STRUKTURER OG ARGUMENTER - LØSNING PÅNOEN OPPGAVER

E. F. WOLD

1. Løsning på noen oppgaver

Oppgave 2.1. Vi antar at P er mengdebyggende. Det vil si at det fins en mengde A slik at

$$\forall x, x \in A \Leftrightarrow P(x).$$

La A' være en vilkårlig mengde slik at

$$\forall x, x \in A' \Leftrightarrow P(x).$$

Da får vi at

$$\forall x, x \in A \Leftrightarrow x \in A',$$

så $A = A'$.

Oppgave 2.2. Anta at A, B er to tomme mengder. Likhetsaksiomet sier at

$$(A = B) \Leftrightarrow (\forall x, x \in A \Leftrightarrow x \in B).$$

Fikser så en x. Da er både $x \in A$ og $x \in B$ usant, så $x \in A \Leftrightarrow x \in B$.

Oppgave 2.3. Anta at det fins en mengde av alle mengder M. Vi kan da, ved spesialisering, danne oss

$$A = \{B \in M : B \notin B\}.$$

Vi får da at $A \notin A \Leftrightarrow A \in A$ - en selvmotsigelse.

Oppgave 2.4. Ved prinsipp 1.4.7 har vi at

(i) $\neg(\forall x, Q(x)) \Leftrightarrow (\exists x, \neg Q(x))$
(ii) $\neg(\exists x, Q(x)) \Leftrightarrow (\forall x, \neg Q(x))$

Set nå $Q(x) = (x \in A \Rightarrow P(x))$. Dette er ekvivalent med

$$\neg(x \in A \wedge \neg P(x))$$

Da får vi ved (i) at

$$\neg(\forall x, x \in A \Rightarrow P(x)) \Leftrightarrow (\exists x, x \in A \wedge \neg P(x))$$

Ved definisjoner (1.24) og (1.25) på side 49 i Spill, har vi da at

$$\neg(\forall x \in A, P(x)) \Leftrightarrow (\exists x \in A, \neg P(x)).$$

Nå kan (6.2) utledes fra (6.1).

Oppgave 2.7 Vi presiserer hva $\{x\}$ er. Aksiom 2.1.4. sier at $\langle\langle y : y = x\rangle\rangle$ er mengdebyggende. Det vil si at det fins en mengde A slik at

$$\forall y, y \in A \Leftrightarrow y = x.$$

Mengden A betegnes ved $\{x\}$. Vi får da også at

$$\forall x, x \in \{y\} \Leftrightarrow x = y.$$

Gitt x og y får vi da at

$$x \in \{y\} \Leftrightarrow x = y \Leftrightarrow y = x \Leftrightarrow y \in \{x\}.$$

Vi har videre at

$$\{x\} = \{y\} \Leftrightarrow \forall z(z \in \{x\} \Leftrightarrow z \in \{y\})$$

Spesielt får vi

$$\{x\} = \{y\} \Rightarrow x \in \{x\} \Leftrightarrow x \in \{y\} \Leftrightarrow x = y.$$

Til slutt er det klart at

$$x = y \Rightarrow \{x\} = \{y\}.$$

Oppgave 2.23

Vi ønsker å vise at det fins en avbilding $h : I \to U$ sånn at $g(i) \in A_i$ for alle $i \in I$. La $f : C \to I$ være avbildingen $f((i, x)) = i$. Denne er surjektiv siden hver $A_i \neq \emptyset$. Da fins $g : I \to C$ slik at $f(g(i)) = i$. For hver $i \in I$ har vi at $g(i) = (j, x_j)$ der $x \in A_j$. Men $f((j, x)) = i$. Så vi kan sette $h(i) = x_i$.

Oppgave 2.39

(i) ($\Rightarrow$) La $a \in A$. Da har vi $b = f(a) \in B$, så $a \in f^*B$.
($\Leftarrow$) La $a \in A$. Da har vi $f(a) \in B$.

