Løsningsforslag TDAT2002 Matematikk 1, DE2
AITeL, Høgskolen i Sør-Trøndelag

Desember 2015

Oppgave 1 (20%)

a) (i) Denne funksjonen er ikke en-til-en siden $f(3) = f(5)$ selv om $3 \neq 5$. (Dette er altså et moteksempel, og beviser at funksjonen ikke er en-til-en).

(ii) Denne funksjonen er en-til-en på grunnlag av følgende bevis:

Anta at $g(x_1) = g(x_2)$. Da er $x_1 - 3 = x_2 - 3$. Det betyr at $x_1 = x_2$. Altså ser vi at $g(x_1) = g(x_2) \Rightarrow x_1 = x_2$, så funksjonen er en-til-en.

(iii) Denne er heller ikke en-til-en, noe vi kan se på grunnlag av følgende moteksempel:

La $n_1 = 2$, og $n_2 = 3$. Da er $h(n_1) = 1 = h(n_2)$ fordi begge er primtall, men $n_1 \neq n_2$. Altså er ikke funksjonen en-til-en.

(iv) Denne er heller ikke en til en, fordi to par av mengder kan ha samme snitt uten at de to parene er like. For eksempel som følger:

La $A_1 = \{0\}, B_1 = \{1\}, A_2 = \{2\}, B_2 = \{3\}$. Da er $A_1 \cap B_1 = \varnothing = A_2 \cap B_2$, men de to parene av mengder er ikke like. Altså er ikke funksjonen en-til-en.

b) (i) Denne funksjonen er surjektiv fordi $f(1) = x, f(3) = y$ og $f(7) = z$. Altså "treffes" alle elementer i B av noe i A.

(ii) Denne funksjonen er surjektiv ved følgende argument:

La $y \in \mathbb{R}$. Da er $g(y + 3) = (y + 3) - 3 = y$, så vi ser at det eksisterer et element $y + 3 \in \mathbb{R}$ slik at $g(y + 3) = y$ uansett hva y er.

(iii) Denne er også surjektiv fordi $h(2) = 1$ og $h(4) = 0$. Altså treffes alle elementer i $\{0, 1\}$.

(iv) Denne er surjektiv. Hvorfor?

La $M \in \mathcal{P}(\mathbb{R})$. Da er $M \subseteq \mathbb{R}$. Da er (for eksempel)

$$m(\mathbb{R}, M) = \mathbb{R} \cap M = M,$$

så det finnes et par av mengder i $\mathcal{P}(\mathbb{R}) \times \mathcal{P}(\mathbb{R})$ som treffer M under funksjonen m.

Oppgave 2 (20%)

a) i) Dette er en sann påstand. Det kan vi for eksempel se vha. mengdelovene som følger:

$$
\begin{aligned}
(A - B) \cup (A \cap B) &= (A \cap B^c) \cup (A \cap B) && \text{(Mengdedifferanseloven)} \\
&= A \cap (B^c \cup B) && \text{(Distributiv lov)} \\
&= A \cap \mathcal{U} && \text{(Negasjonslov)} \\
&= A && \text{(Identitetslov)}
\end{aligned}
$$

ii) Denne påstanden er usann. Et moteksempel følger:

La $\mathcal{U} = \mathbb{Z}, A = \{1\}, B = \{1, 2\}$ og $C = \{1, 3\}$. Da er

- $B \cap C = \{1\}$, mens
- $A^c \cap (B \cup C) = A^c \cap \{1, 2, 3\} = \{2, 3\}$.

Her ser vi at $B \cap C \nsubseteq A^c \cap (B \cup C)$.

b) Skal vise ved matematisk induksjon at formelen $a_n = 3^n - 1$ løser differensligningen

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

- **Basissteg:** $3^0 - 1 = 1 - 1 = 0$, så vi ser at påstanden holder for $n = 0$.
- **Induktivt steg:** Anta at formelen gjelder for a_k, dvs. at

$$a_k = 3^k - 1.$$

Da får vi følgende for a_{k+1}:

$$
\begin{aligned}
a_{k+1} &= 3a_k + 2 = 3 \cdot (3^k - 1) + 2 \\
&= 3^{k+1} - 3 + 2 = 3^{k+1} - 1,
\end{aligned}
$$

så formelen stemmer også for a_{k+1} og løsningen over er gyldig ved matematisk induksjon.

