$\{\forall x = A, G, T | \text{IMA}x2021\}$

LF vår 2022

Noregs teknisk–naturvitskaplege universitet
Institutt for Matematiske Fag
Institutt for Datateknologi og Informatikk

Løsningsforslag

1

La $u = 2 + 3i$ og $v = 1 - 2i$.

Regn ut $u + v$, uv og u/v. Skriv svaret på standard (kartesisk) form.

Løsning:

a) $u + v = (2 + 1) + (3 - 2)i = 3 + i$.

b) $uv = (2 \cdot 1 - 3 \cdot (-2)) + (3 \cdot 1 + 2 \cdot (-2))i = 8 - i$.

c) $u/v = \frac{u\bar{v}}{|v|^2} = \frac{(2\cdot 1 - 3\cdot 2) + (3\cdot 1 + 2\cdot 2)i}{1 + (-2)^2} = -\frac{4}{5} + \frac{7}{5}i$.

2 Faktoriser utrykket $z^2 - 4z + 5$. Svaret må være på formen $(z - z_1)(z - z_2)$, der z_1 og z_2 er komplekse tall på kartesisk form.

Løsning: Vi løser likningen $z^2 - 4z + 5 = 0$ for å finne røttene til $z^2 - 4z + 5$. Abc-formelen gir $z = \frac{-(-4) \pm \sqrt{4^2 - 4 \cdot 1 \cdot 5}}{2}$. Det gir røttene $z_1 = 2 + i$ og $z_2 = 2 - i$. Vi har derfor $z^2 - 4z + 5 = (z - z_1)(z - z_2) = (z - 2 - i)(z - 2 + i)$.

3 Finn alle partielle deriverte av første og andre orden til funksjonen $f(x, y) = x^2y^2 - 9x^2 - y^3/9 + 27y$.

Løsning: Vi deriverer ledd for ledd.

$$\begin{aligned}
\frac{\partial f}{\partial x}(x, y) &= 2x(y^2 - 9) \\
\frac{\partial f}{\partial y}(x, y) &= 2x^2y - y^2/3 + 27 \\
\frac{\partial^2 f}{\partial x^2}(x, y) &= 2y^2 - 18 \\
\frac{\partial^2 f}{\partial x \partial y}(x, y) &= 4xy \\
\frac{\partial^2 f}{\partial y \partial x}(x, y) &= 4xy \\
\frac{\partial^2 f}{\partial y^2}(x, y) &= 2x^2 - 2y/3
\end{aligned}$$

4 Finn og klassifiser alle kritiske punkter til funksjonen $f(x, y) = x^2y^2 - 9x^2 - y^3/9 + 27y$. (Funksjonen er den samme som i forrige oppgave).

Vi finner kritiske punkter ved å sette $\frac{\partial f}{\partial x}(x, y) = \frac{\partial f}{\partial y}(x, y) = 0$.

Først ser vi på $\frac{\partial f}{\partial x}(x,y) = 2x(y^2-9)$ som er null i tre tilfeller, *(i)* x=0, *(ii)* y=3, og *(iii)* y=-3. Vi behandler hvert av tilfellene for seg.

***(i)* x=0.** $\frac{\partial f}{\partial y}(x,y) = 2x^2y - y^2/3 + 27 = -y^2/3 + 27 = 0$, som gir $y = \pm 9$. Kritiske punkter er derfor $(0,9)$ og $(0,-9)$

***(ii)* y=3.** $\frac{\partial f}{\partial y}(x,y) = 2x^2y - y^2/3 + 27 = 6x^2 - 24 = 0$. I dette tilfellet er $x = \pm 2$. Vi har derfor to "nye" kritiske punkter i $(2,3)$ og $(-2,3)$.

***(iii)* y=-3.** $\frac{\partial f}{\partial y}(x,y) = 2x^2y - y^2/3 + 27 = -6x^2 - 24 = 0$. Denne likningen har ingen reelle løsninger.

Vi fant fire kritiske punkter. $(0, \pm 9)$ og $(\pm 2, 3)$.