(ii) La $a \in A$. Da er $f(a) \in f_*A$. Da er $a \in f^*f_*A$.

(iii) Vi har at

$$f^*B = \{a \in A : f(a) \in B\}.$$

Så for hver $a \in f^*B$ har vi $f(a) \in B$. Så $f_*f^*B \subset B$.

(iv) Anta f injektiv. La $a \in f^*f_*A$. Da har vi $f(a) \in f_*A$; det vil si $f(a) = f(a')$ for $a' \in A$. Men da er $a = a'$.

Anta at $f(a) = f(a')$ for $a \neq a'$. Sett $A = \{a\}$. Da er $a' \in f^*f_*A$ så vi har ikke inklusjonen.

(v) Anta surjektiv. La $b \in B$. Da fins $a \in A$ med $f(a) = b$, altså $a \in f^*B$. Men da er $b \in f_*f^*B$.

Anta at ikke surjektiv. Da fins $b \in B$ med $f^*\{b\} = \emptyset$. Da er $f_*f^*\{b\} = \emptyset$.

Oppgave 4.1

(i) Anta at det fins en surjeksjon $f : A \to B$. Da fins en injeksjon $g : B \to A$. Da kan vi ikke ha $|B| > |A|$ ved dueslagsprinsippet. Anta at $|A| \geq |B|$. Da fins bijeksjoner $f_a : A \to S_n, f_b : B \to S_m$ med $n \geq m$. Definer $h : S_n \to S_m$ ved $h(k) = k$ for $k \leq m-1$ og $h(k) = m-1$ for $k \geq m-1$. Da er h surjektiv. Og da er $f_b^{-1} \circ h$ surjektiv.

(ii) Anta $A = \emptyset$. Dersom $B \neq \emptyset$ fins ingen avbildinger $B \to A$, og surjeksjoner er definert for avbildinger (men det fins en surjektiv funksjon, nemlig $\emptyset \subset B \times A$). Dersom $B = \emptyset$ er $\emptyset$ en surjektiv avbilding.

Oppgave 4.3

Anta at A har en øvre skranke n. Da er inklusjonen $A \to S_{n+1}$ en injeksjon, så da er A endelig. REFERANSE

Dersom A er endelig fins en bijeksjon $f : S_n \to A$. Dersom $n = 0$ er alle naturlige tall øvre skranker. Enhver ikke-tom endelig delmengde av S_n har et største element. Dette elementet er en øvre skranke.

(Bevis: Induksjon på n. For $n = 1$ fins det bare ett element, og dette er en øvre skranke. Anta så at det holder for S_n, og la $A \subset S_{n+1}$. Dersom $n \in A$ er n en øvre skranke. Ellers følger det fra induksjonsantagelse av A har en øvre skranke.)

Oppgave 4.6

Det holder å se på S_m og S_n. Induksjon på n. Dersom $n = 0$ har vi $m = 0$ og formelen holder. Anta så at formelen holder for n. Da er antall injeksjoner fra S_m inn i S_{n+1} antall injesjoner inn i S_n pluss antall injeksjoner inn i S_{n+1} der ett element er avbildet på n. Det første antallet er

$$\frac{n!}{(n-m)!},$$

og det andre antallet er

$$\frac{mn!}{(n-(m-1))!}$$

Vi har

$$\frac{mn!}{(n-(m-1))!} + \frac{n!}{(n-m)!} = \frac{mn!}{(n+1-m))!} + \frac{(n+1-m)n!}{(n+1-m)!} = \frac{(n+1)!}{(n+1-m)!}.$$

(ii) $|\sigma(A)| = |A|$.

Oppgave 5.4

(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

Oppgave 9

For en avbilding $A \to B$ så må vi anta at A er totalt ordnet.

Anta at $f : A \to B$ er strengt voksende. Da er f voksende. Anta så at La $a, a' \in A, a \neq a'$. Da kan vi anta at $a < a'$. Da har vi $f(a) < f(a')$, så f er injektiv.