Oppgave 3 (20%)

a) i) Skal finne $\gcd(924, 103)$ og avgjøre om 103 har en invers modulo 924.

$$
\begin{aligned}
924 &= 103 \cdot 8 + 100 \\
103 &= 100 \cdot 1 + 3 \\
100 &= 3 \cdot 33 + 1
\end{aligned}
$$

Vi ser at $\gcd(924, 103) = 1$, så tallene er relativt primiske. Da vet vi ut fra pensum at 103 har en invers modulo 924.

ii) Regner ut $22^{25} \pmod{28}$ og $42^{25} \pmod{989}$ med metoden i pensum. Finner først at

$$25 = 16 + 8 + 1.$$

Finner så de relevante toerpotensene for 22 modulo 28:

$$\begin{aligned} 22^2 &\equiv 22^2 \equiv 484 \equiv 8 \pmod{28} \\ 22^4 &\equiv 8^2 \equiv 64 \equiv 8 \pmod{28} \\ 22^8 &\equiv 8^2 \equiv 8 \pmod{28} \\ 22^{16} &\equiv 8^2 \equiv 8 \pmod{28} \end{aligned}$$

Altså blir

$$\begin{aligned} 22^{25} &\equiv 22^{16+8+1} \equiv 22^{16} \cdot 22^8 \cdot 22 \pmod{28} \\ &\equiv 8 \cdot 8 \cdot 22 \equiv 8 \cdot 22 \equiv 8 \pmod{28}. \end{aligned}$$

Neste regnestykke:

$$\begin{aligned} 42^2 &\equiv 1764 \equiv 775 \pmod{989} \\ 42^4 &\equiv 775^2 \equiv 600625 \equiv 302 \pmod{989} \\ 42^8 &\equiv 302^2 \equiv 91204 \equiv 216 \pmod{989} \\ 42^{16} &\equiv 216^2 \equiv 46656 \equiv 173 \pmod{989} \end{aligned}$$

Altså blir

$$\begin{aligned} 42^{21} &\equiv 42^{16+8+1} \equiv 42^{16} \cdot 42^8 \cdot 42 \pmod{989} \\ &\equiv 173 \cdot 216 \cdot 42 \equiv 902 \pmod{989}. \end{aligned}$$

b) Skal sette opp et RSA-system basert på primtallene $p = 43$ og $q = 23$. Da blir $n = 989$, som vi kjenner igjen som et av tallene fra a).

i) Vi ser at $(p-1)(q-1) = 60 \cdot 22 = 924$, og den første utregningen fra a) viser at 103 har en invers modulo 924. Altså kan vi bruke den som offentlig nøkkel. Den private nøkkelen blir $(989, d)$, der d er en positiv invers til 103 modulo 924. Finner en slik invers ved Euklids utvidede metode (bruker utregningen fra a)):

$$\begin{aligned} 1 &= 100 - 3 \cdot 33 \\ &= 100 - (103 - 100) \cdot 33 = 100 \cdot 34 - 103 \cdot 33 \\ &= (924 - 103 \cdot 8) \cdot 34 - 103 \cdot 33 = 924 \cdot 34 + 103 \cdot (-305) \end{aligned}$$

Vi trenger en positiv invers, så vi kan bruke $-305 + 924 = 619$. Den private nøkkelen er altså $(989, 619)$.

ii) For å kryptere 42, må vi finne $42^{103} \pmod{989}$. Men vi regnet ut $42^{25} \pmod{989}$ i a), så vi kan bruke denne utregningen for å komme raskt i mål. Deler opp 103 i potenser vi allerede har regnet ut, dvs. $25 \cdot 4 + 2 + 1$:

$$\begin{aligned}
42^{103} &\equiv 42^{25\cdot 4+2+1} \equiv (42^{25})^4 \cdot 42^2 \cdot 42 \pmod{989} \\
&\equiv 902^4 \cdot 775 \cdot 42 \equiv (902^2)^2 \cdot 902 \pmod{989} \\
&\equiv 646^2 \cdot 902 \cdot 947 \cdot 902 \equiv 687 \pmod{989}.
\end{aligned}$$

Oppgave 4 (5%)

De partielle deriverte er $f_x = 2xy$, $f_y = x^2 + 4y$ Vi har $z - 3 = f_x(1,1)(x-1) + f_y(1,1)(y-1)$. Det gir $z - 3 = 2(x-1) + 5(y-1)$ eller $2x + 5y - z = 4$.

