Obligatoriske oppgave 2, MAT-1005

Eskil Bjørnbakk Heines

Oppgave 1.1)

La $(A, \prec)$ være en poset, og la X være en mengde.
Betrakte en funksjon $f: X \to A$. Definerer en relasjon $\sqsubseteq$ på X
på følgende måte: sitt $x, y \in X$ er $x \sqsubseteq y$ iff $f(x) \preceq f(y)$.

Vi skal vise at hvis f er injektiv, vil $(X, \sqsubseteq)$ være en poset.
Vi sier at A = "$f: X \to A$ er injektiv"
og B = "$(X, \sqsubseteq)$ er en poset"
Skal vise at $A \to B$, vil bruke motsigelsesbevis for å vise at
$\neg A \to B$ er usant som fører til at $A \to B$ er sant etter definisjon
av de Morgans law.

f er injektiv enten om $x = y \Rightarrow f(x) = f(y)$
eller $x \neq y \Rightarrow f(x) \neq f(y)$

Så ser vi på hvordan $(X, \sqsubseteq)$ er en poset:
$(X, \sqsubseteq)$
For at $(X, \sqsubseteq)$ skal være en poset, må $\sqsubseteq$ være
transitiv, refleksiv og anti-symmetrisk.

$x \sqsubseteq y$ og $y \sqsubseteq z$, altså $x \sqsubseteq z$ h.b.h
$f(x) \sqsubseteq f(y) \wedge f(y) \sqsubseteq f(z) \rightarrow f(x) \sqsubseteq f(z)$.
Da er $(X, \sqsubseteq)$ transitiv.

$x \sqsubseteq x$ h.b.h. $f(x) \preceq f(x)$
altså $(X, \sqsubseteq)$ er refleksiv.

$x \sqsubseteq y$ og $y \sqsubseteq x$ impliserer at $x = y$
h.b.h. $f(x) \preceq f(y) \wedge f(y) \preceq f(x) \rightarrow f(x) = f(y)$
altså er $(X, \sqsubseteq)$ anti-symmetrisk.

Vi antar at $(\forall x, y \in X)(x = y \Rightarrow f(x) \neq f(y))$, altså at f ikke er injektiv.
Da impliserer vi at $x = y \Rightarrow f(x) \neq f(y)$ som gjør at $(X, \sqsubseteq)$ ikke
er anti-symmetrisk og da ikke en poset.
Da er $\neg A \to B$ usann, og $A \to B$ er sann. f er injektiv som gjør
at $(X, \sqsubseteq)$ er en poset

∎

Oppgave 2.1)

Skal vise ved matematisk induksjon at $3^n > n^3$ for alle $n \in \mathbb{N}$ hvor $n \geq 4$.

$P(n) = 3^n > n^3$

Basis steg: $P(4) = 3^4 = 81 > 4^3 = 64$

Vi ser at $P(4)$ er sann

Induksjons steg: Vi vet fra basis steg at $P(n)$, $n \geq 4$ er sann

Skal vise at $P(n+1)$ også er sann

Velger et vilkårlig tall $k \in \mathbb{N}$ for n

Antar at hvis $3^n > n^3$ vil $3^n - n^3 > 0$

og at hvis $P(k)$ er sann er også $P(k+1)$ sann

$$3^{(k+1)} - (k+1)^3 > 0$$

$$3 \cdot (3^k + k^3 - k^3) - (k+1)^3 > 0$$

$$3 \cdot (3^k - k^3) + 3k^3 - k^3 - 3k^2 - 3k - 1 > 0$$

$$3 \cdot (3^k - k^3) + (2k^3 - 3k^2 - 3k - 1) > 0$$

Fra antagelsen ser vi at $(3^k - k^3) > 0$

Viser at $(2k^3 - 3k^2 - 3k - 1) > 0$ hvor $k \geq 4$ ved

å faktorisere uttrykket til $k(k(2k-3)-3) - 1 > 0$

Siden $2k - 3 > 0$, $k \geq 4$, vil hele uttrykket

være større enn 0.

