NTNU

Kunnskap for en bedre verden

Institutt for datateknologi og informatikk

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

Faglig kontakt under eksamen: Hans Jakob Rivertz

Tlf: 938 32 172

Eksamensdato: 4. desember 2019

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

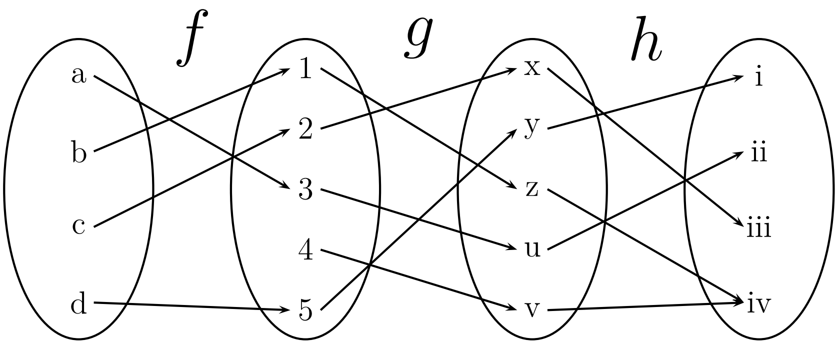
Oppgave 1 (20%)

a) La $A = \{1, 2, 3\}$, $B = \{1, \{1, 2\}, 3\}$ og $C = \{1, 2\}$ være mengder. Avgjør om påstandene under er sanne eller usanne.

(i) $A \cup C = A$.
(ii) $A \cap C = C$.
(iii) $B \subset A$.
(iv) $\emptyset \in B$.
(v) $\emptyset \subset B$.
(vi) $2 \in B$.
(vii) $C \in B$.
(viii) $C \in A$.
(ix) $A - B = A \cap B^c$.
(x) $\mathscr{P}(A) \cap B = \emptyset$.

b) Avgjør for hver av funksjonene under om de er injektive, surjektive og bijektive.

(i) f
(ii) g
(iii) h
(iv) $h \circ g \circ f$
(v) $g \circ f$



Oppgave 2 (20 %)

a) Løs differenslikningen

$$a_k + a_{k-1} = 6a_{k-2}, \quad a_0 = 5, a_1 = 0.$$

b) I landet Utopia har de bare penger med verdiene 3 Mark og 7 Mark. Prisen for den billigste bussreise er 12 Mark. I Utopia er det uendelig mange bussruter R_k, $k > 11$. Rute R_k koster k Mark. På bussene i Utopia krever man nøyaktig betaling.

i) Vis at det er mulig å betale biletter som koster 12, 13 og 14 Mark.

ii) Bevis ved hjelp av sterk induksjon at det er mulig å betale alle bussreiser i Utopia uten å betale for mye. (Hint: Anta at det er mulig å betale alle biletter som koster fra 12 Mark til og med k Mark for $k \geq 14$.)

Oppgave 3 (20 %)

a) i) Avgjør om 102 har en multiplikativ invers modulo 240, og hvis den har det, finn en slik invers.

ii) Avgjør om 103 har en multiplikativ invers modulo 240, og hvis den har det, finn en slik invers.

b) I denne oppgaven skal du jobbe med et RSA-kryptosystem basert på primtallene $p = 17$ og $q = 31$.

i) Finn en offentlig og en privat nøkkel for dette kryptosystemet (som hører sammen).

ii) Krypter meldingen 42 i kryptosystemet du har laget.

iii) Dekrypter meldingen fra b.ii) og vis at du får tilbake 42.

Oppgave 4 (20 %)

a) Finn gradienten til $f(x, y, z) = xy + 2yz + 3xz$.

b) Finn den retningsderiverte til $f(x, y, z)$ i retningen $\mathbf{u} = (2, 6, -3)$ i punktet $(1, 2, 1)$.

c) I hvilken retning øker $f(x, y, z)$ mest i punktet $(1, 2, 1)$?

c) Finn en likning for tangentplanet til flaten $f(x, y, z) = 9$ i punktet $(1, 2, 1)$.

Oppgave 5 (20 %)
Gitt funksjonen $f(x, y) = 6x(x^2 - 1)y^2 - 4x^3 + 3x^2 + 6x$.

a) Finn alle kritiske punkter til $f(x, y)$. (Hint: det er 6 kritiske punkter.)

b) Klassifiser de kritiske punktene fra punkt a).

c) Finn absolutt maksimum og minimum på kvadratet gitt ved $D = [-1, 1] \times [-1, 1] \subset \mathbb{R}^2$.

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 $\mathbf{t}$ og $\mathbf{c}$:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

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 $\vec{u}$:

$$D_{\vec{u}} f = \nabla f \cdot \vec{u}$$