Oppgave 5 (5%)

Langs linjen $x = y$ er grensen

$$\lim_{x\to 0} q(x,x) = \lim_{x\to 0} = \frac{3x^2}{2x^2} = \frac{3}{2}.$$

Langs linjen $y = -x$ er grensen

$$\lim_{x\to 0} q(x,-1) = \lim_{x\to 0} = \frac{x^2}{2x^2} = \frac{1}{2}.$$

Grensene er forskjellige i de forskjellige retningene. Det gjør at funksjonen ikke er kontinuerlig.

Oppgave 6 (30%)

a)

$$\begin{aligned}
f_x(x,y) &= 6x - 6x \\
f_y(x,y) &= -3x^2 + 4y \\
f_{xx}(x,y) &= 6 - 6y \\
f_{xy}(x,y) &= -6x \\
f_{yy}(x,y) &= 4 \\
\nabla f(x,y) &= 6x(1-y)\mathbf{\hat{i}} + (4y - 3x^2)\mathbf{\hat{j}}
\end{aligned}$$

b) I retningen til gradienten $\nabla f(1,3) = -12\mathbf{\hat{i}} + 9\mathbf{\hat{j}}$ vokser $f(x,y)$ mest. Det vil si i retningen

$$\frac{\nabla f(1,3)}{|\nabla f(1,3)|} = -\tfrac{4}{5}\mathbf{\hat{i}} + \tfrac{3}{5}\mathbf{\hat{j}}$$

I denne retningen er den retningsderiverte lik

$$|\nabla f(1,3)| = 15.$$

c) i)

$$f_x(x, y) = 6x - 6xy = 0$$
$$f_y(x, y) = -3x^2 + 4y = 0$$

Første likning gir $y = 1$ eller $x = 0$ I tilfellet $x = 0$ gir andre likning $y = 0$. I tilfellet $y = 1$ gir andre likning $x = \pm 2/\sqrt{3}$. Vi har derfor 2 kritiske punkter. $(0, 0)$, $(2/\sqrt{3}, 1)$ og $(-2/\sqrt{3}, 1)$.

ii) Vi har

$$D(x, y) = f_{xx} f_{yy} - [f_{xy}(x, y)]^2 = 24 - 24y - 36x^2$$

I punktet $(0, 0)$ er $D = 24$ og $f_{xx} = 6$. Derfor er (0,0) et bunnpunkt. I begge de to andre punktene er $D = -48$ og vi har derfor 2 sadelpunkter.

d)

$$6x - 6xy = 2\lambda x$$
$$-3x^2 + 4y = 2\lambda y$$
$$x^2 + y^2 = 5^2$$

Den første likningen gir $x = 0$ eller $3 - 3y = \lambda$.

I tilfellet $x = 0$ blir de 2 siste likningene

$$4y = 2\lambda y$$
$$y^2 = 25$$

Det gir $y = \pm 5$ (og $\lambda = \pm 2$)

I tilfellet $3 - 3y = \lambda$ blir den andre likningene

$$-3x^2 + 4y = 6y - 6y^2$$

Vi adderer siste likning multiplisert med 3 til denne likningen

$$3y^2 + 4y = 6y - 6y^2 + 75$$

Vi løser denne og får

$$9y^2 - 2y - 75 = 0$$
$$y = \frac{2 \pm \sqrt{4 + 4 \cdot 9 \cdot 75}}{18}$$
$$y = (1 \pm 26)/9$$

$y = 3$ eller $y = -25/9$ Det gir kritiske punkter

$(\pm 4, 3)$ og $(\sqrt{1400}/9, -25/9)$. Vi setter inn i funksjonen og får.

$$f(0, \pm 5) = 50$$
$$f(\pm 4, 3) = -78$$
$$f(\sqrt{1400}/9, -25/9) = 211.3169$$