HØGSKOLEN I SØR-TRØNDELAG
Avdeling for informatikk og e-læring

Målform:	Bokmål
Eksamensdato:	11. desember 2015
Varighet/eksamenstid:	4 timer
Emnekode:	TDAT2002
Emnenavn:	Matematikk 2
Klasse(r):	
Studiepoeng:	10 (denne deleksamenen teller 45% av sluttresultatet)
Faglærer(e):	Anette Wrålsen (mobil 97 79 68 78) Hans Jakob Rivertz (mobil 93 83 21 72)
Kontaktperson(adm.)	
Hjelpemidler:	Kalkulator, emnegruppe 1
Oppgavesettet består av:	6 sider bestående av forside, 6 oppgaver fordelt på 2 sider og et vedlegg på 3 sider.
Vedlegg består av:	3 sider formelsamling

Merknad: Oppgaveteksten kan beholdes av studenter som sitter eksamenstiden ut.

Les gjennom hele oppgaven før du begynner slik at du kan disponere tiden best mulig. Dersom noe virker uklart i oppgavesettet, skal du gjøre dine egne antagelser og forklare dette i besvarelsen.

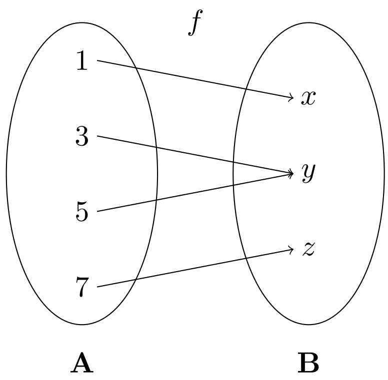
Lykke til!

Husk: *Ha alltid med nok begrunnelse/utregning til at det ikke er tvil om hvordan du har løst oppgaven!*

Oppgave 1 (20%)

Gitt følgende funksjoner:

(i) $f : A \to B$ gitt ved diagrammet under:



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

$$g(x) = x - 3$$

(iii) $h : \mathbb{N} \to \{0, 1\}$ der

$$h(n) = \begin{cases} 0 & \text{hvis } n \text{ er et sammensatt tall eller 1} \\ 1 & \text{hvis } n \text{ er et primtall} \end{cases}$$

(iv) $m : \mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R}) \to \mathcal{P}(\mathbb{R})$ gitt ved at

$$m(A, B) = A \cap B$$

For hver av de fire funksjonene, vis eller motbevis (for eksempel ved hjelp av et moteksempel) at funksjonen er

a) injektiv (en-til-en) og

b) surjektiv (på).

Oppgave 2 (20%)

a) Gitt tre mengder A, B og C inneholdt i en universalmengde $\mathcal{U}$. Vis påstandene under ved å bruke mengdelovene eller elementbeskrivelser, eller, om du mener en eller begge er usanne, gi et moteksempel.

   i) $(A - B) \cup (A \cap B) = A$

   ii) $B \cap C \subseteq A^c \cap (B \cup C)$

b) Gitt differensligningen med initalbetingelse som følger:

$$a_{n+1} = 3a_n + 2, \quad a_0 = 0, n \geqslant 0.$$

Vis ved matematisk induksjon at følgen $a_n = 3^n - 1$ er en løsning på denne differensligningen.

Oppgave 3 (20%)

a) i) Finn $\gcd(924, 103)$ ved hjelp av Euklids metode. Har 103 en invers modulo 924?

ii) Finn $22^{25} \pmod{28}$ og $42^{25} \pmod{989}$. Ta med all utregning.

b) Du skal sette opp et RSA-system basert på primtallene $p = 43$ og $q = 23$.

i) Forklar hvorfor du kan la $(n, 103)$ være offentlig nøkkel, der $n = pq$. Hva blir da din private nøkkel?

ii) Krypter meldingen 42 i dette systemet.

Oppgave 4 (5%)

La $h(x, y) = x^2y + 2y^2$. Finn tangentplanet til $z = h(x, y)$ i punktet $(1, 1, 3)$.

Oppgave 5 (5%)

Avgjør om funksjonen

$$q(x, y) = \frac{x^2 + xy + y^2}{x^2 + y^2}$$

er kontinuerlig i $(0, 0)$.

Oppgave 6 (30%)

Betrakt følgende funksjon:

$$f(x, y) = 3x^2 - 3x^2y + 2y^2$$

a) Finn alle 1. og 2. ordens partielle deriverte av $f(x, y)$. Skriv ned gradienten til f.

b) i) I hvilken retning vokser $f(x, y)$ mest i punktet $(1, 3)$?

ii) Finn den retningsderiverte i denne retningen i punktet $(1, 3)$.

c) i) Finn alle de kritiske punktene til $f(x, y)$.

ii) Regn ut $D(x, y) = f_{xx}(x, y)f_{yy}(x, y) - f_{xy}(x, y)^2$ for hvert punkt du fant i delpunkt i).
Klassifiser de kritiske punktene.

d) Finn største og minste verd av $f(x, y)$ med avgrensing $g(x, y) = x^2 + y^2 = 25$. (Dvs: Finn største verdi av $f(x, y)$ for punkter (x, y) på sirkelen med radius 5 og senter i origo.)

1. Logikk

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

2. Induksjon og rekursjon

Regneregler for rekker

Hvis $a_m, a_{m+1}, a_{m+2}, \ldots$ og $b_m, b_{m+1}, b_{m+2}, \ldots$ er følger av reelle tall og c er et reellt tall, har vi følgende for ethvert 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: For alle heltall $n \geq 1$ er

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

Summen av en geometrisk rekke: For alle heltall $n \geq 0$ og alle 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 la a være et bestemt heltall. 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 en differensligning

$$a_k = Aa_{k-1} + Ba_{k-2} \text{ for alle heltall } k \geq 2 \text{ og reelle tall } A, B,$$

og la a_0 og a_1 være gitte tall (initialbetingelser).

Tilfelle 1: Distinkte røtter
Hvis den karakteristiske ligningen

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

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

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

Tilfelle 2: Sammenfallende røtter
Hvis den karakteristiske ligningen

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

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

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

I begge tilfeller bestemmes C og D ut fra initialbetingelsene.

3. Mengdelære

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:	$A - B = A \cap B^c$	

4. Tallteori

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 $n > 1$, og anta 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.

5. RSA

RSA er offentlig nøkkel-kryptografi. Et RSA-kryptosystem er basert på to (helst veldig 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. Du må da kjenne mottakerens offentlige nøkkel (n, e).

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

6. 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 $\vec{u}$:

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