Norges teknisk–naturvitskaplege universitet
Institutt for Datateknologi og Informatikk

Løsningsforslag

$\boxed{1}$ (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) $\mathcal{P}(A) \cap B = \emptyset$.

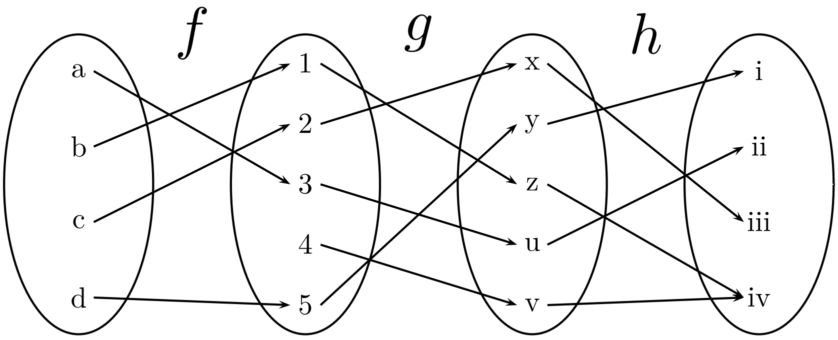
Løsning:

(i) $A \cup C = A$ er sant fordi $A \subset C$.
(ii) $A \cap C = C$ er sant fordi $A \subset C$.
(iii) $B \subset A$ er ikke sant fordi $\{1, 2\} \in B$, men $\{1, 2\} \notin A$.
(iv) $\emptyset \in B$ er ikke sant fordi $\emptyset$ er delmengde men ikke element i B.
(v) $\emptyset \subset B$ er sant fordi $\emptyset$ er delmengde av alle mengder.
(vi) $2 \in B$, er ikke sant da 2 ikke er et element i B. Det hjelper ikke at 2 er element i $\{1, 2\}$. $\{1, 2\}$ er et element i
(vii) $C \in B$ er sant. Se forklaringen til vi).
(viii) $C \in A$ er ikke sant. $C \subset A$ er ikke det samme som $C \in A$.
(ix) $A - B = A \cap B^c$ er sant for alle mengder A og B.
  (1) Om $x \in A - B$ så er $x \in A$ men $x \notin B$. Det betyr at $x \in A$ og $x \in B^c$. Derfor er $x \in A \cap B^c$. Vi har derfor $A - B \subseteq A \cap B^c$.
  (2) Om $x \in A \cap B^c$ så er $x \in A$ og $x \in B^c$. Det betyr at $x \in A$ og $x \notin B$. Derfor er $x \in A - B$. Vi har derfor $A \cap B^c \subseteq A - B$.

  Fra en og to har vi at $A - B \subseteq A \cap B^c$ og $A \cap B^c \subseteq A - B$. Derfor er $A - B = A \cap B^c$.
(x) $\mathcal{P}(A) \cap B = \emptyset$ er ikke sant fordi $\{1, 2\} \in \mathcal{P}(A)$ og $\{1, 2\} \in B$.

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) $g \circ f$



Løsning: La $A = \{a, b, c, d\}$, $B = \{1, 2, 3, 4, 5\}$, $C = \{x, y, z, u, v\}$ og $D = \{i, ii, iii, iv\}$.

(i) f er injektiv fordi f sender elementene i A på forskjellige elementer i B. f er ikke surjektiv fordi f sender ingen elementer på 4.

(ii) g er injektiv fordi g senfer elementene i B på forskjellige elementer i C. g er surjektiv fordi alle elementer i C er med i verdimengden til g. g er bijektiv fordi g er surjektiv og injektiv.

(iii) h er surjektiv da alle elementer i D "nås" av h. h er ikke injektiv fordi $h(z) = h(v)$.

(iv) $h \circ g \circ f$ er surjektiv da alle elementer i D nås av funksjonen: $(h \circ g \circ f)(a) = ii$, $(h \circ g \circ f)(b) = iv$, $(h \circ g \circ f)(c) = iii$, $(h \circ g \circ f)(d) = i$. Den er også injektiv da 4 elementer sendes på 4 elementer da kan ingen par av elementer i A sendes til samme element i D.

(v) $g \circ f$ har samme egenskaper som f.

