|  |  |  |
| --- | --- | --- |
| **Navn** | **leses** | **symbol** |
| Negasjon | Ikke | ¬ |
| Konjunksjon | Og | ∧ |
| Disjunksjon | Eller | ∨ |
| Eksklusiv eller | Xor | ⊕ |
| Implikasjon | Impliserer (medfører) | ⇒ |
| Bi-implikasjon | Hvis og bare hvis | ⇔ |

**Oppgave 6. Eksamen 2017**

15 personer skal deles i grupper på 5.

a) **Hvor mange slike inndelinger fins det?**



b) **Are og Britt er blant de 15 personene. Hva er sannsynligheten for at de havner i same gruppe?**

Are og Britt i samme gruppe:



Sannsynligheten for blir derfor:



|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **p** | **q** | **r** | **q∧r** | **p∨( q∧r)** | **p∨q** | **p∨r** | **(p∨q)∧(p∨r)** |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **p** | **q** | **¬p** | **¬q** | **p∧q** | **p∨q** | **p⊕q** | **p⇒q** | **p⇔q** | **¬q**∧( **p∨q**) | **¬**( **p**⇒**q**) |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |

**Differenslikning/Rekursjonslikning**

Lineær homogen differenslikning:

an = C1an-1 + C2an-2 + ... + Ckan-k

**Fremgangsmåte:**

1. Skrive likningen som en andregradslikning
2. abc-formel = r1 og r2
3. an = C1(r1)n + C2(r2)n
4. Finner to enkle uttrykk:

a0 = C1(r1)0 + C2(r2)0  = C1 + C2

a1 = C1(r1)1 + C2(r2)1  = C1\*r1+ C2\*r2

1. Løse for en C

C1 = a0 - C2

1. Sette inn i den andre likningen.

1. Når C1 og C2 er kjent:

an = C1(r1)n + C2(r2)n

**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.

Eks: +…+ (n+1)2n = n\*2n+1 +1

1. P(0)

(0+1)20 = 0\*20+1+1

1 = 1 🡪 stemmer for P(0)

2. P(k)

(k+1)2k = k\*2k+1+1

3. P(k+1)

(k+2)2k+1 = (k+1)\*2k+2 +1

4.

+…+(k+1)2k = k\*2k+1+1

+…+(k+1)2k +(k+2)2k+1 = k\*2k+1+1+(k+2)2k+1

5.

= k2k+1+1+(k+2)2k+1

= k2k+1 + 1 + k2k+1 + 4k+1

= 2k2k+1 + 4kk+1 + 1

= 2(k+1)2k+1 +1

= (k+1)2k+1+1+1

= (k+1)\*2k+2 +1 🡪 ser at dette stemmer med 3. og har derfor bevist at den stemmer for (k+1) om vi antar at den stemmer for p(k).

**Matrise**

Matrisemultiplikasjon:

MR[1] = • MR[1] =

= MR[2] =

Dersom MR[n] = MR[n-1] vil alle matriser etter MR[n-1] være lik.

**Fermats lille teorem:**

P = primtall

aP-1 = 1 (mod p)

**Eks.** 220182018mod 11

P = 11

211-1 = 1 mod 11

Trick:

20182018/11-1 = 2018201 + 8

(210)2018201 = 12018201mod 11

28(220182010) = 28 mod 11

220182018 = 3 mod 11

**Kinesisk restteorem**

X = a1 mod m1

X = a2 mod m2

X = an mod mn

M = m1\*m2\*…\*mn

M1=M/ m1

M2=M/ m2

Mn=M/ mn

Dersom gcd(m1,m2) = 1 fins en entydig løsning for å finne x

M1y1 = 1 mod m1

M2y2 = 1 mod m2 – Euklids algoritme

Mnyn = 1 mod mn

Tilbakesubstitusjon gir y1, y2… yn

X = a1M1y1+ a2M2y2+…+ anMnyn (mod M)

For å teste om vi har riktig x kan man sette inn x i uttrykkene øverst.