Vi regner ut diskriminanten $D = f_{xx}f_{yy} - f_{xy}^2$ for de kritiske punktene.

	f_{xx}	f_{yy}	f_{xy}	D	Type
(0,9)	144	-18	0	-2592	Sadel
(0,-9)	144	18	0	2592	Minimum
(2,3)	0	4	24	-576	Sadel
(-2,3)	0	12	-24	-576	Sadel

5 Matrisen $A = \begin{bmatrix} 5 & -7 & 2 \\ 2 & -4 & 2 \\ 2 & 2 & 5 \end{bmatrix}$ har tre forskjellige eigenverdier.

To av egenvektorene til A er gitt ved $v_1 = \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix}$ og $v_2 = \begin{bmatrix} 1 \\ 1 \\ 4 \end{bmatrix}$.

a) Finn egenverdiene λ_1 og λ_2 som hører til egenvektorene v_1 og v_2.
(i) Egenverdien λ_1 som hører til egenvektoren v_1 er -3. Det ser vi ved å multiplisere A med v_1.

$$Av_1 = \begin{bmatrix} 5 & -7 & 2 \\ 2 & -4 & 2 \\ 2 & 2 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \\ -1 \end{bmatrix} = \begin{bmatrix} -6 \\ -6 \\ 3 \end{bmatrix} = -3v_1$$

(ii) Egenverdien λ_2 som hører til egenvektoren v_2 er 6. Det ser vi ved å multiplisere A med v_2.

$$Av_2 = \begin{bmatrix} 5 & -7 & 2 \\ 2 & -4 & 2 \\ 2 & 2 & 5 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 4 \end{bmatrix} = \begin{bmatrix} 6 \\ 6 \\ 24 \end{bmatrix} = 6v_2$$

b) Finn den siste egenverdien til A. Den siste egenverdien til A er $\lambda_3 = 3$. Det kan du finne ut på diverse måter. En er å regne ut karakteristisk polynom

$$p(\lambda) = \det(A - \lambda I) = \begin{vmatrix} 5-\lambda & -7 & 2 \\ 2 & -4-\lambda & 2 \\ 2 & 2 & 5-\lambda \end{vmatrix} =$$

$$= (5-\lambda)\begin{vmatrix} -4-\lambda & 2 \\ 2 & 5-\lambda \end{vmatrix} - (-7)\begin{vmatrix} 2 & 2 \\ 2 & 5-\lambda \end{vmatrix} + 2\begin{vmatrix} 2 & -4-\lambda \\ 2 & 2 \end{vmatrix} =$$

$$= (5-\lambda)\Big((-4-\lambda)(5-\lambda) - 2\cdot 2\Big) + 7\Big(2(5-\lambda) - 2\cdot 2\Big) + 2\Big(2\cdot 2 - 2(-4-\lambda)\Big)$$

$$= -\lambda^3 + 6\lambda^2 + 9\lambda - 54.$$

Det er mange veier videre her. En er å løse likningen $p(\lambda) = 0$. Å løse en tredjegradslikning er ikke enkelt, så vi unngår det. Strategien er å benytte de øvrige to løsningene. Vi utfører polynomdivisjon for å faktorisere $p(\lambda)$. Det gir $p(\lambda) = -(\lambda+3)(\lambda-6)(\lambda-3)$. Det gir røttene, -3,6, og 3.

c) Finn en egenvektor v_3 til A som tilhører egenverdien λ_3.

Løsning: For å finne egenvektoren så løser vi egenverdiproblemet $Av = 3v$:

$$\begin{bmatrix} 5-3 & -7 & 2 & 0 \\ 2 & -4-3 & 2 & 0 \\ 2 & 2 & 5-3 & 0 \end{bmatrix} = \begin{bmatrix} 2 & -7 & 2 & 0 \\ 2 & -7 & 2 & 0 \\ 2 & 2 & 2 & 0 \end{bmatrix} \sim = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Det gir likningene $x + z = 0$ og $y = 0$. Vi har en fri parameter t. Da er $z = t$ og $y = 0$ og $x = -z = -t$. Egenvektorene tilhørende egenverdien 3 er derfor

$$v_3 = \begin{bmatrix} -t \\ 0 \\ t \end{bmatrix}, \quad t \neq 0.$$

Sett for eksempel $t = 1$.