Anta at f er voksende og injektiv. For $a < a'$ har vi da $f(a) \leq f(a')$. Men da har vi $f(a) < f(a')$.

Oppgave 5.10

(i) For alle x har vi at $x|x$. Anta at $x|y$ og $y|z$. Da er $y = ax$ og $z = by$. Da er $z = abx$ så $x|z$. Anta så at $x|y$ og $y|x$. Da har vi $y = ax$ og $x = by$. Vi får at $x = abx$, så $ab = 1$. Da må vi ha at $a = b = 1$, så $x = y$.

(ii) Et element $x \in \mathbb{N}^*$ er et infimum for A dersom vi for alle $a \in A$ har at $x|a$ og dersom vi for alle nedre skranker y for A har at $y|x$.

La så x være det største tallet slik at $x|a$ for alle $a \in A$. Da er x en nedre skranke. Dersom vi lar $P = \{p_1, ..., p_m\}$ være mengden av alle primtall slik at $p \in P \Rightarrow p|a, \forall a \in A$, har vi $x = p_1 \cdots p_m$. Dersom y er en nedre skranke for A må y være et produkt av en undermengde av disse primtallene, så $y|x$. Altså er x den største nedre skranken.

Hint til resten: multipliser hvert element med en minimum antall primtall for å finne et minste felles multiplum.

Oppgave 5.15

Vi lar $\triangle$ betegne relasjonen. Vi har $x \triangle x$ for alle $x \in A$. Anta at $x \triangle y$. Da har vi at $y \triangle x$ siden $\triangle$ er en ekvivalensrelasjon. Da har vi at $y = x$ siden $\triangle$ er en ordensrelasjon.

Oppgave 5.27

(i) Transitivitet. Anta at $(x_i) \preceq (y_i)$ og $(y_i) \preceq (z_i)$. Dersom vi har likhet mellom noen av elementene er det klart. Vi har $x_{i_0} < y_{i_0}$ og $x_i = y_i$ for alle $i < i_0$, og vi har har $y_{i'_0} < z_{i'_0}$ og $y_i = z_i$ for alle $i < i'_0$.

Dersom $i_0 = i'_0$ er transitiviteten klar.

En annen mulighet er at $i'_0 < i_0$. Da er $x_{i'_0} = y_{i'_0} < z_{i'_0}$. Da har vi at $i''_0 \leq i'_0$, og $x_i = z_i$ for alle $i < i'_0$.

En siste mulighet er at $i_0' > i_0$. Da er $z_{i_0} = y_{i_0} > x_{i_0}$, og $x_i = y_i = z_i$ for alle $i < i_0$.

(ii) La $(x_i), (y_i) \in \Pi_{i \in I} A_i$ være forskjellige. La i_0 være som over. Da er $x_{i_0} \neq y_{i_0}$, så vi har enten at $x_{i_0} < y_{i_0}$ eller at $y_{i_0} < x_{i_0}$.

(iii) Definer $x_k = (x_j)$ der $x_j = 0$ for $k = 0, ..., k$, og $x_j = 1$ for $j > k$. La A være mengden av alle slike x_k'er. Da har vi $x_{k+1} < x_k$ for alle k, så A kan ikke ha noe minste element. Altså er dette ingen velorden.

Oppgave 5.44

La $B \subset A$ være en ikke-tom delmengde. Dersom B består av ett element har vi et minste element. Ellers har vi $x, y \in B$ og vi kan anta at $x < y$. Da har vi $B \cap A_y \neq \emptyset$ og må derfor ha et minste element.

Oppgave 5.49

Anta at f er en bijeksjon. Dersom $(y, x), (y, x') \in F^T$ har vi at $x = x'$ siden f er injektiv. Dette viser at f^T er en funksjon. Siden f er surjektiv er domenet til f^T lik Y. For $(x, y) \in F$ har vi $f(x) = y$ og vi har at $f^T(y) = x$. Så $f^T(f(x)) = f^T(y) = x$, så f^T er en venstre invers til f. Tilsvarende viser man at f er en venstreinvers til f^T.

