NTNU
Kunnskap for en bedre verden

Institutt for datateknologi og informatikk

Eksamensoppgave i **TDAT2002 A S1 Matematikk 2, Del 1**

Faglig kontakt under eksamen: Anette Wrålsen [a], Hans Jakob Rivertz [b]

Tlf: [a] 977 96 878 , [b] 938 32 172

Eksamensdato: 14. desember 2017

Eksamenstid (fra–til): 09:00–13:00

Hjelpemiddelkode/Tillatte hjelpemidler: Godkjent kalkulator emnetype 1

Annen informasjon:
Husk: *For å få full uttelling må du alltid ha med nok begrunnelse/utregning til at det ikke er tvil om hvordan du har løst oppgaven!*

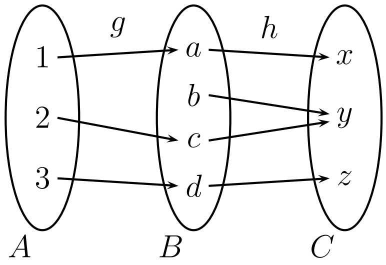
Målform/språk: bokmål

Antall sider (uten forside): 2

Antall sider vedlegg: 3

Oppgave 1 (20 %)

(i) $f : A \to C$ er gitt ved den sammensatte funksjonen $f = h \circ g$ der $g : A \to B$ og $h : B \to C$ er gitt i diagrammet under.



(ii) $h : \mathbb{R} \to \mathbb{R}$ gitt ved

$$h : x \mapsto x^2.$$

(iii) $g : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ gitt ved

$$g : n \mapsto n^3 \,\%\, 5.$$

(iv) $m : \mathscr{P}(\mathbb{Z}) \to \mathscr{P}(\mathbb{Z})$ gitt ved

$$m : A \mapsto A^c$$

For hver av funksjonene over, bevis eller motbevis utsagnene under.

a) Funksjonen er injektiv (en-til-en)

b) Funksjonen er surjektiv (på)

Oppgave 2 (20 %)

a) Løs differensligningen:

$$2a_k + 2a_{k-1} = 12a_{k-2}, \quad a_0 = 5, \quad a_1 = 0$$

b) Vis at formelen $b_n = n + 3^n$ er en løsning av differensligningen

$$b_n = 4b_{n-1} - 3b_{n-2} - 2, \quad b_0 = 1, \quad b_1 = 4$$

for alle $n \geq 2$.

Oppgave 3 (20 %)

a) (i) Finn $\gcd(352, 151)$ ved å bruke Euklids algoritme. Har 151 en multiplikativ invers modulo 352? Forklar hvorfor eller hvorfor ikke.

(ii) Finn $244^7 \pmod{391}$.

b) Et RSA-kryptosystem er basert på primtallene $p = 17$ og $q = 23$.

(i) Forklar hvorfor du kan bruke $(n, 151)$ med $n = pq$ som privat nøkkel. Finn også den offentlige nøkkelen.

(ii) Dekrypter meldingen 244 i dette systemet.

Oppgave 4 (15 %)

a) Regn ut den retningsderiverte til funksjonen $f(x, y) = \cos \pi xy$ i punktet $(1, 1/2)$ i retningen $\mathbf{u} = (4/5, 3/5)$.

b) I hvilken retning $\mathbf{v}$ har $f(x, y)$ størst retningsderivert i punktet $(1, 1/2)$?

c) Hva er den retningsderiverte til funksjonen $f(x, y) = \cos \pi xy$ i punktet $(1, 1/2)$ i retningen $\mathbf{v}$ som du fant i punkt b?

Oppgave 5 (20 %)
La $f(x, y) = 3x^2y - 6xy + 2y^3 - 3y$

a) Regn ut gradienten til $f(x, y)$ og alle andrederiverte av $f(x, y)$

b) Finn og klassifiser alle kritiske punkter til $f(x, y)$

c) Finn største og minste verdi av $f(x, y)$ på området begrenset av sirkelen $x^2 - 2x + y^2 = 0$ med radius 1 og senter i punktet $(1, 0)$

Oppgave 6 (5 %)
Eksisterer følgende grense? Regn også ut grenseverdien hvis den eksisterer.

$$\lim_{(x,y)\to(0,0)} \frac{x^2 + y^2}{\sqrt{x^2 + y^2 + 1} - 1}$$

Formelsamling TDAT2002 Matematikk 2
Institutt for informatikk og e-læring, NTNU

Logikklovene

Kommutative lover:	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Assosiative lover:	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive lover:	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identitetslover:	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
Negasjonslover:	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
Dobbel negativ-lov:	$\sim (\sim p) \equiv p$	
Idempotente lover:	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universalgrenselover:	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
DeMorgans lover:	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
Absorpsjonslover:	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negasjon av **t** og **c**:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

Mengdelovene

Alle mengder er inneholdt i en universalmengde U.

Kommutative lover:	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Assosiative lover:	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
Distributive lover:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Identitetslover:	$A \cap U = A$	$A \cup \emptyset = A$
Negasjonslover:	$A \cup A^c = U$	$A \cap A^c = \emptyset$
Dobbel negativ-lov:	$(A^c)^c = A$	
Idempotente lover:	$A \cap A = A$	$A \cup A = A$
Universalgrenselover:	$A \cup U = U$	$A \cap \emptyset = \emptyset$
DeMorgans lover:	$(A \cap B)^c = A^c \cup B^c$	$(A \cup B)^c = A^c \cap B^c$
Absorpsjonslover:	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Komplement av U og $\emptyset$:	$U^c = \emptyset$	$\emptyset^c = U$
Mengdedifferensloven:	$A - B = A \cap B^c$	

Regneregler for rekker

Hvis $\{a_k\}$ og $\{b_k\}$ er følger av reelle tall og $c \in \mathbb{R}$, har vi følgende for heltall $n \geq m$:

$$\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$$

$$c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} (c \cdot a_k)$$

$$\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} (a_k \cdot b_k)$$

Noen kjente rekker

Summen av de n første heltallene:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Summen av en endelig geometrisk rekke: For reelle tall $r \neq 1$ er

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

Prinsippet for matematisk induksjon

La $P(n)$ være en påstand om heltall n, og $a \in \mathbb{Z}$. Anta videre følgende:

1) $P(a)$ er sann. **(Basissteg)**
2) For ethvert heltall $k \geq a$, hvis $P(k)$ er sann så er $P(k+1)$ sann. **(Induktivt steg)**

Da er $P(n)$ sann for alle heltall $n \geq a$.