6 La $f(x) = \frac{1}{5-x}$.

a) Finn de tre første leddene i Taylorrekken til $f(x)$ om $x = 2$.

Løsning: Vi har $f(2) = \frac{1}{5-2} = \frac{1}{3}$. Den deriverte av f er $f'(x) = \frac{1}{(5-x)^2}$. Da er $f'(2) = \frac{1}{(5-2)^2} = \frac{1}{9}$. Den andrederiverte er $f''(x) = \frac{2}{(5-x)^3}$. Da er $f''(2) = \frac{2}{(5-2)^3} = \frac{2}{27}$. Taylorpolynomet er av grad 2 (3 ledd i Taylorrekken) er

$$p_2(x) = \frac{f(2)}{0!} + \frac{f'(2)}{1!}(x-2) + \frac{f''(2)}{2!}(x-2)^2 = \frac{1}{3} + \frac{1}{9}(x-2) + \frac{1}{27}(x-2)^2.$$

b) Hva er konvergenssenteret til Taylorrekken i oppgave a? Vi fortsetter og finner

Løsning: Vi regner ut $f'''(x) = \frac{6}{(5-x)^4}$. Da er $f'''(2) = \frac{6}{(5-2)^4} = \frac{2}{27}$. Det fjerde leddet i Taylorrekken er derfor $\frac{f'''(2)}{6!}(x-2)^3 = \frac{1}{81}(x-2)^3$. Vi ser et mønster om at hvert ledd ser ut til å være på formen $\frac{1}{3^{n+1}}(x-2)^n$. Vi gjenkjenner det som starten på den geometriske rekken

$$\sum_{n=0}^{\infty} ar^n$$

med $a = \frac{1}{3}$ og $r = \frac{x-2}{3}$. Den konvergerer for $|r| < 1$ og har sum lik

$$\frac{a}{1-r} = \frac{1/3}{1-\frac{x-2}{3}} = \frac{1}{5-x}.$$

Denne konvergerer altså når $|r| = |x-2|/3 < 1$. Dvs, når $-1 < (x-2)/3 < 1$. Multipliserer med 3 i alle tre leddene: $-3 < x - 2 < 3$. Konvergenssenteret er derfor 2.

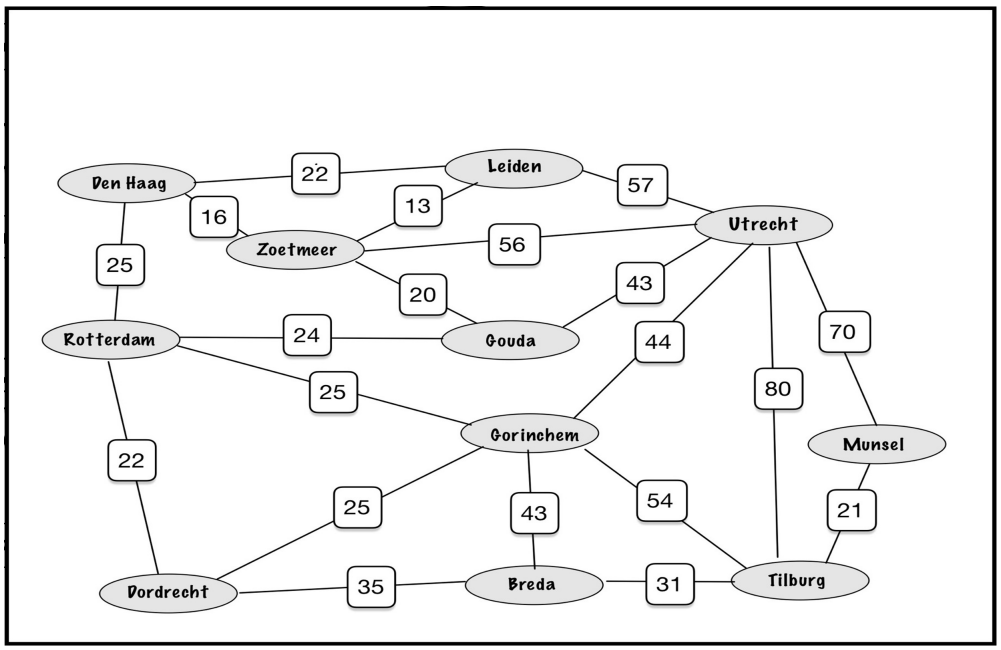
c) Hva er konvergensradiusen til Taylorrekken i oppgave a?