Der kan vi konkludere med at $3^{k+1} > (k+1)^3$ er sann $\boxed{//}$

Oppgave 2.2)

Skal bevise at $F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$ for alle $n \geq 1$

Vi vet at: $F_0 = 0$ og $F_1 = 1$

For alle $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$

$P(n) = F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$

Basis steg:

$$P(1) = F_{1+1} \cdot F_{1-1} - F_1^2 = (-1)^1$$

$$= F_2 \cdot 0 - 1 = -1$$

$$= 0 - 1 = -1$$

$P(1)$ er sann

Induksjons steg: Det finnes heltall $k = n$, $k \in \mathbb{Z}$

$$F_{k+1} \cdot F_{k-1} - F_k^2 = (-1)^k$$

$$F_{k-1} \cdot (F_{k+2} - F_k) - (F_{k+2} - F_{k+1})^2 = (-1)^k$$

$$F_{k-1} \cdot F_{k+2} - F_{k-1} \cdot F_k - F_{k+2}^2 + 2 \cdot F_{k+2} \cdot F_{k+1} + F_{k+1}^2 = (-1)^k$$

$$(F_{k+1} - F_k)\cdot F_{k+2} - F_k\cdot(F_{k+1} - F_k) - (F_{k+1} + F_k)^2 + 2\cdot F_{k+2}\cdot F_{k+1} + F_{k+1}^2 = (-1)^k$$

$$F_{k+1}\cdot F_{k+2} - F_k\cdot F_{k+2} - F_k\cdot F_{k+1} + \cancel{F_k^2} - F_{k+1}^2 - 2\cdot F_{k+1}\cdot F_k - \cancel{F_k^2} + 2\cdot F_{k+2}\cdot F_{k+1} - F_{k+1}^2 = (-1)^k$$

$$3F_{k+2}\cdot F_{k+1} - 3F_k\cdot F_{k+1} - F_k\cdot F_{k+2} - 2F_{k+1}^2 = (-1)^k$$

$$3(F_{k+1} + F_k)F_{k+1} - 3F_k\cdot F_{k+1} - F_k\cdot F_{k+2} - 2F_{k+1}^2 = (-1)^k$$

$$3F_{k+1}^2 + \cancel{3F_k F_{k+1}} - \cancel{3F_k F_{k+1}} - F_k F_{k+2} - 2F_{k+1}^2 = (-1)^k$$

$$-F_k\cdot F_{k+2} + F_{k+1}^2 = (-1)^k \quad | \cdot (-1)$$

$$F_k\cdot F_{k+2} + F_{k+1}^2 = (-1)^k$$

altså $P(k+1)$ er sann. $\square$

Oppgave 3)

Vi har fått en melding å dekryptere med hjelp av RSA-kryptering.
Vi har fått tildelt $n = 2537$ og $d = 311$.
1605 og 0790 er tallene vi skal dekryptere til bokstaver
hvor $00 = a$, $01 = b$, $02 = c$, ..., $25 = z$.
Vi løser dekrypteringen ved hjelp av formelen: $c^d \% n = m$
hvor m = dekryptert melding og c = kryptert melding.
Vi regner ut:

$$\begin{aligned}
m &\equiv 1605^{311} && \mod 2537 \\
&\equiv 1605^{256+32+16+4+2+1} && \mod 2537 \\
&\equiv (1605)^{256}(1605)^{32}(1605)^{16}(1605)^{4}(1605)^{2}(1605)^{1} && \mod 2537 \\
&\equiv (1605)^2 = 2576025 \equiv 970 && \mod 2537 \\
&\equiv (1605)^4 = (1605^2)^2 = (970)^2 = 940900 \equiv 2210 && \mod 2537 \\
&\equiv (1605)^8 = (1605^4)^2 = (2210)^2 = 4884100 \equiv 375 && \mod 2537 \\
&\equiv (1605)^{16} = (1605^8)^2 = (375)^2 = 140625 \equiv 1090 && \mod 2537 \\
&\equiv (1605)^{32} = (1605^{16})^2 = (1090)^2 = 1188100 \equiv 784 && \mod 2537 \\
&\equiv (1605)^{64} = (1605^{32})^2 = (784)^2 = 614656 \equiv 702 && \mod 2537 \\
&\equiv (1605)^{128} = (1605^{64})^2 = (702)^2 = 492804 \equiv 626 && \mod 2537 \\
&\equiv (1605)^{256} = (1605^{128})^2 = (626)^2 = 391876 \equiv 1178 && \mod 2537
\end{aligned}$$

$$\begin{aligned}
M &\equiv (1605)^{256}(1605)^{32}(1605)^{16}(1605)^{4}(1605)^{2}(1605)^{1} && \mod 2537 \\
&\equiv (1178)(784)(1090)(2210)(970)(1605) && \mod 2537 \\
&\equiv 3463593339067680000 && \mod 2537 \\
&\equiv \underline{\underline{812}} && \mod 2537
\end{aligned}$$

1605 dekryptert blir 0812, som vi kan oversette til I M.