$\boxed{2}$ (20 %)

a) Løs differenslikningen

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

Løsning: Det ryddes opp i likningen slik at høyresiden er null. $a_k + a_{k-1} - 6a_{k-2} = 0$ Karakteristisk polynom $m^2 + m - 6 = (m + 3)(m - 2)$ har nullpunktene $m_1 = 2$ og $m_2 = -3$. Generell løsning er $a_k = A(2)^k + B(-3)^k$. Bestemmer A og B: $a_0 = A + B = 5$ og $a_1 = 2A - 3B = 0$ som gir $A = 3$ og $B = 2$.

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.
Løsning: 12 er mulig å betale fordi $12 = 4 \cdot 3$, 13 fordi $13 = 7 + 3 + 3$, 14 fordi $14 = 7 + 7$.

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 $k \geq 14$.)
Løsning: Vi har bevist start trinnet i punkt i). $k = 12, 13, 14$
Anta at vi kan betale for $k = 12, 13, \ldots, n - 1$ for $n > 14$. Da kan man betale $k = n - 3$ og derfor også for $k = n$ved å betale med en 3-Mark mynt ektra.

$\boxed{3}$ (20 %)

a) i) Avgjør om 102 har en multiplikativ invers modulo 240, og hvis den har det, finn en slik invers.
Løsning: Siden 2 deler både 102 og 240 så er di ikke innbyrdes primiske. Derfor finnes ingen invers av 102 modulo 240.

ii) Avgjør om 103 har en multiplikativ invers modulo 240, og hvis den har det, finn en slik invers.
Løsning: Vi utfører Euklids divisjonsalgoritme.
$240 : 103 = 2$ med 34 i rest
$103 : 34 = 3$ med 1 i rest.
$\gcd(103, 240) = 1$ og det finnes en invers av 103 modulo 240.
Vi fortsetter med Euklids utvidede algoritme.
$1 = 103 - 3 \cdot 34 = 103 - 3 \cdot (240 - 2 \cdot 103) = 7 \cdot 103 - 3 \cdot 240 \equiv 7 \cdot 103 \pmod{240}$.
7 og 103 er hverandres inverse modulo 240.

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).
Løsning.
Alternativ 1. Vi har $(p-1)(q-1) = 16 \cdot 30 = 480$ og ønsker å finne to tall e og d som er inverse til hverandre modulo 480. Dvs $ed = (p-1)(q-1)k + 1$ for et heltall k. Tallparet e og d kan brukes i nøkler fordi $a^{ed} = a^{1+(p-1)(q-1)k} =\equiv a \pmod{pq}$ for alle a. Det lønner seg at et av de er så lite som mulig. Vi vil finne et lite primtall som er inbyrdes prim til 480. Vi påstår at 7 er et slik tall. Vi utfører Euklids divisjonsalgoritme.
$480 : 7 = 68$ med 4 i rest.
$7 : 4 = 1$ med 3 i rest.
$4 : 3 = 1$ med 1 i rest.
Dvs $\gcd(7, 480) = 1$. Vi fortsetter med Euklids utvidede algoritme.
$1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (480 - 68 \cdot 7) - 7 = 2 \cdot 480 - 137 \cdot 7$. -137 og 7 er inbyrdes inverse men vi må legge til 480 for en positiv invers mindre enn 480.
Vi lar $e = 7$ og $d = 480 - 137 = 343$.
Alternativ 2. Vi har $\text{lcm}(p-1, q-1) = 16 \cdot 15 = 240$. Vi kan da bruke $e = 7$ og $d = 103$ fra punkt a) fordi $ed = 1 + k\,\text{lcm}(p-1, q-1)$ der k er et heltall og $a^{ed} = a^{1+\text{lcm}(p-1,q-1)k} =\equiv a \pmod{pq}$ for alle a.
Alternativ 3. Vi har $1 = 7 \cdot 103 - 3 \cdot 240$ fra oppgave a). Vi legger til og trekker fra $7 \cdot 240$ på høyre side av uttrykket.
$1 = 7{\cdot}103-3{\cdot}240+7{\cdot}240-7{\cdot}240 = 7{\cdot}(103+240)-(3+7){\cdot}240 = 7{\cdot}343-10{\cdot}240 = 7{\cdot}343-5{\cdot}480$.

