Noregs teknisk–naturvitskaplege
universitet
Institutt for Datateknologi og Informatikk

Løsningsforslag

1 (i) **a)** Vi ser at $g(0) = 1$, $g(1) = 2$, $g(2) = 4$, og $g(3) = 3$. Videre har vi $f(0) = h(g(0)) = 2$, $f(1) = h(2) = 4$, $f(2) = h(4) = 0$, $f(3) = h(3) = 6$. Vi ser da at f er både injektiv og surjektiv.

(ii) Funksjonen $h : \mathbb{R} \to \mathbb{R}$ gitt ved $h : x \mapsto x^3$. har invers $h^{-1}(x) = \sqrt[3]{x}$. Den er derfor bijektiv. En injektiv funksjon er både surjektiv og injektiv.

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

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

b) Funksjonen er ikke surjektiv fordi ingen n i $\{0,1,2,3\}$ gir verdien $g(n) = 2$ nås og **a)** ikke injektiv fordi $g(0) = g(2)$ og $0 \neq 2$.

(iv) Funksjonen $m : \mathcal{P}(\{0,1\}) \to \mathcal{P}(\{0,1,2,3\})$ gitt ved $m : A \mapsto \#A + \#(A \cap \{0\})$ er både surjektiv og injektiv. Vi har $m(\{0,1\}) = 2 + 1 = 3$, $m(\emptyset) = 0 + 0 = 0$, $m(\{0\}) = 1 + 1 = 2$ og $m(\{1\}) = 1 + 0 = 1$.

2 a) Differensligningen $a_k = 5a_{k-1} - 4a_{k-2}$ løses ved å løse karakteristisk ligning $t^2 = 5t - 4$. Oppryddning i likningen gir $t^2 - 5t + 4 = 0$ som er det samme som $(t-4)(t-1) = 0$. Røttene er derfor $t_1 = 4$ og $t_2 = 1$. Generell løsning av diferenslikningen er $a_n = A\,4^n + B\,1^n = A\,4^n + B$.

b) **Startsteg.** Vi sjekker først startverdiene $b_0 = 0 + 1 = 1$ som er OK og $b_1 = 1 + 1 = 2$ som også er OK. Vi skekker så om likningen er tilfredstilt: **Induksjonsteg.** Anta at løsningen av likningen er $b_n = n + 1$ for alle $n < k$ der $k \geq 2$. Da er

$$b_k = 5b_{k-1} - 4_{k-2} - 2 = 5(k-1+1) - 4(k-2+1) - 3 = 5k - 4(k-1) - 3 = 5k - 4k + 4 - 3 = k + 1.$$

c) Siden a_n er generell løsning av og b_n er løsninger av likningene i a) og b) så er

$$\begin{aligned} c_n &= a_n + b_n \\ &= 5a_{n-1} - 4a_{n-2} + 5b_{n-1} - 4b_{n-2} - 3 \\ &= 5(a_{n-1} + b_{n-1}) - 4(a_{n-2} + b_{n-2}) - 3 \\ &= 5c_{n-1} - 4c_{n-2} - 3. \end{aligned}$$

3 a) (i) Først er $230 : 33 = 6$ med 32 i rest. $33 : 32 = 1$ med 1 i rest. Det betyr at $\gcd(230, 33) = 1$. 33 har en multiplikativ invers modulo 230 fordi $\gcd(230, 33) = 1$. Vi finner den inverse ved å bruke Eulers utvidede metode.

$$\begin{aligned} 1 &= 33 - 32 \\ 1 &= 33 - (230 - 6 \cdot 33) \\ 1 &= 7 \cdot 33 - 230 \end{aligned}$$

Siden $7 \cdot 33 \equiv 1 \pmod{230}$ er 7 invers til 230 modulo 33.

(ii) For å finne $65^7 \pmod{517}$ regner vi ut $65^2 = 4225 \equiv 89 \pmod{517}$, $65^4 \equiv 89^2 = 7921 \equiv 166 \pmod{391}$. Da er $65^7 = 65^4 \cdot 65^2 \cdot 65 \equiv 166 \cdot 89 \cdot 65 = 960310 \equiv 241 \pmod{517}$.

b) Et RSA-kryptosystem er bassert på primtallene $p = 11$ og $q = 47$.