Anta at f^T er en avbilding. For alle $y \in Y$ fins da en unik $(y, x) \in F^T$, og da fins unik $(x, y) \in F$. Så f er injektiv og surjektiv.

Oppgave 6.8

(i) For alle elementer $n \in \bar{\mathbb{N}}$ setter vi $n + \infty = \infty + n = \infty$.

(ii) Det naturlige ville være å definere $n + \infty = \infty$ for alle $n \in \mathbb{N} \cup \infty$, $n - \infty = -\infty$ for alle $n \in \mathbb{N} \cup \{-\infty\}$, og $\infty - \infty = 0$. Men da har vi

$$(-\infty + \infty) + \infty \neq -\infty + (\infty + \infty)$$

Oppgave 6.11

Vi antar at $G \neq 0$. La k være det minste elementet i G med $G > 0$. Da er $G_k = \{kn : n \in \mathbb{Z}\}$ en undergruppe av G. Anta at det fins et element $g > 0$ som ikke er med i G_k. Da må vi ha $kn < g < k(n+1)$ for $n \geq 0$. Da har vi at $g' = g - kn$ tilfredsstiller $0 < g' < k$ som er en motsigelse. Så $G_k = G$.

Oppgave 6.17

(i) Hvis $x, y \geq 0$ har vi $x + y \geq 0$, slik at $x + y \in P$. Det følger at $P + P \subseteq P$. Forøvrig for $x \in P$ har vi $x + 0 = x \in P + P$ så $P \subseteq P + P$.

For $x, y \geq 0$ har vi $xy \geq 0$ så $P \times P \subseteq P$. Har også $P \subseteq P \times P$.

Anta $x \in P \cap -P$. Da har vi $x \geq 0$ og $x = -y$ for $y \geq 0$. Da er $x \leq 0$. Så $x = 0$.

(ii) Anta så at $P \subseteq A$ er en delmengde med de oppgitte egenskapene. For alle $x \in A$ har vi at $x-x = 0 \in P$, så $x \leq x$. Anta at $y-x \in P$ og $z-y \in P$. Da har vi at $y - x + (z - y) = z - x \in P$, så relasjonen er transitiv. Anta at $y - x \in P$ og $x - y \in P$. Vi har $x - y = -(y - x)$, så $x - y \in -P$. Så $x - y = 0$, og relasjonen er antisymmetrisk.

La så $x \geq y$ - det vil si $y-x \in P$ - og la $z \in A$. Da har vi $y+z-(x+z) \in P$ så relasjonen er kompatibel med addisjon. La $x, y \geq 0$ - det vil si $x, y \in P$. Da har vi $xy \geq 0$, så relasjonen er kompatibel med multiplikasjon.

Anta så at P er indusert av en orden $\geq$, og at $\geq_2$ er ordenen indusert av P. Da har vi at $y \geq x \Leftrightarrow y - x \geq 0 \Leftrightarrow y - x \in P \Leftrightarrow y \geq_2 x$. Så $\geq = \geq_2$.

Anta at relasjonen er total. For alle x har vi da $x \geq 0$ eller $x \leq 0$. Det vil si $x \in P$ eller $x \in -P$. Omvendt, hvis $A = P \cup -P$ har vi for alle x at $x \in P$ eller $x \in -P$, så $x \geq 0$ eller $x \leq 0$.

Oppgave 6.19

Anta at $\leq$ er en total orden på $\mathbb{C}$ som er kompatibel med ringstrukturen. Anta først at $i > 0$. Da får vi $-1 = i^2 > 0$, og så $i \cdot (-1) = -i > 0$. Da har vi $0 = i - i > 0$ som er en motsigelse.

Liknende argument dersom $i < 0$.

