P \to Q) \iff P \land \neg Q$

Kinesisk rest teorem

$x \equiv a_1 \mod m_1$
$x \equiv a_2 \mod m_2$
$x \equiv a_n \mod m_n$

$M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$

$M_1 = M / m_1$
$M_2 = M / m_2$
$M_n = M / m_n$

Dersom $\gcd(m_1, m_2) = 1$ finnes det en entydig løsning for å finne x

$$\left.\begin{aligned} M_1 \cdot y_1 &= 1 \mod m_1 \\ M_2 \cdot y_2 &= 1 \mod m_2 \\ M_n \cdot y_n &= 1 \mod m_n \end{aligned}\right\} \text{løser kongruensen for å finne } y_n$$

$A = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots + a_n \cdot M_n \cdot y_n$

$x \equiv A \mod M$

RSA-kryptering

$n = (p-1) \cdot (q-1)$

$d = \gcd(e, n)$

$e \cdot d \mod n = 1$

Rask eksponentiering

$1605^{311} \mod 2537$

$1605^{311} = 1605^{256+32+16+4+2+1}$

$1605^2 = 2576025 \equiv 970 \mod 2537$

$1605^4 = (1605^2)^2 = 970^2 = 940900 \equiv 2210 \mod 2537$

$1605^8 = (1605^4)^2 = 2210^2 \ldots$

For å løse ganger vi så svarene i lag fra originale uttrykk

$(1605)^{256} \cdot (1605)^{32} \cdot (1605)^{16} \cdot (1605)^4 \cdot (1605)^2 \cdot (1605)^1 \mod 2537$

$\equiv 1178 \cdot 784 \cdot 1090 \cdot 2210 \cdot 970 \cdot 1605 \mod 2537$

$\equiv 3463593359067680000 \mod 2537$

$\equiv \underline{812} \mod 2537$

Binomialkoeffisient

$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$ "n velg k"

$\binom{n}{k} = \binom{n}{n-k}$

$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

$\binom{10}{4} = \frac{10!}{(10-4)! \cdot 4!} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot \cancel{6!}}{\cancel{6!} \cdot 4!} = \frac{5040}{24} = 210$

$\binom{10}{4} = \binom{10}{6}$

$\binom{11}{4} = \binom{10}{3} + \binom{10}{4}$

Inklusjon-eksklusjonsprinsippet

For to mengder:

$|A \cup B| = |A| + |B| - |A \cap B|$

For tre mengder

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Multiplikasjonsprinsippet

To hendelser med m, n muligheter $= m \cdot n$

M av n: $\binom{n}{m} = \frac{n!}{m! \cdot (n-m)!}$

Dueslagsprinsippet

Vi har k esker og N objekter, da fins minst en eske som inneholder minst $\lceil N/k \rceil$ objekter.

$\lceil 3400/8 \rceil = 425$, minst 1 av 8 har over 425

Matematisk induksjon

1. Sjekker om $P(1)$ er sann
2. Setter inn $P(k)$
3. Setter inn $P(k+1)$ i formlene
4. Plusser på leddet for $P(k+1)$ i likningen for $P(k)$
5. Regner det ut og sjekker om summen fra punkt 4 er lik summen fra punkt 3

$(0+1) \cdot 2^0 + \ldots + (n+1) \cdot 2^n = n \cdot 2^{n+1} + 1$

1. $P(0) = (0+1) \cdot 2^0 = 0 \cdot 2^{0+1} + 1$, $1 = 1$ Sant

2. $P(k) = (k+1) \cdot 2^k = k \cdot 2^{k+1} + 1$

3. $P(k+1) = (k+2) \cdot 2^{k+1} = (k+1) \cdot 2^{k+2} + 1$

4. $+ \ldots + (k+1) \cdot 2^k = k \cdot 2^{k+1} + 1$

$+ \ldots + (k+1) 2^k + (k+2) \cdot 2^{k+1} = k \cdot 2^{k+1} + 1 + (k+2) \cdot 2^{k+1}$

5. $= k2^{k+1} + 1 + (k+2) \cdot 2^{k+1}$

$= k2^{k+1} + 1 + k2^{k+1} + 4^{k+1}$

$= 2k2^{k+1} + 4k^{k+1} + 1$

$= 2 \cdot (k+1) 2^{k+1} + 1$

$= (k+1) \cdot 2^{k+1+1} + 1$

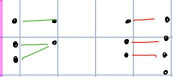
$= (k+1) \cdot 2^{k+2} + 1$

Ser at svaret stemmer overens med svaret i punkt 3 og har da bevist at den stemmer for $(k+1)$ om vi antar at den stemmer for $p(k)$

Surjektiv funksjon

En funksjon $f: A \to B$ er surjektiv hvis det for alle $y \in B$, finnes en $x \in A$ slik at $f(x) = y$. Vi sier i så fall at f er en surjeksjon og på.

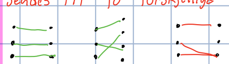
En surjektiv funksjon treffer alt i verdiområdet



Injektiv funksjon

En funksjon $f: A \to B$ er injektiv hvis det for alle elementer x og y i A er slik at hvis $x \neq y$, så er $f(x) \neq f(y)$. Vi sier i så fall at f er en injeksjon og en-til-en.