(i) Vi har $n = pq = 517$. Vi kan bruke $(517, 7)$ som offentlig nøkkel fordi $(p-1)(q-1) = 460$ og $\gcd(460, 7) = 1$ fordi 7 er et primtall og 7 deler ikke 460. Den offentlige nøkkelen er den multiplikative inverse til 7 modulo 460. Den multiplikative inversen fås ved å bruke Euklids utvidede algoritme.

$$460 : 7 = 65 \text{ med } 5 \text{ i rest}$$

$$7 : 5 = 1 \text{ med } 2 \text{ i rest}$$

$$5 : 2 = 2 \text{ med } 1 \text{ i rest}$$

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3 \cdot (460 - 65 \cdot 7) - 2 \cdot 7 = 3 \cdot 460 - 197 \cdot 7.$$

Den multiplikative inversen til 7 modulo 460 er $-197 \equiv 263 \pmod{460}$. Den private nøkkelen er $(517, 263)$.

(ii) Vi har 263=256+4+2+1.

$$241^2 \equiv 177 \ (mod\ 517)$$

$$241^4 \equiv 177^2 \equiv 309 \ (mod\ 517)$$

$$241^8 \equiv 309^2 \equiv 353 \ (mod\ 517)$$

$$241^{16} \equiv 353^2 \equiv 12 \ (mod\ 517)$$

$$241^{32} \equiv 12^2 \equiv 144 \ (mod\ 517)$$

$$241^{64} \equiv 144^2 \equiv 56 \ (mod\ 517)$$

$$241^{128} \equiv 56^2 \equiv 34 \ (mod\ 517)$$

$$241^{256} \equiv 34^2 \equiv 122 \ (mod\ 517)$$

$$241^{263} = 241^{1+2+4+256} = 241 \cdot 241^2 \cdot 241^4 \cdot 241^{256} \equiv 241 \cdot 177 \cdot 309 \cdot 122$$

$$\equiv 263 \cdot 309 \cdot 122 \equiv 98 \cdot 122 \equiv 65 \ (mod\ 517).$$

Svaret er 65.

Alternativt:

(i) Vi har $n = pq = 517$. Vi kan bruke $(517, 7)$ som offentlig nøkkel fordi $lcm(p-1, q-1) = 230$ og $\gcd(230, 7) = 1$ fordi 7 er et primtall og 7 deler ikke 230. Den offentlige nøkkelen er den multiplikative inverse til 7 modulo 230. Den multiplikative inversen fås ved å bruke Euklids utvidede algoritme.

$$230 : 7 = 32 \text{ med } 6 \text{ i rest}$$

$$7 : 6 = 1 \text{ med } 1 \text{ i rest}$$

$$1 = 7 - 6 = 7 - (230 - 7 \cdot 32) = 7 \cdot 33 - 230$$

Den multiplikative inversen til 7 modulo 230 er 33. Den private nøkkelen er $(517, 33)$.

(ii) Vi har 33=32+1.

$$241^2 \equiv 177 \ (mod\ 517)$$

$$241^4 \equiv 177^2 \equiv 309 \ (mod\ 517)$$

$$241^8 \equiv 309^2 \equiv 353 \ (mod\ 517)$$

$$241^{16} \equiv 353^2 \equiv 12 \ (mod\ 517)$$

$$241^{32} \equiv 12^2 \equiv 144 \ (mod\ 517)$$

$$241^{33} = 241^{1+33} = 241 \cdot 241^{33} \equiv 241 \cdot 144$$

$$\equiv 65 \ (mod\ 517).$$

Svaret er 65.

Alternativt kunne vi brukt at $65^7 \equiv 241 \pmod{517}$. Vi kan bruke resultatet fra 3aii til å skrive $241^{33} = (65^7)^{33} = (65^e)^d \equiv 65 \pmod{517}$.

4 a) Om vi setter inn $y = 0$ i formelen over får vi

$$f(x,0) = \frac{x \cdot 0}{x^2 + 0} = 0$$

. Om vi setter inn $x = 0$ i formelen over får vi

$$f(0,y) = \frac{0 \cdot x}{0 + y^2} = 0$$

. De partsielle deriverte i $(0,0)$ blir da

$$f_x(0,0) = \lim_{h\to 0} \frac{f(0+h,0) - f(0,0)}{h} = \lim_{h\to 0} \frac{0-0}{h} = 0$$

$$f_y(0,0) = \lim_{h\to 0} \frac{f(0,0+h) - f(0,0)}{h} = \lim_{h\to 0} \frac{0-0}{h} = 0.$$

b) Vi bruker regel for å derivere en brøk. Vi finner

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

og

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

c) $f(x,y)$ er ikke kontinuerlig i $(0,0)$. Det ser vi fordi grensen $\lim_{x\to 0} f(x,x) = 1/2 \neq 0 = f(0,0)$.