Prinsippet for sterk matematisk induksjon

La $P(n)$ være en påstand om heltall n, og la a og b være bestemte heltall slik at $a \leq b$. Anta videre følgende:

1) $P(a), P(a+1), \ldots, P(b)$ er sanne. **(Basissteg)**
2) For ethvert heltall $k > b$, hvis $P(i)$ er sann for alle heltall i slik at $a \leq i < k$, så er $P(k)$ sann. **(Induktivt steg)**

Da er $P(n)$ sann for alle heltall $n \geq a$.

Andreordens lineære homogene differensligninger med konstante koeffisienter

La følgen $a_0, a_1, a_2 \ldots$ oppfylle differensligningen $a_k = Aa_{k-1} + Ba_{k-2}$ for alle heltall $k \geq 2$ og $A, B \in \mathbb{R}$.

Tilfelle 1: Distinkte røtter
Hvis den karakteristiske ligningen

$$t^2 - At - B = 0$$

har to forskjellige røtter r og s, er følgen gitt ved

$$a_n = Cr^n + Ds^n \text{ for alle } n \geq 0.$$

Tilfelle 2: Sammenfallende røtter
Hvis den karakteristiske ligningen

$$t^2 - At - B = 0$$

har en dobbelrot $t = r$, er følgen gitt ved

$$a_n = Cr^n + Dnr^n \text{ for alle } n \geq 0.$$

Hvis intitalbetingelser er gitt kan C og D bestemmes ut fra disse.

Aritmetikkens fundamentalteorem

Gitt et heltall n eksisterer det et positivt heltall k, forskjellige primtall $p_1, p_2, p_3, \ldots, p_k$ og positive heltall $e_1, e_2, e_3, \ldots, e_k$ slik at

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \ldots \cdot p_k^{e_k}.$$

Videre er denne måten å skrive n som et produkt av primtall på unik bortsett fra rekkefølgen på faktorene.

Euklids algoritme

Euklids algoritme brukes til å bestemme $\gcd(A, B)$ for to heltall A og B, der vi antar at $A > B \geq 0$.

1. Hvis $B = 0$, er $\gcd(A, B) = A$.
2. Hvis ikke, finn q og r slik at

   $$A = Bq + r \text{ slik at } 0 \leq r < B.$$

   Da er $gcd(A, B) = gcd(B, r)$.
3. Sett $A := B$ og $B := r$ og gå tilbake til trinn 1.

Regneregler for kongruenser

La a, b, c, d, n være heltall slik at $n > 1$, slik at $a \equiv c \pmod{n}$ og $b \equiv d \pmod{n}$. Da har vi at

a) $(a + b) \equiv (c + d) \pmod{n}$
b) $(a - b) \equiv (c - d) \pmod{n}$
c) $ab \equiv cd \pmod{n}$
d) $a^m \equiv c^m \pmod{n}$ for alle positive heltall m.

RSA

RSA er offentlig nøkkel-kryptografi. Et RSA-kryptosystem er basert på to (store) primtall p og q.

Prosedyre for å finne nøkler

1. Finn et tall e som er relativt primisk med $(p-1)(q-1)$ og finn så en positiv invers d til dette tallet modulo $(p-1)(q-1)$.
2. La $n = pq$. Da blir (n, e) *offentlig nøkkel* og
3. (n, d) *privat nøkkel*.

Kryptering og dekryptering

Du ønsker å sende en melding M, og kjenner mottakerens offentlige nøkkel (n, e).

- Den krypterte meldingen C er gitt ved
$$C \equiv M^e \pmod{n}.$$
- C dekrypteres ved å beregne
$$M \equiv C^d \pmod{n}.$$

Flervariabelanalyse – diverse formler

Likningen for sirkelen med radius r og sentrum i (x_0, y_0):
$$(x-x_0)^2 + (y-y_0)^2 = r^2$$
Likningen for ellipsen med sentrum i (x_0, y_0) og halvakser a og b:
$$1 = \frac{(x-x_0)^2}{a^2} + \frac{(y-y_0)^2}{b^2}$$
Tangentplanet til funksjonen $z = f(x, y)$ i punktet (x_0, y_0, z_0):
$$z - z_0 = f_x(x_0, y_0)(x-x_0) + f_y(x_0, y_0)(y-y_0)$$
Lineærapproksimasjonen til funksjonen $z = f(x, y)$ rundt punktet $(x_0, y_0, f(x_0, y_0))$:
$$L(x, y) = f(x_0, y_0) + f_x(x_0, y_0)(x-x_0) + f_y(x_0, y_0)(y-y_0)$$
Gradienten til en funksjon $z = f(x, y)$:
$$\nabla f = f_x(x, y)\mathbf{i} + f_y(x, y)\mathbf{j}$$
Den retningsderiverte til en funksjon $z = f(x, y)$ i retningen gitt ved enhetsvektoren $\vec{u}$:
$$D_{\vec{u}} f = \nabla f \cdot \vec{u}$$