Løsning: Fra $-3 < x - 2 < 3$ finner vi konvergensradius til å være 3.

d) Hva er riktig for endepunktene til konvergensintervalet til Taylorrekken i oppgave a?

Løsning: Fra $-3 < x - 2 < 3$ finner vi at det er ikke konvergens i endepunktene.

7 Du skal benytte Prims algoritme til å finne det minimale utspennende treet. Du skal starte i Den Haag. Om du har to muligheter for valg av neste kant så kan du velge den du vil.



Trinn:		0	1	2	3	4	5	6	7	8	9	10
Den Haag—Leiden	22	+	–	x								
Den Haag—Zoetmeer	16	+	1									
Den Haag—Rotterdam	25	+	–	–	–	x						
Zoetmeer—Leiden	13		+	2								
Zoetmeer—Utrecht	56		+	–	–	–	–	–	–	–	–	x
Zoetmeer—Gouda	20		+	–	3							
Leiden–Utrecht	57			+	–	–	–	–	–	–	–	x
Gouda—Rotterdam	24				+	4						
Gouda—Utrecht	43				+	–	–	–	–	–	–	10
Rotterdam—Gorinchem	25					+	–	6a				
Rotterdam—Dordrecht	22					+	5					
Dordrecht—Breda	35						+	–	7			
Dordrecht—Gorinchem	25						+	6b				
Gorinchem—Utrecht	44							+	–	–	–	x
Gorinchem—Tilburg	54							+	–	x		
Gorinchem—Breda	43							+	x			
Breda—Tilburg	31								+	8		
Tilburg—Utrecht	80									+	–	x
Tilburg—Munsel	21									+	9	
Munsel—Utrecht	70										+	x

Tabellen over viser Prims algoritme. Hver søyle er et trinn. Vi starter med å legge til alle kanter som grenser til **Den Haag**. Vi markerer disse med +. Vi velger den korteste av disse (Den Haag–Zoetmeer 16) og markerer raden med tallet 1 i trinn 2. Vi legger til kanter fra Zoetmeer (+). Alternativer nå er markert med – og +. Vi velger den korteste (Zoetmeer—Leiden 13) og legger til Leiden–Utrecht. Vi fjerner (x) Den Haag—Leiden for å ungå en krets. Slik fortsettes det og vi får fasiten.

Kantene legges til i følgende rekkefølge: Den Haag–Zoetmeer (1), Zoetmeer–Leiden (2), Zoetmeer–Gouda (3), Gouda–Rotterdam (4), Rotterdam–Dordrecht (5), Rotterdam–Gorinchem eller Dordrecht–Gorinchem (6), Dordrecht–Breda (7), Breda–Tilburg (8), Tilburg–Munsel (9), og Gouda–Utrecht (10).

8 Et tre med 5 noder har 4 kanter. Det lineære treet

```
1-2-3-4-5   (Tre 1)
```

har grader 1,2,2,2,1. Alle trær som har disse gradene må være isomorfe. Om vi tar bort –5 og limer det på i node 3 så får vi et tre med grader 3,2,1,1,1.

```
    5
    |
1-2-3-4     (Tre 2)
```

Det er bare en mulighet med et tre med fem hjørner der et av de har grad 3. Om vi fjerner 1– fra dette treet så får vi

```
  5
  |
2-3-4       (Tre 3)
  |
  1
```

som har grader 41111. Et tre med fem hjørner og et hjørne med grad 4 må ha grader 41111, da er det bare en mulighet. Vi kan ikke fortsett med en node med grad 5, da hver av de fem kantene må gå til et unikt element, med det er bare 4 kandidater. Derfor slutter det her.

