Direkte bevis.

MAT 1140

20. sept. 2016

4.3

Hvis a er odde, så er

$$n = a^2 + 3a + 5$$

odde.

Hva vet vi? En proposisjon i teksten sier at a^2 er odde når a er odde. (a)

~~Vi bruker~~

Mtp. å bruke at summen av to tall med motsatt paritet er odde skriver vi om: (b)

$$n = (a^2 + 2a) + (a + 4) + 1$$

(a) og (b)
$$= (2b+1) + (2c+1) + 1$$
$$= 2(b+c+1) + 1.$$

Ved definisjonen er da n odde.

4.4

Hvis x og y er odde, så er xy odde.
Vi vet da at $x = 2a+1$ og $y = 2b+1$.
Produktet blir

$$xy = (2a+1)(2b+1) = 4ab + 2a + 2b + 1$$
$$= 2(2ab + a + b) + 1$$

som er odde.

4.6

Vis at $a \mid (b+c)$ hvis $a \mid b$ og $a \mid c$.

Vi ønsker å ende opp med et uttrykk

$$b + c = ap, \quad p \in \mathbb{Z}.$$

Hypotesen er ~~det som~~ nettopp eksistensen av to likninger

$$b = am, \quad m \in \mathbb{Z}$$
$$c = an, \quad n \in \mathbb{Z}.$$

Summen av b og c kan da skrives

$$b + c = am + an = a(m+n),$$

og $m+n \in \mathbb{Z}$. Dette viser at a deler $b+c$.

4.18

Anta at x og y er positive reelle tall. Hvis $x < y$ er $x^2 < y^2$.

Løsning.

Anta at

$$x < y$$

for positive reelle tall x, y. Fordi y er positivt er

$$xy < y^2.$$

Hvis vi igjen tar utgangspunkt i den oppgitte ulikheten og bruker at x er positivt får vi

$$x^2 < xy.$$

Kombinert gir de to ulikhetene at

$$x^2 < y^2.$$

4.24

Hvis $n \in \mathbb{N}$ og $n \geq 2$, så er

$$n!+2,\ n!+3,\ n!+4, \ldots, n!+n$$

alle "komposittet".

Vi ønsker å vise at hvert av tallene kan skrives som et produkt

$$n!+j = ab, \quad a,b \in \mathbb{Z},$$

der $a, b > 1$. Her er $j \in \mathbb{N}$ med $2 \leq j \leq n$ som i hypotesen.

Definisjonen av fakultetet gir ~~at vi kan skrive~~

$$n!+j = n(n-1)\ldots 2\cdot 1 + j$$
$$= j\left(n(n-1)\ldots \hat{j} \ldots 2\cdot 1 + 1\right).$$

Vel, vi antok at $j \geq 2$ og faktoren

$$n(n-1)\ldots \hat{j} \ldots 2\cdot 1+1$$

er større enn 1. Dermed er $n!+j$ kompositt. På grunn av at vi lot $j \in \mathbb{N}$ variere med $2 \leq j \leq n$ følger det umiddelbart at alle de oppgitte tallene er "komposittet".

5.4

Anta at $a, b, c \in \mathbb{Z}$. Hvis a ikke deler bc, så deler ~~ikke a b~~ a ikke b.

Løsning

Anta at a deler b. Dette betyr at

$$b = ak, \quad k \in \mathbb{Z}.$$

Vi ønsker å vise at a deler bc, dvs. at

$$bc = am,$$

for en $m \in \mathbb{Z}$. Likningen vi fikk fra multiplisering med c, slik at vi får

$$bc = a(ck).$$

Dette viser at a deler bc.

Hvordan gjør man et direkte bevis?

Anta at a ikke deler bc. Vi ønsker å vise at a ikke deler b.

At a ikke deler bc er det samme som at

$$bc \neq am$$

for alle $m \in \mathbb{Z}$, inkludert $m = 0$.

Med andre ord er

$$b \nmid 0 \nmid c.$$

Vi ønsker å vise at

$$b \neq an$$

for alle $n \in \mathbb{Z}$. Ta derfor en vilkårlig $n \in \mathbb{Z}$. Hypotesen gir at

$$bc \neq (acn)$$

$$\Leftrightarrow \quad b \neq an.$$

På grunn av at $n \in \mathbb{Z}$ var vilkårlig viser dette at a ikke deler b.

5.9

Anta at $n \in \mathbb{Z}$. Hvis $3 \nmid n^2$, så $3 \nmid n$.

Husk at oppg. 5.4 var

$$a \nmid bc \Rightarrow a \nmid b.$$

Vi kan sette $a = 3$, $b = n = c$.

5.15

Anta at $x \in \mathbb{Z}$. Hvis x^3-1 er like, så er x odde.

Kontrapositivt.

Anta at x ikke er odde, dvs. like.

Vi ønsker å vise at

$$x^3-1 = 2a+1$$

for en $a \in \mathbb{Z}$, dvs. at x^3-1 er odde, dvs. ikke like.

Vi har at $x = 2k$ for en $k \in \mathbb{Z}$.

Dermed er

$$x^3-1 = (2k)^3-1 = 2\cdot 4k^3-1$$

$$= 2\cdot 4k^3 - 2 + 1 = 2(4k^3-1)+1$$

som viser at x^3-1 er odde.