**Rask ekponentiering (modular exponentiation)**

**Merk:** Ikke samme som Euklids algoritme

**Eks.**

**572 mod 73**

|  |  |  |
| --- | --- | --- |
|  | **Power (potens)** | **X** |
| 72 = 36\*2 + 0 | 5 | 1 |
| 36 = 18\*2 + 0 | 52 mod 73 = 25 | 1 |
| 18 = 9\*2 + 0 | 252 mod 73 = 41 | 1 |
| 9 = 4\*2 + 1 | 412 mod 73 = 2 | 2\*1 mod 73 = 2 |
| 4 = 2\*2 + 0 | 22 mod 73 = 4 | 2 |
| 2 = 1\*2 + 0 | 42 mod 73 = 16 | 2 |
| 1 = 0\*2 +1 | 162 mod 73 = 37 | 37\*2 mod 73 = 74 |

**74 mod 73 = 1**

**572 mod 73 = 1**

**Euklids algoritme**

**gcd(**29, 37**)**

37 = 29\*1 + 8

29 = 8\*3 + 5

8 = 5\*1 +3

5 = 3\*1 + 2

3 = 2\*1 +**1 –** gcd = 1

2 = 1\*2 + 0

**Tilbakesubstitusjon**

1 = 3 - 2

= 3 - (5-3)

= 2(3) - 5

=2(8-5) - 5

=2(8) - 3(5)

=2(8) – 3(29-8\*3)

=11(8) – 3(29)

= 11(37-29) – 3(29)

=11(37) – 14(29)

**Finne d i RSA**

d = gcd(e, (p-1)(q-1))

e\*d mod (p-1)(q-1) = 1

**Inklusjons- eksklusjonsprinsippet**

**For to mengder:**

|A∪B|=|A|+|B|-|A∩B|

**For tre mengder:**

|A∪B∪C|=|A|+|B|+|C|-|A∩B|-|A∩C|-|B∩C|+ |A∩B∩C|

**Multiplikasjonsprinsippet**

To hendelser med m, n muligheter = m\*n

M av n: =

**Dueslagsprinsippet**

Vi har k esker og N objekter, da fins minst en eske som inneholder minst objekter.

EKS: Det er 8 fakulteter ved UiT og mer enn 3400 faglig ansatte. Da må det finnes minst ett fakultet med mer enn = 425 ansatte

**Grafer**

**Eulersti**: benytter alle kantene i grafen en gang

**Eulersykel:** eulersti som ender opp i startpunktet

(en sammenhengende multigraf med minst to hjørner har en eulersykel hvis og bare hvis alle hjørner er av lik grad. En sammenhengende multigraf har en **Eulersti**, men ikke en Eulersykel hvis det er nøyaktig **to** hjørner av odde grad)

**Finne korteste veg (Djikstras algoritme):**

Et bilde som inneholder skjermbilde

Automatisk generert beskrivelseEt bilde som inneholder skjermbilde

Automatisk generert beskrivelse

**Relasjon = R**

(mengden A)

**Refleksiv:** (a,a) ∈ R for alle a ∈ A

**Symetrisk:** (b,a) ∈ R ⇔ (a,b) ∈ R

**Transitiv:** (a,b) ∈ R og (b,c) ∈ R medfører (a,c) ∈ R

**Union:** R1 U R2 = legger til alle relasjoner

**Snitt:** R1 ∩ R2 = kun like relasjoner

**Differens:** R1 - R2 = R1-( R1 ∩ R2)

**XOR:** R1 **⊕** R2 = legger til eksklusive relasjoner

**Ekvivalensrelasjon:** Dersom refleksiv, symetrisk og transitiv

**Ekvivalensklasse:** forteller hvilke relasjoner [a] har

[a] = {s | (a, s) ∈ R}

Ekvivalensklassene utgjør en **partisjon** av A.