5 Gitt funksjonen $f(x,y) = x^2y^2 - x^2 - 2y^3 - 3y^2$.

a) Gradienten til $f(x,y)$ er $\nabla f = f_x(x,y)\,\hat{\mathbf{i}} + f_y(x,y)\,\hat{\mathbf{j}} = 2x(y^2-1)\,\hat{\mathbf{i}} + (2x^2y - 6y^2 - 6y)\,\hat{\mathbf{j}}$. De andrederiverte av $f(x,y)$ er $f_{xx}(x,y) = 2(y^2-1)$, $f_{xy}(x,y) = 4xy$ og $f_{yy}(x,y) = 2x^2 - 12y - 6$.

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

punkt	f_{xx}	f_{yy}	f_{xy}	$f_{xx}f_{yy} - f_{xy}^2$	Type
$(0,0)$	-2	-6	0	12	Lokalt Max
$(0,-1)$	0	6	0	0	Uavklart
$(-\sqrt{6},1)$	0	-6	$-4\sqrt{6}$	-96	Sadel
$(\sqrt{6},1)$	0	-6	$4\sqrt{6}$	-96	Sadel

c) Finn største og minste verdi av $f(x,y)$ på området $D = \{(x,y) \in \mathbb{R}^2 | x^2 + y^2 \leq 1\}$, det vil si sirkelskiven med radius 1 og senter i punktet $(0,0)$.

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

$$\begin{aligned} 2x(y^2-1) &= 2x\lambda \\ 2y(x^2-3y-3) &= 2y\lambda \\ x^2+y^2 &= 1 \end{aligned}$$

Fra første likning har vi $x = 0$ eller $\lambda = y^2 - 1$. Fra andre likning har vi at $y = 0$ eller $\lambda = x^2 - 3y - 3$

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

$(y = 0)$ Innsatt i 3.re likning gir $x^2 = 1$ som gir $x = 1$ eller $x = -1$.

$(\lambda = \lambda)$ gir

$$y^2 - 1 = x^2 - 3y - 3$$

Vi bruker $x^2 = 1 - y^2$ fra tredje likning og erstatter x^2 med $1 - y^2$:

$$y^2 - 1 = 1 - y^2 - 3y - 3$$

Opprydning gir $2y^2 + 3y + 1 = 0$. Faktorisering gir $(2y+1)(y+1) = 0$. Vi løser og får $y = -1$ eller $y = -1/2$. Det gir punktene $(0, -1)$, $(-\sqrt{3}/2, -1/2)$ og $(\sqrt{3}/2, -1/2)$ Vi har derfor til sammen 6 kritiske punkter på randen. I tillegg er $(0, 0)$ et kritisk punkt innenfor randen.

(x, y)	$f(x, y)$
$(0, 0)$	0
$(1, 0)$	-1
$(-1, 0)$	-1
$(0, 1)$	-5
$(0, -1)$	-1
$(\sqrt{3}/2, -1/2)$	-17/16
$(-\sqrt{3}/2, -1/2)$	-17/16

$(0, 0)$ er globalt max og $(0, 1)$ er globalt min. Verdiene er $f(0, 0) = 0$ og $f(0, 1) = -5$.

d) Finn største og minste verdi av $f(x, y)$ på på området begrenset av kvadratet med hjørner $A(-1, -1)$, $B(1, -1)$, $C(1, 1)$ og $D(-1, 1)$.

Løsning. Vi har $f(x, 1) = -5$ og $f(x, -1) = -1$. Videre er $f(-1, y) = f(1, y) = -2y^3 - 2y^2 - 1$. og $f_y(-1, y) = f_y(1, y) = -4y - 6y^2 = -2y(2 + 3y)$. Kritiske punkter er $y = 0$ og $y = -2/3$. I de kritiske punktene og i hjørnene er $f(\pm 1, 1) = -5$, $f(\pm 1, -1) = -1$, $f(\pm 1, 0) = -1$, og $f(\pm 1, -2/3) = -2y^3 - 2y^2 - 1 = -35/27$. Det er et kritisk punkt $(0, 0)$ inne i området. $f(0, 0) = 0$ Vi får derfor maksverdi 0 og minimumsverdi -5.