Oppgave 6.20

Vi definerer $S : \mathbb{Z} \to \mathbb{Z}$ ved $S(n) = n + 1$, og restrikterer S til $\mathbb{N}$. For $n \geq 0$ har vi da $S(n) = n + 1 \geq 0$ så $S(\mathbb{N}) \subset \mathbb{N}$.

(i) Vi har $S(n) = 0 \Leftrightarrow n + 1 = 0 \Leftrightarrow n = -1$, så $n \notin \mathbb{N}$. Så $0 \notin S(\mathbb{N})$.

(ii) Vi har $S(n) = S(m) \leftrightarrow n + 1 = m + 1 \Leftrightarrow n = m$, så S er injektiv.

(iii) Per antagelse.

Oppgave 6.23

Anta at I tilfredsstiller Definisjon 6.5.2. For $x \in I$ har vi da at $-x = -1 \cdot x \in I$, så I er en additiv undergruppe.

Motsatt, dersom I er en additiv undergruppe har automatisk punkt en og to i definisjonen.

2. Tallteori

Oppgave 1.4

a) Vi har at $(7, 4) = 1$ så dette lar seg løse. Vi ser at en løsning er $x = -1, y = 2$. Da er alle løsningene $x_k = x + k4, y_k = y - k7$, $k \in \mathbb{Z}$.

b) Vi har at $(9, 15) = 3$. Vi har ikke at $3|4$, så det er ingen løsning.

c) Vi ser at en løsning er $x = 0$ og $y = -6$. Da er alle løsninger på formen $x_k = k, y_k = -6 - k4, k \in \mathbb{Z}$.

Oppgave 1.5 Vi har $455 = 5 \cdot 7 \cdot 13$ og $2772 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 \cdot 11$. Vi har da at $(455, 2772)|21$. Vi bruker Euklid.

$$2772 = 6 \cdot 455 + 42$$
$$455 = 10 \cdot 42 + 35$$
$$42 = 1 \cdot 35 + 7$$
$$35 = 5 \cdot 7.$$

Vi har

$$7 = 42 - 35 = 42 - (455 - 10 \cdot 42) = 11 \cdot 42 - 455$$

så

$$7 = 11(2772 - 6 \cdot 455) - 455 = 11 \cdot 2772 - 67 \cdot 455.$$

Oppgave 1.8.

a) Det er klart at $I(a, b)$ inneholder et element som ikke er null, så vi har (i). Vi har $s_1a + t_1b + s_2a + t_2b = (s_1 + s_2)a + (t_1 + t_2)b$ så vi har (ii). Vi har $n(sa + tb) = (ns)a + (nt)b$ så vi har (iii).

b) Fra (i) og (iii) får vi at $0 \cdot a = 0 \in I$. Dersom $a > 0$ får vi fra (ii) at $-a \in I$, og omvendt hvis $a < 0$.

c) Det følger fra (iii) at $nd \in \mathbb{I}$ for alle $n \in \mathbb{Z}$. La så $k \in I$. Da kan vi skrive $k = nd + r$ med $0 \leq r < d$. Det følger fra (ii) at $k - nd = r \in I$. Da må $r = 0$ siden d er det minste positive tallet i I.

(d) Mengden av alle tall som kan skrives som en sum $\sum_{j=1}^{k} s_i m_i$ er et ideal I. La d været tallet fra (c). Spesielt er da hver m_i et multiplum av d, så d er en felles divisor. Men siden

$$d = \sum_{j=1}^{k} s_i m_i$$

vil enhver felles divisor også dele d. Så d er største felles divisor.

Hvis et tall a nå er delelig med d har vi $a \in I$. Hvis $a \in I$ så er a et multiplum av d.