ii) Krypter meldingen 42 i kryptosystemet du har laget.
Løsning:
Alternativ 1, 2 og 3. Vi skal regne ut $42^7 = 42 \cdot 42^2 \cdot 42^4 \pmod{pq}$. $pq = 527$.
$42^2 = 1764 \equiv 183 \pmod{527}$
$42^4 = 183^2 \equiv 288 \pmod{527}$
$42^7 = 42 \cdot 42^2 \cdot 42^4 \equiv 42 \cdot (183 \cdot 288) \equiv 42 \cdot 4 \equiv 168 \pmod{527}$
Den kodede meldingen er 168.

iii) Dekrypter meldingen fra b.ii) og vis at du får tilbake 42.
Løsning: *Alternativ 1 og 3.* Vi skal regne ut $193^{343} \pmod{517}$.
Vi bruker binær representasjon av 343=1+2+4+16+64+256.
Da er $168^{343} = 168 \cdot 168^2 \cdot 168^4 \cdot 168^{16} \cdot 168^{64} \cdot 168^{256}$.
$168^2 \equiv 293 \pmod{527}$
$168^4 \equiv 293^2 \equiv 475 \pmod{527}$
$168^8 \equiv 475^2 \equiv 69 \pmod{527}$
$168^{16} \equiv 69^2 \equiv 18 \pmod{527}$
$168^{32} \equiv 18^2 \equiv 324 \pmod{527}$
$168^{64} \equiv 324^2 \equiv 103 \pmod{527}$
$168^{128} \equiv 103^2 \equiv 69 \pmod{527}$
$168^{256} \equiv 69^2 \equiv 18 \pmod{527}$
Da er $168^{343} = 168 \cdot 168^2 \cdot 168^4 \cdot 168^{16} \cdot 168^{64} \cdot 168^{256} \equiv (168 \cdot 293) \cdot (475 \cdot 18) \cdot (103 \cdot 18) \equiv 213 \cdot (118 \cdot 273) \equiv 213 \cdot 67 \equiv 42 \pmod{527}$.
Alternativ 2. Vi skal regne ut $193^{103} \pmod{517}$.

Vi bruker binær representasjon av 103=1+2+4+32+64.
Da er $168^{103} = 168 \cdot 168^2 \cdot 168^4 \cdot 168^{32} \cdot 168^{64}$.
$168^2 \equiv 293 \pmod{527}$
$168^4 \equiv 293^2 \equiv 475 \pmod{527}$
$168^8 \equiv 475^2 \equiv 69 \pmod{527}$
$168^{16} \equiv 69^2 \equiv 18 \pmod{527}$
$168^{32} \equiv 18^2 \equiv 324 \pmod{527}$
$168^{64} \equiv 324^2 \equiv 103 \pmod{527}$
Da er $168^{103} = 168 \cdot 168^2 \cdot 168^4 \cdot 168^{32} \cdot 168^{64} \equiv (168 \cdot 293) \cdot (475 \cdot 324) \cdot 103 \equiv (213 \cdot 16) \cdot 103 \equiv 246 \cdot 103 \equiv 42 \pmod{527}$.

$\boxed{4}$ (20 %)

a) Finn gradienten til $f(x,y,z) = xy + 2yz + 3xz$.
Løsning: $\nabla f = (f_x, f_y, f_z) = (y + 3z, x + 2z, 2y + 3x)$.

b) Finn den retningsderiverte til $f(x,y,z)$ i retningen $\mathbf{u} = (2, 6, -3)$ i punktet $(1, 2, 1)$.
Løsning: Lengden til $\mathbf{u}$ er $|\mathbf{u}| = \sqrt{2^2 + 6^2 + (-3)^2} = \sqrt{4 + 36 + 9} = \sqrt{49} = 7$. Retningsvektoren er derfor $\hat{\mathbf{u}} = \mathbf{u}/|\mathbf{u}| = (2/7, 6/7, -3/7)$. Gradienten til f i (1,2,1) er $\nabla f = (5, 3, 7)$. Den retningsderiverte til f i punktet (1,2,1) i retningen $\hat{\mathbf{u}}$ er

$$D_{\hat{\mathbf{u}}} f(1,2,1) = \hat{\mathbf{u}} \cdot \nabla f(1,2,1) = 10/7 + 18/7 - 3 = 1.$$

c) I hvilken retning øker $f(x,y,z)$ mest i punktet $(1, 2, 1)$?
Løsning: F øker mest i retningen til gradienten til f i punktet $(1, 2, 1)$.