For å fullføre må vi tegne de komplementære grafene. Komplementærgrafen til tre 1 er

```
  1-4          2             5-2
 /| |         /|\           /|/
3-5-2        1-+-3  3      3-1-4
              \|/
               4
```

9 *i.)* Gitt følgende pseudokode:

```
if(a){
    if(b){
        run();
    }
    else if(not c){
        run();
    }
}
```

Hvilke logiske utsagn korresponderer til de tilfellene der funksjonen run() blir kjørt? Finn alle riktige svaralternativer.

Løsning: For at koden skal kjøre må a være sann. I tillegg må b være sann eller c ikke være sann. `run()` kjøres derfor hvis $a \wedge (b \vee \neg c)$ er sann. Det er alternativ (i.) i listen nedenfor.

(i.) $a \wedge (b \vee \neg c)$ er riktig. (Se forklaring over).

(ii.) $(a \wedge b) \vee (a \wedge \neg c)$ er riktig da den er ekvivalent med (i.) som er riktig. (Distributiv lov.)

(iii.) $a \wedge \neg(\neg b \wedge c)$ er riktig da den er ekvivalent med (i.) som er riktig. (De Morgans lov.)

(iv.) $a \vee (b \wedge \neg c)$ er ikke riktig da den kan være sann når a er usann. ($b = S$ og $c = U$), men da kjøres ikke `run()`.

(v.) $(a \vee b) \wedge (a \vee \neg c)$ er ikke riktig, da den er ekivalent med (iv.) som ikke er riktig. (Distributiv lov).

(vi.) $a \to (b \vee \neg c)$ er ikke riktig da sannhetsverdien er sann alltid når a er usann, men da kjøres ikke `run()`.

ii.) La P, Q og R være mengder med universalmengde U. Gitt følgende pseudokode der vi bruker mengdeoperasjoner og P, Q, R og U er av datatype set (mengde):

```
clear(R);             // fjern alle elementene fra R
for u in U{           // for alle elementene u i U:
    add(R, u);        // legg til element u i R
}
for p in P{
    remove(R, p);     // fjern element p fra R
}
for q in Q{
    add(R, q);
}
```

Hvilke sammensatte mengder korresponderer til mengde R etter at denne koden er kjørt? Finn alle riktige svaralternativer.

Løsning:

1. Første for-løkke legger til alle elementene i U til R, vi har da U.
2. Andre for-løkke tar bort alle elementer i P fra R. Vi har da $(U - P)$
3. Tredje for-løkke legger til alle elementene i Q. Vi har da unionen $(U - P) \cup Q$. Alternativ (i.)

(i.) $(U - P) \cup Q$ er riktig. (Se forklaring over.)

(ii.) $\overline{P} \cup Q$ er riktig da den er ekivalent med (i.). ($\overline{P} = (U - P)$ per definisjon).

(iii.) $\overline{P \cap \overline{Q}}$ er riktig da den er ekivalent med (ii.). (De Morgans lov)

(iv.) $U - (P \cup Q)$ er **ikke** riktig. (Inneholder ingen av elementene fra P.)

(iv.) $\overline{P} \cap Q$ er **ikke** riktig. (Inneholder ingen av elementene fra P.)

(v.) $\overline{P \cup \overline{Q}}$ er **ikke** riktig da den er ekivalent med (iv.), (De Morgans lov.))

10 Hvilke utsagn er negasjoner av følgende utsagn?

$$\forall n \in \mathbb{Z}, n|36 \to (n|4 \vee n|9)$$

Angi alle riktige alternativer.

Løsning: Alle alternativene er negasjoner av utsagnet.

(i.) $\exists n \in \mathbb{Z}, \neg(n|36 \to (n|4 \vee n|9))$, er negasjon da det kommer direkte fra $\neg(\forall n \in S, p(n)) \Leftrightarrow \exists n \in S, \neg p(n)$.

(ii.) $\exists n \in \mathbb{Z}, \neg(\neg(n|36) \vee (n|4 \vee n|9))$ er en omskrivning der vi har brukt at $p \to q$ er ekivalent med $\neg p \vee q$.

(iii.) $\exists n \in \mathbb{Z}, n|36 \wedge \neg(n|4 \vee n|9)$. De Morgans lov er anvendt på (ii.)

(vi.) $\exists n \in \mathbb{Z}, n|36 \wedge (\neg(n|4) \wedge \neg(n|9))$. De Morgans lov er anvendt på (iii.)