Injeksjon betyr at to forskjellige elementer sendes til to forskjellige elementer:



Komposisjon av relasjoner

$R: A \to B$ og $S: B \to C$

Sammensatt relasjon $S \circ R: A \to C$

gitt ved

$S \circ R = \{(a,c) \mid (\exists b \in B)((a,b) \in R \land (b,c) \in S)\}$

Binær relasjon

Binær relasjon på A er relasjonen $R: A \to A = A \times A$

Eks: Relasjoner på $[3] = \{1, 2, 3\}$

$id_{[3]} = \{(1,1), (2,2), (3,3)\}$???

Sannhetstabell

F	G	F∧G
1	1	1
1	0	0
0	1	0
0	0	0

F	G	F∨G
1	1	1
1	0	1
0	1	1
0	0	0

P	Q	R	P	→	Q	(P	∨R)	→	Q
1	1	1	1	1	1	1	1	1	1
1	0	1	1	0	0	1	1	0	0
0	1	1	0	1	1	0	1	1	1
0	0	1	0	1	0	0	1	0	0
1	1	0				1	0	1	1
1	0	0				1	0	0	0
0	1	0				0	0	1	1
0	0	0				0	0	1	0

Kinesisk rest teorem for 2 kongruenser

$x \equiv a \mod m$

$x \equiv b \mod n$

Krav: $GCD(m,n) = 1$

Det finnes heltall u og v slik at

$m \cdot u \equiv 0 \mod m$ $\quad n \cdot v \equiv 1 \mod m$

$m \cdot u \equiv 1 \mod n$ $\quad n \cdot v \equiv 0 \mod n$

Vi finner u og v ved å bruke Euklids Algoritme på $m \cdot u + n \cdot v = 1$

Da kan vi finne c

$c = a \cdot n \cdot v + b \cdot m \cdot u$

$x \equiv c \mod_{m \cdot n}$

Grafer

node - hver prikk i en graf

kant - strek mellom to noder

grad - antall kanter koblet til noden

Isomorfi

La G og H være to grafer. En isomorfi fra G til H er en bijektiv funksjon f fra nodene i G til nodene i H som er slik at naboene u og v er naboer i G h.b.h. nodenene $f(u)$ og $f(v)$ er naboer i H.

Euler krets

En Eulerkrets er når vi starter og slutter i samme node. Kravet er at vi må ha partall grad på alle nodene

Euler sti:

Når vi starter og slutter i forskjellige noder som begge har oddetall grad.

Permutasjon

En permutasjon av en mengde er en ordning av elementene i den. Hvis vi allerede har en ordning, er en permutasjon en endring av rekkefølgen.

En permutasjon av mengden M er en bijeksjon fra M til M.

Poset

Et partiell ordnet sett er et set satt i lag med en partiell ordning på det. Et partiellt ordnet sett er definert som et ordnet parr $P = (X, \leq)$, hvor X er grunnsettet av P og $\leq$ er den partielle ordningen på P.

Rekursjon

Hvis en mengde M er induktivt definert, kan vi definere en funksjon rekursivt f med definisjonsområdet M på følgende måte:

- For hvert element x i basismengden til M, spesifiserer en verdi for $f(x)$. Dette kalles basissteget eller basistilfellet for funksjon
- For hvert element x i M som fremkommer i et induksjonssteg, definerer verdien til $f(x)$ ved å bruke de tidligere definerte verdiene for f. Dette kalles rekursjonssteget.

$d(1) = d(0) + 2 = 0 + 2 = 2$

$d(2) = d(1) + 2 = 2 + 2 = 4$

$d(3) = d(2) + 2 = 4 + 2 = 6$

Partisjon

En partisjon av en mengde S er en mengde X av ikke-tomme delmengder av S slik at følgende betingelser holder:

- Unionen av alle mengdene i X er lik S
- Snittet mellom to forskjellige mengder fra X er tomt

Hvis $S_1, S_2, \dots, S_n$ er ikketomme delmengder av S, S er lik $S_1 \cup S_2 \cup \dots \cup S_n$, og for alle S_i og S_j slik at $i \neq j$ er det slik at $S_i \cap S_j = \emptyset$, er $\{S_1, S_2, \dots, S_n\}$ en partisjon av S.

Kardinalitet

To mengder M og N har lik kardinalitet hvis det finnes en en-til-en korrespondanse mellom elementene i M og N. Vi skriver $|M| = |N|$ når det er tilfellet. Mengden M har kardinalitet mindre enn eller lik N hvis det finnes en en-til-en korrespondanse mellom M og en delmengde av N. Vi skriver $|M| \leq |N|$ når det er tilfellet. Hvis M er en endelig mengde, er kardinaliteten til M lik antall elementer i M, og i så fall bruker vi notasjonen $|M|$ for antall elementer i M.

$M = \{1, 2, 3\}$ $N = \{a, b, c\}$

bijeksjon $f: M \to N$

$f(1) = a$, $f(2) = b$, $f(3) = c$

$1 \to a$

$2 \to b$

$3 \to c$

Tellbar

En uendelig mengde M er tellbar hvis det er en en-til-en korrespondanse mellom elementene i M og de naturlige tallene. Hvis ikke, er M overtellbar. Alle endelig mengder er tellbare.

Shröder-Bernstein theorem

hvis vi har to injektive funksjoner $f: A \to B$ og $g: B \to A$ mellom settene A og B, da finnes det en bijektiv funksjon $h: A \to B$.