Norges teknisk–naturvitskaplege universitet
Institutt for Datateknologi og Informatikk

Løsningsforslag

1

(i) **a)** Funksjonen er injektiv fordi den kun 1 sendes til x, kun 2 sendes til y og kun 3 sendes til z. **b)** Den er surjektiv fordi alle verdier av C nås av funksjonen.

(ii) **a)** Funksjonen $h : \mathbb{R} \to \mathbb{R}$ gitt ved $h : x \mapsto x^2$. er ikke surjektiv fordi det ikke finnes noen x slik at $h(x) - 1$. **b)** Den er ikke injektiv fordi $h(-1) = h(1)$ men $-1 \neq 1$.

(iii) Vi regner ut alle verdier for funksjonen $g : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ gitt ved $g : n \mapsto n^3 \,\%\, 5.$:

$$\begin{array}{lllllll} g(0) & = & 0^3 \,\%\, 5 & = & 0 \,\%\, 5 & = & 0 \\ g(1) & = & 1^3 \,\%\, 5 & = & 1 \,\%\, 5 & = & 1 \\ g(2) & = & 2^3 \,\%\, 5 & = & 8 \,\%\, 5 & = & 3 \\ g(3) & = & 3^3 \,\%\, 5 & = & 27 \,\%\, 5 & = & 2 \\ g(4) & = & 4^3 \,\%\, 5 & = & 64 \,\%\, 5 & = & 4 \end{array}$$

b) Funksjonen er surjektiv fordi hver verdi i mengden $\{0, 1, 2, 3, 4\}$ nås og **a)** injektiv fordi $g(x) = g(y)$ hvis og bare hvis $x = y$.

(iv) Funksjonen $m : \mathcal{P}(\mathbb{Z}) \to \mathcal{P}(\mathbb{Z})$ gitt ved $m : A \mapsto A^c$ er både surjektiv og injektiv. **a)** Hvis $m(A) = m(B)$ så er $A^c = B^c$. VI tar komplementet på begge sider og får $(A^c)^c = (B^c)^c$. Bruker vi at $(A^c)^c = A$ for alle mengder A så har vi at $A = B$. Derfor er m injektiv. **b)** Funskjonen m er også surjektiv fordi for enhver mengde $A \in \mathcal{P}(\mathbb{Z})$ så er $m(A^c) = (A^c)^c = A$.

2

a) Differensligningen $2a_k + 2a_{k-1} = 12a_{k-2}$, $a_0 = 5$, $a_1 = 0$ løses ved å løse karakteristisk ligning $2t^2 + 2t = 12$. Divisjon med 2 og samling på venstre side av $=$ tegnet gir $t^2 + t - 6 = 0$. Faktorisering gir $(t + 3)(t - 2) = 0$. Røttene er $t_1 = 2$ og $t_2 = -3$. Generell løsning av diferenslikningen er $a_n = A\,2^n + B(-3)^n$. Startverdiene gir likningssystemet

$$\begin{aligned} a_0 = A + B &= 5 \\ a_1 = 2A - 3B &= 0 \end{aligned}$$

Løsningen på systemet er $A = 3$, $B = 2$. Svaret er derfor

$$a_n = 3\,2^n + 2(-3)^n$$

for alle $n \geq 2$.

b) Vi sjekker først startverdiene $b_0 = 0 + 3^0 = 0 + 1$ som er OK og $b_1 = 1 + 3^1 = 1 + 3 = 4$ som også er ok. Vi skekker så om likningen er tilfredstilt: Høyresiden er $4b_{n-1} - 3b_{n-2} - 2 = 4(n - 1 + 3^{n-1}) - 3(n - 2 + 3^{n-2}) - 2 = 4n - 4 + 4 \cdot 3^{n-1} - 3n + 6 - 3 \cdot 3^{n-2}) - 2 = 4n - 4 + 4 \cdot 3^{n-1} - 3n + 6 - 3^{n-1}) - 2 = n + (4 - 1) \cdot 3^{n-1} = n + 3^n$ som er det samme som venstresiden.

3

a) (i) Først er $352 : 151 = 2$ med 50 i rest. $151 : 50 = 3$ med 1 i rest. Det betyr at $\gcd(352, 151) = 1$. 151 har en multiplikativ invers modulo 352 fordi $\gcd(352, 151) = 1$.

(ii) For å finne $244^7 \pmod{391}$ regner vi ut $244^2 = 59536 \equiv 104 \pmod{391}$, $244^4 =\equiv 104^2 = 10816 \equiv 259 \pmod{391}$. Da er $244^7 = 244^4 \cdot 244^2 \cdot 244 \equiv 259 \cdot 104 \cdot 244 = 6572384 \equiv 65 \pmod{391}$.

b) Et RSA-kryptosystem er bassert på primtallene $p = 11$ og $q = 23$.

(i) Vi har $n = pq = 391$. Vi kan bruke $(391, 151)$ som privat nøkkel fordi $(p - 1)(q - 1) = 352$ og $\gcd(352, 151) = 1$. Den offentlige nøkkelen er den multiplikative inverse til 151 modulo 352.

Den multiplikative inversen fås ved å bruke Euklids utvidede algoritme. $1 = 151 - 3 \cdot 50 = 151 - 3(352 - 2 \cdot 151) = 7 \cdot 151 - 3 \cdot 352$. Den multiplikative inversen til 151 modulo 352 er 7. Den offentlige nøkkelen er $(391, 7)$

(ii) Vi dekrypterer 244 ved å bruke den offentlige nøkkelen. Fra deloppgave a,ii) fikk vi $244^7 \equiv 65 \pmod{391}$. Meldingen er 65.