(v.) $\exists n \in \mathbb{Z}, n|36 \wedge \neg(n|4) \wedge \neg(n|9)$. Parantesene er overflødige.

11 La universalmengden være $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Skriv følgende på formen $\{a_1, \cdots, a_n\}$ der a_i, $i = 1 \cdots n$ er elementene i mengden. F. eks.: Mengden som inneholder elementene 2 og 3 kan noteres som $\{2, 3\}$

Løsning:

(i.) $\{x \in S | 5x \in S\} = \{0, 1, 2\}$.

(ii.) $\{x \in S | (x-3)^2 \in S\} = \{0, 1, 2, 3, 4, 5, 6\}$

(iii.) $\{x \in S | (x-1)/3 \in \mathbb{Z}\} = \{1, 4, 7, 10\}$

(iv.) $\{x \in S | \exists y \in S\ (x = \sqrt{2y})\} = \{0, 2, 4\}$

(v) $\{x \in S | \exists y \in S \forall z \in S\ (x = yz)\} = \{0\}$

12 Haakon, Olav og Harald er i en iskrembar og skal velge is. På menyen er det 8 smaker kuleis.

a) Haakon vil bestille 3 kuler med 3 forskjellige smaker stablet i høyden. Kulenes plassering har betydning for Haakon da han gjerne vil spise dem i en gitt rekkefølge.

(i.) Hva slags problem er dette? (ii.) Hvilken utregning er riktig? (iii.) Hvor mange valgmuligheter har Haakon?

Løsning. (i.) Dette er et problem uten tilbakelegging da samme smak ikke kan velges mer enn en gang. Det er et ordnet utvalg da rekkefølgen har en betydning.

(ii.) Vi finner antall muligheter $8P3 = \frac{8!}{(8-3)!}$.

(iii.) Haakon har 336 valgmuligheter.

b) Olav vil bestille is i beger. Han vil ha 4 iskuler med 4 forskjellige smaker. Han er ikke opptatt av hvordan isen ligger i skålen. Det er tilfeldig i hvilken rekkefølge han bestiller iskulene.

(i.) Hva slags problem er dette? (ii.) Hvilken utregning er riktig? (iii.) Hvor mange valgmuligheter har Olav?

Løsning. (i.) Dette er et problem uten tilbakelegging da samme smak ikke kan velges mer enn en gang. Utvalget er uordnet da rekkefølgen ikke har noe å si. (ii.) $8C4 = \binom{8}{4}$ er riktig formel. (iii.) Olav har 70 forskjellige valgmuligheter.

c) Harald har oppdaget at han kan velge samme smak flere ganger. Han vil kjøpe 5 iskuler. Rekkefølgen har ikke noe å si og iskulene kan ha samme smak.

(i.) Hva slags problem er dette? (ii.) Hvilken utregning er riktig? (iii.) Hvor mange valgmuligheter har Olav?

Løsning:

(i.) Dette er et problem med tilbakelegging da samme smak kan velges mer enn en gang. Utvalget er uordnet da rekkefølgen ikke har noe å si. (ii.) Riktig formel er $12C5 = \binom{12}{5}$. (iii.) Harald har 792 valgmuligheter.

NB. Det var noen trykkfeil i oppgave settet på denne oppgaven som vi ikke oppdaget i tide. Alle studenter som fikk riktig svar på del (iii.) og ikke svarte på (ii.) fikk full uttelling på (ii.)

13 **a)** Hvor mange forskjellige injektive funksjoner er det fra mengden $\{A, B, C, D\}$ til mengden $\{1, 2, 3, 4, 5\}$?

