naturvitenskapelige universitet
Institutt for matematiske fag

Faglig kontakt under eksamen:
Finn Knudsen 73 59 35 23

EKSAMEN I FAG SIF5015 DISKRET MATEMATIKK

Onsdag 2. august 2000
Tid: 0900–1400

Hjelpemidler: Typegodkjent kalkulator med tomt minne tillatt.
Ingen trykte eller håndskrevne hjelpemidler tillatt.

Sensuren faller i uke 36.

Oppgave 1 Finn en så enkel som mulig formel på disjunktiv normalform, som er ekvivalent med formelen

$(p \wedge ((\neg q) \to r)) \oplus ((\neg p) \to (q \oplus (\neg r)))$.

Oppgave 2

E	A	C
B	D	D

A	E	A
B	B	C

E	E	C
D	A	B

Vi skal se på skilt av typen vist over. Bokstavene som kan benyttes er A, B, C, D eller E. La U være mengden av skilt som har minst to like bokstaver i første rad, og la V være mengden av skilt som ikke har bokstaven A i siste kolonne. Finn antall skilt i mengdene U, V, $U \cap V$ og $U \cup V$.

Oppgave 3

a) Finn alle hele tall x som tilfredsstiller $16x - 2 \equiv 15 - 3x \pmod{241}$.

b) Finn alle tall x med $100 \leq x < 1000$, som tilfredsstiller

$x \equiv 4 \pmod{7}$,
$x \equiv 5 \pmod{8}$,
$x \equiv 1 \pmod{9}$.

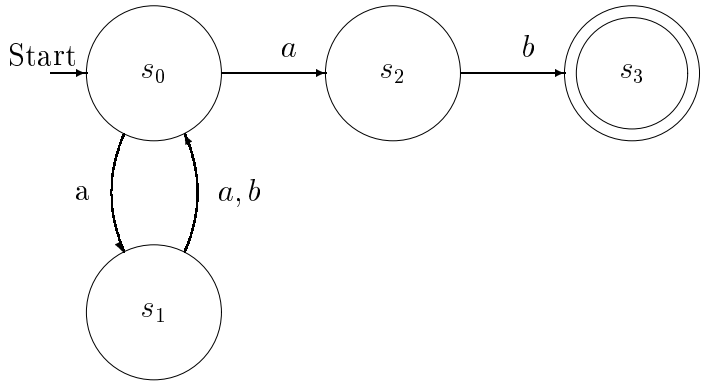
c) Beregn tallet $x = 235^{72723} \bmod 241$.

Oppgave 4 La relasjonen R på mengden $A = \{a, b, c\}$ være $R = \{(a, a), (a, c), (b, c), (c, b)\}$.

a) Representer R ved en matrise og finn matrisen til den transitive tillukningen R^*.

b) Tegn den rettede grafen til R^*.

Oppgave 5 En endelig automat M som gjenkjenner språket $L = \mathrm{L}(M)$ er gitt ved den merkede grafen vist under. Merk at både a og b fører fra s_1 til s_0.



a) Lag et regulært uttrykk R, slik at $L = \mathrm{L}(R)$.

b) Lag en deterministisk endelig automat N, slik at $L = \mathrm{L}(N)$. Bruk tabell, men representer tilslutt N som en merket graf.

Oppgave 6 Funksjonen s, er definert for alle hele tall ≥ 2, som

$$s(n) = \sum_{j=2}^{n} (2j-1)^2$$

Velg den korrekte formelen under, og vis dens gyldighet ved matematisk induksjon.

1) $s(n) = 25n - 41$
2) $s(n) = \frac{3}{2}n^2 + \frac{35}{2}n - 32$
3) $s(n) = \frac{4}{3}n^3 - \frac{1}{3}n - 1$

Oppgave 7 Det Kinesiske restteoremet og Fermats lille teorem, samt det faktum at det er lett å finne store primtal og vanskelig å faktorisere store tall, gjør det mulig i praksis å implementere et meget godt offentlig kryptosystem, nemlig RSA systemet.

Fortell så kort og presist som mulig, uten bruk av noe matematikk, hva et offentlig og et privat kryptosystem er.

Beskriv en måte som et offentlig kryptosystem kan brukes på til å sende en signert kryptert melding, slik at mottakeren kan være rimelig sikker på at meldingen ble sent av den personen som utgir seg for senderen.