$\boxed{4}$ a) Først regner vi ut gradienten til $f(x,y)$. $\nabla f = -\pi y \sin \pi xy \mathbf{\hat{i}} - \pi x \sin \pi xy \mathbf{\hat{j}}$. Gradienten i punktet (1/2,1) er $\nabla f(1/2,1) = -\pi \mathbf{\hat{i}} - (\pi/2)\mathbf{\hat{j}}$. Den retningsderiverte er $D_{\mathbf{u}} f = \nabla f(1/2,1) \cdot \mathbf{u} = (-\pi, -\pi/2) \cdot (4/5, 3/5) = -11\pi/10$.

b) Funksjonen $f(x,y)$ har størst retningsderivert i punktet $(1, 1/2)$ i retningen til $\nabla f(1/2,1) = -\pi \mathbf{\hat{i}} - (\pi/2)\mathbf{\hat{j}}$.?

c) Den retningsderiverte til funksjonen $f(x,y) = \cos \pi xy$ i punktet $(1, 1/2)$ i retnignen til $\nabla f(1/2,1)$ er $|\nabla f(1/2,1)| = \pi\sqrt{5/4}$.

$\boxed{5}$ La $f(x,y) = 3x^2 y - 6xy + 2y^3 - 3y$

a) Gradienten til $f(x,y)$ er $\nabla f = f_x(x,y)\,\mathbf{\hat{i}} + f_y(x,y)\,\mathbf{\hat{j}} = (6xy - 6y)\,\mathbf{\hat{i}} + (3x^2 - 6x + 6y^2 - 3)\,\mathbf{\hat{j}}$. De andrederiverte av $f(x,y)$ er $f_{xx}(x,y) = 6y$, $f_{yy}(x,y) = 12y$ og $f_{xy}(x,y) = 6x - 6$.

b) Man finne de kritiske punkter til $f(x,y)$ til å løse likingen $\nabla f = \mathbf{0}$. Dvs. $f_x(x,y) = 6xy - 6y = 0$ og $f_y(x,y) = 3x^2 - 6x + 6y^2 - 3$. Fra $6xy - 6y = 0$ har vi at $x = 1$ eller $y = 0$. **Første tilfelle** $(x = 1)$ gir andre likning $f_y(1,y) = 6y^2 - 6 = 0$ som er ekivalent med at $y = -1$ eller $y = 1$. **Andre tilfelle** $(y = 0)$ gir andre likning $f_y(x,0) = 3x^2 - 6x - 3 = 0$ som har løsninger $x = 1 \pm \sqrt(2)$. Vi har derfor 4 kritiske punkter $(1,-1)$, $(1,1)$, $(1-\sqrt{2}, 0)$ og $(1+\sqrt{2}, 0)$.

punkt	f_{xx}	f_{yy}	f_{xy}	$f_{xx}f_{yy} - f_{xy}^2$	Type
$(1,-1)$	-6	-12	0	72	Lokalt Max
$(1,1)$	6	12	0	72	Lokalt Min
$(1+\sqrt{2}, 0)$	0	0	$6\sqrt{2}$	-72	Sadel
$(1-\sqrt{2}, 0)$	0	0	$-6\sqrt{2}$	-72	Sadel

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 $(1,0)$ La $g(x,y) = x^2 - 2x + y^2$ Vi setter opp Lagrange for problemet. $\nabla f = \lambda \nabla g$, $g(x,y) = 0$. Det gir likningene

$$\begin{aligned} 6xy - 6y &= \lambda(2x - 2) \\ 3x^2 - 6x + 6y^2 - 3 &= \lambda 2y \\ x^2 - 2x + y^2 &= 0 \end{aligned}$$

Fra liking 1 har vi at $x = 1$ eller $\lambda = 3y$.

$(x = 1)$ Innsatt i 3.je likning får vi $1 - 2 + y^2 = 0$ som gir $y = 1$ eller $y = -1$.

$(\lambda = 3y)$ Innsatt i 2.re likning får vi $3x^2 - 6x + 6y^2 - 3 = 6y^2$. Opprydning gir $3x^2 - 6x - 3 = 0$. Vi trekker fra 3 ganger 3.je liking og får $-3 - y^2 = 0$ som ikke har en reell løsning. Vi har derfor kun to kritiske punkter $(1,-1)$ og $(1,1)$. Fra deloppgave b har vi de samme punktene. $(1,-1)$ er globalt max og $(1,1)$ er globalt min. Verdiene er $f(1,-1) = 4$ og $f(1,1) = -4$.

$\boxed{6}$ Eksisterer følgende grense? Regn også ut grenseverdien hvis den eksisterer. Vi skriver om ved å gange med $\sqrt{x^2+y^2+1}+1$ oppe og nede i brøken.

$$\begin{aligned}
\lim_{(x,y)\to(0,0)} \frac{x^2+y^2}{\sqrt{x^2+y^2+1}-1} &= \lim_{(x,y)\to(0,0)} \frac{(x^2+y^2)(\sqrt{x^2+y^2+1}+1)}{(\sqrt{x^2+y^2+1}-1)(\sqrt{x^2+y^2+1}+1)} \\
&= \lim_{(x,y)\to(0,0)} \frac{(x^2+y^2)(\sqrt{x^2+y^2+1}+1)}{x^2+y^2} = \lim_{(x,y)\to(0,0)} (\sqrt{x^2+y^2+1}+1) = 2.
\end{aligned}$$

Grensen eksisterer og grensen er 2.