Oppgave 1.9

Et hvert tall $a \in \mathbb{Z}_+$ kan skrives på formen $2^k y$ der y er et oddetall. Så vi har elementer på formen $a_j = 2^{k_j} y_j$, der y_j er et oddetall mellom 1 og $2n$ for $j = 1, ..., n + 1$. Det er bare n oddetall mellom 1 og $2n$, så samme oddetall må forekomme minst to ganger, for eksempel $y_1 = y_2$. Men vi har $k_1 \leq k_2$ eller omvendt, så a_1 må dele a_2 eller omvendt.

Oppgave 2.1

a)

Det er klart at $d = p_1^{\mu_1} \cdots p_n^{\mu_n}$ deler både a og b. Videre, hver p_j enten deler ikke a/d eller deler ikke b/d, så a/d og b/d har ingen felles faktorer.

b)

La $ak = bl = [a, b]$. Vi har

$$p_1^{\alpha_1} \cdots p_n^{\alpha_n} q_1^{\gamma_1} \cdots q_m^{\gamma_m} = p_1^{\beta_1} \cdots p_n^{\beta_n} q_1^{\delta_1} \cdots q_m^{\delta_m}$$

Hvis det forekommer primtall som ikke var i den opprinnelige mengden $\{p_j\}$ kan vi kansellere dem, for de må forekommer på hver side. Hvis vi da misbruker notasjon kan vi skrive

$$p_1^{\alpha_1+\gamma_1} \cdots p_n^{\alpha_n+\gamma_n} = p_1^{\beta_1+\delta_1} \cdots p_n^{\beta_n+\delta_n}$$

Da har vi $\alpha_j + \gamma_j = \beta_j + \delta_j$ for alle j. Da har vi enten $\gamma_j = 0$ eller $\delta_j = 0$, ellers kan vi kansellere. Dermed blir λ_j den største av de to potensene.

Oppgave 2.3

Klart for $n = 1$. Se nå på $p_1 \cdots p_n \cdot p_{n+1}$. Vi vet at p deler enten p_{n+1} eller $p_1 \cdots p_n \cdot p_n$. I det første tilfellet er vi fremme. I det andre tilfelle bruker vi induksjonshypotesen.

Oppgave 2.4

Dersom $(p/q)^2 = n$ og vi primtallsfaktoriserer p og q til det ikke fins felles faktorer, ser vi at $q = 1$.

Oppgave 2.5

a)

Dersom $2^{p/q} = 5$ har vi $2^p = 5^q$. Det ville vært to forskjellige primtallsfaktoriseringer av det samme tallet.

b) Dersom $a^{p/q} = b$ har vi $a^p = b^q$. Umulig av samme grunn som før.

Oppgave 3.2

Vi vil da løse

$$27x + 31y = 5.$$

Vi ser at $(27, 31) = 1$ så vi starter med å løse

$$27x + 31y = 1.$$

Vi bruker Euklid.

$$\begin{aligned} 31 &= 1 \cdot 27 + 4 \\ 27 &= 6 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

Vi får

$$1 = 4 - 3 = 4 - (27 - 6 \cdot 4) = -27 + 7 \cdot (31 - 27) = 7 \cdot 31 - 8 \cdot 27$$

så en løsning er $\overline{-8}$ som er $\overline{23}$ (mod(31)). Så løsningen til den opprinnelige ligningen er $\overline{115} = \overline{22}$.

Oppgave 3.4

Vi vil løse

$$770x + 1173y = 7$$

Vi bruker Euklid for å finne $(1173, 770)$

$$\begin{aligned}
1173 &= 770 + 403 \\
770 &= 403 + 367 \\
403 &= 367 + 36 \\
367 &= 10 \cdot 36 + 7 \\
36 &= 5 \cdot 7 + 1
\end{aligned}$$

Videre har vi

$$\begin{aligned}
1 &= 36 - 5 \cdot 7 = 36 - 5(367 - 10 \cdot 36) = 51 \cdot 36 - 5 \cdot 367 \\
&= 51(403 - 367) - 5 \cdot 367 = 51 \cdot 403 - 56 \cdot 367 \\
&= 51 \cdot 403 - 56(770 - 403) = 107 \cdot 403 - 56 \cdot 770 \\
&= 107(1173 - 770) - 56 \cdot 770 = 107 \cdot 1173 - 163 \cdot 770.
\end{aligned}$$

Så $x = -163, y = 107$ løser

$$770x + 1173y = 1,$$

så $x = -5 \cdot 163 = -358$ løser ligningen over. Vi har $-358 = 815$ (mod(1173)), så $\overline{815}$ løser den opprinnelige ligningen. Det fins ingen flere løsninger ettersom $(1173, 770) = 1$.