Så løser vi tallet 790:

$$
\begin{aligned}
m &\equiv 790^{311} && \mod 790\\
&\equiv (790)^{256}(790)^{32}(790)^{16}(790)^{4}(790)^{2}(790)^{1} && \mod 790\\
&\equiv (790)^2 = 624100 \equiv 2535 && \mod 790\\
&\equiv (790)^4 = (790^2)^2 = 2835^2 = 6426225 \equiv 4 && \mod 790\\
&\equiv (790)^8 = (790^4)^2 = 4^2 = 16 \equiv 16 && \mod 790\\
&\equiv (790)^{16} = (790^8)^2 = 16^2 = 256 \equiv 256 && \mod 790\\
&\equiv (790)^{32} = (790^{16})^2 = 256^2 = 65536 \equiv 2111 && \mod 790\\
&\equiv (790)^{64} = (790^{32})^2 = 2111^2 = 4456321 \equiv 1349 && \mod 790\\
&\equiv (790)^{128} = (790^{64})^2 = 1349^2 = 1819801 \equiv 772 && \mod 790\\
&\equiv (790)^{256} = (790^{128})^2 = 772 = 595984 \equiv 2326 && \mod 790
\end{aligned}
$$

$$
\begin{aligned}
m &\equiv (790)^{256}(790)^{32}(790)^{16}(790)^{4}(790)^{2}(790)^{1} && \mod 790\\
&\equiv (2326)(2111)(256)(4)(2535)(790) && \mod 790\\
&\equiv 1006938520872960 0 && \mod 790\\
&\equiv \underline{\underline{11}} && \mod 790
\end{aligned}
$$

790 dekryptert blir 0011, altså AL.

Vi dekrypterte resten av meldingen ved hjelp av en RSA-kalkulator og fikk meldingen:

IMALITTLETEAPOTX

Oppgave 4.1)

Skal løse kongruensen

$$
\begin{aligned}
63x &\equiv 12 \mod 13\\
(13\cdot 4+11)x &\equiv 12 \mod 13\\
11x &\equiv 12 \mod 13
\end{aligned}
$$

Regner ut som invers kongruens. Med kongruens skrevet som $ax \equiv b \mod m$, er det krav at $GCD(a,m)$ må være 1:

$GCD(13,11) = 1$

Euklids Alogoritm: $13 = 11\cdot 1 + 2$
$11 = 2\cdot 5 + 1$

Løser lineær kombinasjon:

$$
\begin{aligned}
1 &= 11 - 2\cdot 5\\
&= 11 - (13-11)\cdot 5\\
&= 6\cdot 11 - 5\cdot 13
\end{aligned}
$$

Siden vi jobber med mod 13, kan vi fjerne $13\cdot 5$ fra likningen og får da $\bar{a}$, altså inversen til a.

$1 = 6\cdot 11 - \cancel{5\cdot 13}$

$1 = 6\cdot 11 \Rightarrow \bar{a} = 6$

Vi setter så inn $\bar{a}$ i kongruensen for å finne løsninger til kongruensen:

$$
\begin{aligned}
6\cdot 11x &\equiv 6\cdot 12 \mod 13\\
x &\equiv 72 \mod 13
\end{aligned}
$$

Løsningene til kongruensen blir da:
$72, 59, 46, 32, 20, 7$

$x = 7$ er kongruensens minste løsning og
$x = 7 + 13k, k \in \mathbb{Z}$ er likning for alle løsninger

Oppgave 4.2)

For å løse systemet av kongruensene:

$x \equiv 11 \mod 4$
$x \equiv 5 \mod 7$
$x \equiv -2 \mod 9 \Leftrightarrow x \equiv 7 \mod 9$

Bruker vi kinesisk rest teorem:

$x \equiv 11 \mod 4 \qquad x \equiv 5 \mod 7 \qquad x \equiv -2 \mod 9$

$M_1 = 7 \cdot 9 = 63 \qquad M_2 = 4 \cdot 9 = 36 \qquad M_3 = 4 \cdot 7 = 28$

$M_n \cdot y_n \equiv a_n \mod m_n \rightarrow y_n = ?$

$63 \cdot y_1 \equiv 1 \mod 4 \qquad 36 \cdot y_2 \equiv 1 \mod 7 \qquad 28 y_3 \equiv 1 \mod 9$
$3 \cdot y_1 \equiv 1 \mod 4 \qquad 1 y_2 \equiv 1 \mod 7 \qquad 1 y_3 \equiv 1 \mod 9$
$y_1 = 3 \qquad y_2 = 1 \qquad y_3 = 1$

$$A = M_1 \cdot y_1 \cdot a_1 + \dots + M_n \cdot y_n \cdot a_n = \sum_{k=1}^{n} M_k y_k a_k$$

$$A = 63 \cdot 3 \cdot 11 + 36 \cdot 1 \cdot 5 + 28 \cdot 1 \cdot (-2)$$
$$= 2079 + 180 - 56$$
$$= 2203$$

Hvis x løser systemet er

$x \equiv 2203 \mod_{4 \cdot 7 \cdot 9} \rightarrow x \equiv 2203 \mod_{252}$
$x \equiv 252 \cdot 8 + 187 \mod_{252}$
$x \equiv 187 \mod_{252}$

Altså er 187 den minste mulige positive løsningen til systemet,
og $187 + 252k, k \in \mathbb{Z}$ er alle mulige løsninger.

$\blacksquare$

Oppgave 4.3)

Vi skal løse systemet av kongruensene:

$3x \equiv 114 \mod 60 \quad |:3 \qquad x \equiv 55 \mod 28$
$x \equiv 38 \mod 20 \qquad x \equiv 27 \mod 28$
$x \equiv 18 \mod 20$

Vi starter med å sjekke GCD til $m = 20$ og $n = 28$ i begge kongruensene:
$GCD(20, 28) = 4$

Løser vi kongruensene får vi:

$x \equiv 18 \mod 4$ og $x \equiv 27 \mod 4$
$\equiv 2 \mod 4$ $\equiv 3 \mod 4$

Altså er kongruensene i konflikt siden GCD(m,n) gir ulike svar i hver av kongruensene. Vi vet at vi ikke kan bruke kinesisk rest teorem siden GCD(m,n) $\neq 0$.
Siden det ikke finnes et heltall x som løser begge kongruensene, har ikke systemet noen løsning for $x \in \mathbb{Z}$.

$\blacksquare$

Oppgave 5.1)

Norske registreringsnummer har formen XYabcde, hvor X og Y er store latinske bokstaver A, B, C, ..., Z, altså 26 muligheter.
Og a,b,c,d og e er siffer 0,1,2,...,9, altså 10 muligheter.
Vi multipliserer antall muligheter for hvert tegn i registreringsnummeret:
XYabcde $\Rightarrow 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 67\,600\,000$
Altså har norske registreringsnummer 67 600 000 forskjellige mulige kombinasjoner.

$\blacksquare$

Oppgave 5.1)

Hva blir antall mulige registreringsnummer om Vegvesenet ikke tillater at 3 eller flere siffer er lik?
Vi deler sifferene opp i de mulige kombinasjonene, uten hensyn til orden og teller mulige ordnet kombinasjoner for hver kombinasjon:

abcde - 120
aabcd - 10
aabbc - 15
aaabc - 10
aaabb - 10
aaaab - 5
aaaaa - 1

Så regner vi alle mulighetene for hver kombinasjon:

abcde $= \frac{10!}{5!} = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 = 30\,240$
aabcd $= 10 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 50\,400$
aabbc $= 15 \cdot 10 \cdot 9 \cdot 8 = 10\,800$
aaabc $= 10 \cdot 10 \cdot 9 \cdot 8 = 7200$
aaabb $= 10 \cdot 10 \cdot 9 = 900$
aaaab $= 5 \cdot 10 \cdot 9 = 450$
aaaaa $= 10 \cdot 1 = 10$

Vi vet at kombinasjonene aaaaa, aaaab, aaabb og aaabc ikke tillates av vegvesenet og fjerner disse fra totalt mulige kombinasjoner av abcde $= 10^5 = 100\,000$

$100\,000 - (10 + 450 + 900 + 7200) = 91\,440$

Så legger vi til X og Y

$91\,440 \cdot 26 \cdot 26 = 61\,813\,440$

Altså vil det være 61 813 440 mulige registreringsskilt hvis 3 eller fler siffer ikke kan være lik.

$\blacksquare$