d) Finn en likning for tangentplanet til flaten $f(x,y,z) = 9$ i punktet $(1, 2, 1)$.
Løsning: Tangentplanet har normalvektor $\nabla f(1,2,1) = (5, 3, 7)$. Likningene for planet med tangent $(5, 3, 7)$ er

$$5(x - 1) + 3(y - 2) + 7(z - 1) = 0$$

som gir

$$5x + 3y + 7z = 18.$$

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

Løsning:

a) Finn alle kritiske punkter til $f(x,y)$. (Hint: det er 6 kritiske punkter.)
Løsning: Skriver om $f(x,y) = 6(x^3 - x)y^2 - 4x^3 + 3x^2 + 6x$.
Partsiell deriverer
$f_x(x,y) = 6(3x^2 - 1)y^2 - 12x^2 + 6x + 6$
$f_y(x,y) = 12x(x^2 - 1)y$
Finner først løsningene for $f_y = 0$.
$f_y(x,y) = 12x(x^2 - 1)y = 0$ er ekvialent med at $x = -1 \vee x = 0 \vee x = 1 \vee y = 0$.
For hvert av de fire tilfellene skal vi løse $f_x(x,y) = 0$

$(x = -1)$ Gir $f_x(-1, y) = 12y^2 - 12 = 0$ som er ekivalent med $y = \pm 1$. Det gir kritiske punkter $(-1, 1)$ og $(-1, -1)$.

$(x = 0)$ Gir $f_x(0, y) = -6y^2 + 6 = 0$ som er ekivalent med $y = \pm 1$. Det gir kritiske punkter $(0, 1)$ og $(0, -1)$.

($x = 1$) Gir $f_x(1, y) = 12y^2 = 0$ som gir $y = 0$. Det gir kritiske punkter $(1, 0)$.

($y = 0$) Gir $f_x(x, 0) = -12x^2 + 6x + 6 = 0$ som er ekivalent med $x = 1 \vee x = -1/2$. Det gir kritiske punkter $(1, 0)$ og $(-1/2, 0)$.

b) Klassifiser de kritiske punktene fra punkt a).

Løsning: Vi må regne ut de andre ordens deriverte av f.

$f_{xx}(x, y) = 36xy^2 - 24x + 6$

$f_{xy} = 12(3x^2 - 1)y$

$f_{yy} = 12x(x^2 - 1)$

Tabell:

Kr.pkt	f_{xx}	f_{yy}	f_{xy}	$D = f_{xx}f_{yy} - {f_{xy}}^2$	Type
$(-1, 1)$	6	0	24	-576	sadel
$(-1, -1)$	6	0	-24	-576	sadel
$(0, 1)$	6	0	-12	-144	sadel
$(0, -1)$	6	0	12	-144	sadel
$(1, 0)$	-18	0	0	0	Ubestemt
$(-1/2, 0)$	18	9/2	0	81	Lokalt minimum

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

Løsning: D er kvadratet avgrenset av linjene $x = 1$, $x = -1$, $y = -1$, $y = 1$.

Vi betrakter hver av linjene

($x = 1$) Vi har $f(1, y) = 5$.

($x = -1$) Vi har $f(-1, y) = 1$.

($y = \pm 1$) Vi har $f(x, \pm 1) = 2x^3 + 3x^2$. Vi finner maks og min av $f(x, \pm 1) = 2x^3 + 3x^2$:
$f_x(x, \pm 1) = 6x^2 + 6x = 0 \Leftrightarrow x = 0 \vee x = -1$. $f(0, \pm 1) = 0$.

På randen har vi derfor $f = 5$ og $f = 1$ langs linjene $x = \pm 1$ og $f = 0$ i punktene $(\pm 1, 0)$. Vi må også sjekke det eneste kritiske punktet fra a) og b) som vi ikke har sjekket. $f(-1/2, 0) = -7/4$.

Vi har maksimal verdi 5 på randen $x = 1$ og minimal verdi -7/4 i punktet $(-1/2, 0)$.