Løsning: En injektiv funksjon må ha forskjellige verdier. $f(A)$ kan ha 5 forskjellige valg av verdier, 1,2,3,4, eller 5. Deretter kan $f(B)$ ha kun 4 forskjellige verdier. Alle de gjennværende når vi har tatt bort $f(A)$. Det er 3 forskjellige valg for verdien til $f(C)$ når $f(A)$ og $f(B)$ er bestemt. Til slutt er det 2 valg for $f(D)$. Til sammen blir det $5 \cdot 4 \cdot 3 \cdot 2 = 120$ forskjellige injektive funksjoner er det fra mengden $\{A, B, C, D\}$ til mengden $\{1, 2, 3, 4, 5\}$.

b) Hvor mange forskjellige funksjoner er det fra mengden $\{A, B, C, D\}$ til mengden $\{0, 1, 2\}$?
Løsning: Det er 3 valg for hver av $f(A)$, $f(B)$ etc. Dvs det er $3^4 = 81$ forskjellig funksjoner fra mengden $\{A, B, C, D\}$ til mengden $\{0, 1, 2\}$.

c) Hvor mange forskjellige bijektive funksjoner er det fra mengden $\{A, B, C, D\}$ til mengden $\{0, 1, 2, 3\}$?
Løsning: Det er $4! = 24$ forskjellige bijektive funksjoner er det fra mengden $\{A, B, C, D\}$ til mengden $\{0, 1, 2, 3\}$.

d) Hvor mange forskjellige surjektive funksjoner er det fra mengden $\{1, 2, 3, 4, 5\}$ til mengden $\{A, B, C, D\}$?
Løsning. Siden det er 1 mer i den første mengden og funksjonen er surjektiv så må to elementer sendes til samme verdi. Det er $\binom{5}{2}$ forskjellige måter å velge disse to elementene. Vi har 4 valg for deres verdier. Vi har 3! mulige valg for valget verdien av de 3 øvrige elementene. Det gir til sammen $\binom{5}{2} \cdot 4 \cdot (3!) = 240$.

14 Gitt primtallene $p = 29$ og $q = 149$, og produktet $n = pq = 4321$.

a) Finn $\phi(4321)$ (ϕ er Eulers totientfunksjon)
Løsning: Vi regner ut $\phi(n) = \phi(pq) = (p-1)(q-1) = 28 \cdot 148 = 4144$.

b) Du vil bruke RSA med offentlig krypteringsnøkkel (n,e)=(4321,25).
Løsning: Du kan bruke dette som offentlig nøkkel fordi: 25 og $\phi(4321)$ er relativt primiske.

c) Krypter meldingen 42 med nøkkelen ovenfor.
Løsning: Vi lager en tabell

$$\begin{array}{rcrcrcrl} 42^2 & \equiv & 42^2 & = & 1764 & \equiv & 1764 & (\mathrm{mod}\, 4321) \\ 42^4 & \equiv & 1764^2 & = & 3111696 & \equiv & 576 & (\mathrm{mod}\, 4321) \\ 42^8 & \equiv & 576^2 & = & 331776 & \equiv & 3380 & (\mathrm{mod}\, 4321) \\ 42^{16} & \equiv & 3380^2 & = & 11424400 & \equiv & 3997 & (\mathrm{mod}\, 4321) \end{array}$$

Vi regner ut $42^{25} = 42^{16} \cdot (42^8 \cdot 42) \equiv 3997 \cdot (3380 \cdot 42) = 3997 \cdot 141960 = 14740936 \equiv 2005 \,(\mathrm{mod}\, 4321)$
Svar: 2005.

d) Finn den private dekrypteringsnøkkelen (n,d) tilhørende den offentlige nøkkelen (n,e) ovenfor.
Løsning: Vi utfører Euklids utvidede algoritme for å finne invers til 25 modulo 4144.

$$\begin{aligned} 4144 : 25 &= 165, \text{ med rest: } 19 \\ 25 : 19 &= 1, \text{ med rest: } 6 \\ 19 : 6 &= 3, \text{ med rest: } 1 \\ 6 : 1 &= 6, \text{ med rest: } 0 \end{aligned}$$

Vi har derfor

$$\begin{aligned} 1 &= 19 - 3 \cdot 6 \\ 1 &= 19 - 3 \cdot (25 - 19) = -3 \cdot 25 + 4 \cdot 19 \\ 1 &= -3 \cdot 25 + 4 \cdot (4144 - 165 \cdot 25) = 4 \cdot 4144 - 663 \cdot 25 \end{aligned}$$

Derfor er -663 en multiplikativ invers til 25 modulo 4144. Vi legger til 4144 for å få en invers mellom 0 og 4144.

$$d = 4144 - = 3481.$$