Oppgave 3.9

a)

Bruk Euklid til a finne ut at $7 \cdot 11 - 4 \cdot 19 = 1$. Altså er $7 = 11^{-1}$ i $\mathbb{Z}_{19}$.

b) Ganger vi den første ligningen med $\overline{2}$ og legger den til den andre får vi ligningen $\overline{11}\overline{x} = \overline{8}$. Vi får da at $\overline{x} = \overline{7 \cdot 8} = \overline{18} = \overline{-1}$. Fra den første ligningen får vi da $y = \overline{4}$.

Oppgave 3.14

Kan ikke løse $3x + 2 = y^2$ med heltall heller. I så fall ville vi ha $\overline{y}^2 = \overline{2}$ i $\mathbb{Z}_3$. Det er ikke mulig siden $\overline{1}^2 = \overline{1}, \overline{2}^2 = \overline{1}$.

Hvis man vil ta det fra scratch, anta at det fins en løsning. Da kan vi skrive $y = k \cdot 3 + r, 0 \leq r < 3$. Da har vi

$$y^2 - 2 = 9k^2 + 6k + r^2 - 2.$$

Men da er $r^2 - 2 \in \{-2, -1, 2\}$ og ingen av disse tallene er delelige med 3.

Oppgave 4.1

a) Bruker vi Fermat har vi mod(5) at

$$n^8 + 2n^6 + 2n^2 + 4 = n^4 + 2n^2 + 3n^2 + 4 = 5 + 5n^2.$$

b) Vi viser at

$$\frac{3n^5 + 5n^3 + 7n}{5 \cdot 3}$$

er et helt tall. Vi har $5n^3 + 7n = 5n + 7n = 12n \pmod{3}$ og vi har $3n^5 + 7n = 3n + 7n = 10n \pmod{5}$, så det er klart.

c) Vi har at $5n^7 + 2n = 7n \pmod{7}$ så det er delelig med 7. Vi har $-7n^5 + 2n = -5n \pmod{5}$ så uttrykket er delelig med 5.

d) Vi har $42 = 7 \cdot 3 \cdot 2$. Regner vi mod(7) har vi $n^7 - n = n - n = 0$. Regner vi mod(3) har vi $n^7 - n = n^3 n^3 n - n = n - n = 0$. Regner vi mod(2) har vi

$$n^7 - n = n^2 n^2 n^2 n - n = n^4 - n = n^2 n^2 - n = n^2 - n = n - n = 0.$$

Oppgave 4.9

Vi har at $70! = -1 \pmod{71}$. Vi har

$$70! = 70 \cdot 69 \cdot 68 \cdot 67 \cdot 66 \cdot 65 \cdot 64 \cdot 63!$$

og vi får at

$$70! = (-1)^7 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 63! (\mathrm{mod}(71)).$$

Vi har $7 \cdot 5 \cdot 2 = 70 = -1 \pmod{71}$, så vi har

$$70! = 3 \cdot 4 \cdot 6 \cdot 63! (\mathrm{mod}(71)) = 63! (\mathrm{mod}(71)).$$

Det vil si at $63! = -1 \ (\mathrm{mod}(71))$. Til slutt bruk at $9 \cdot 8 = 72$.

References

E. F. Wold: Department of Mathematics, University of Oslo, PO-BOX 1053 Blindern, 0316 Oslo, Norway.