5.24

Hvis $a \equiv b \pmod{4}$ og $c \equiv d \pmod{4}$, så er $ac \equiv bd \pmod{4}$.

Direkte bevis.

Anta at

$$4 \mid a-b$$

og at

$$4 \mid d-c.$$

Vi ønsker å vise at

$$4 \mid bd-ac.$$

Ved definisjonene er

$$a-b = 4 \cdot m_1, \quad m_1 \in \mathbb{Z} \qquad (1)$$

$$d-c = 4 \cdot m_2, \quad m_2 \in \mathbb{Z}. \qquad (2)$$

Omformulert ønsker vi ~~[illegible]~~ å vise at

$$bd-ac = 4 \cdot m_3, \quad m_3 \in \mathbb{Z}$$

Vi multipliserer likning (1) med c og likning (2) med b og får ...

$$ac = bc + n \cdot m_1 c \qquad (1')$$

$$bd = bc + n \cdot m_2 b \qquad (2')$$

Nå kan vi $(2') - (1')$ og får

$$bd - ac = n \cdot m_2 b - n \cdot m_1 c$$

$$= n(m_2 b - m_1 c),$$

som viser at $n \mid (bd - ac)$. Da har

$$ac \equiv bd \pmod{n}.$$

Kapittel 6 - lærebok

6.7. Hvis $a, b \in \mathbb{Z}$ er $a^2 - 4b - 3 \neq 0$.

Anta for motsigelse at

$$a^2 - 4b - 3 = 0$$

for $a, b \in \mathbb{Z}$. Da er

$$\begin{aligned} a^2 &= 4b + 2 + 1 \\ &= 2(2b+1) + 1, \end{aligned}$$

så a^2 er odde. Da er a odde også, så

$$a = 2c + 1$$

for en $c \in \mathbb{Z}$. Dermed er

$$(2c+1)^2 - 4b - 3 = 0$$

$$\Rightarrow \quad 4c^2 + 4c + 1 - 4b - 3 = 0$$

$$\Rightarrow \quad 4(c^2 + c - b) = 2$$

$$\Rightarrow \quad 2(c^2 + c - b) = 1$$

$\Rightarrow$ 1 er et partall.

Dette er en motsigelse.
Den eneste antakelsen vi ikke hadde dekning for var at det er $a, b \in \mathbb{Z}$ s.a. $a^2 - 4b - 3 = 0$.

6.19

Induksjon

Ytre induksjon

Anta at $(n-1)!$ deler ethvert produkt av $n-1$ påfølgende heltall.
Se på tilfellet med n påfølgende heltall, dvs. se på

$$P(k) = (k+1)\cdots(k+n).$$

De ikke-trivielle tilfellene er
$k+n < 0$ og $k+1 \geq 1 \iff k \geq 0$.
~~Anta k~~
Se på $k \geq 0$.

Indre induksjon.

Induksjon på k (indre hypotese):
Anta at $n!$ deler $P(k)$ og se på $P(k+1)$.

Siden

$$P(k+1) = (k+2)\cdots(k+n+1)$$

$$= \underbrace{[(k+2)\cdots(k+n)](k+1)}_{P(k)} + \underbrace{[(k+2)\cdots(k+n)]}_{} n$$

$P(k)$ indre hypotese

$n-1$ påfølgende heltall, delelig med $n-1$

ytre hypotese

6.20

Vis at kurven

$$x^2+y^2-3=0 \qquad (1)$$

ikke har rasjonale punkter.

Løsning

Anta for motsigelse at det er rasjonale $x=\frac{a_x}{b_x}$, ~~gcd(a_x, b_x~~ og $y=\frac{a_y}{b_y}$ som oppfyller likningen (1). Vi kan utelukke mulighetene $x=0$ og $y=0$, for ved oppg. 6.5 er $\sqrt{3}$ irrasjonal. Vi kan anta at

$$\gcd(a_x, b_x)=1$$

og

$$\gcd(a_y, b_y)=1$$

~~fordi~~ $x \neq 0 \neq y$.

Nå kan (1) skrives

~~Her er~~

$$a_x^2 b_y^2 + a_y^2 b_x^2 = 3 b_x^2 b_y^2.$$

La $c = a_x b_y$, $d = a_y b_x$, $p = b_x b_y$.
Da er 1 største felles divisor/faktor til c, d og p, for

$$\gcd(d, p) = b_x$$

og en ~~divisor~~ faktor av b_x må dele a_x hvis den skal dele c, noe den ikke gjør, for faktoren b_y i $c = a_x b_y$ er "brukt opp".

Nå står vi igjen med likningen

$$c^2 + d^2 = 3p^2 \qquad (2)$$

der største felles faktor/divisor til c, d og p er 1.

Vi argumenterer nå for at 3 deler c og d.

Til å vise det skal vi bruke at 3 deler c^2+d^2.
Bruk "Divisjonsalgoritmen" til å skrive

$$c^2 = q_c \cdot 3 + r_c, \quad 0 \le r_c < 3$$
$$d^2 = q_d \cdot 3 + r_d, \quad 0 \le r_d < 3.$$

Summerer vi likningene får vi

$$c^2+d^2 = (q_c+q_d)\cdot 3 + (r_c+r_d),$$

der $r_c + r_d$ må være delelig med 3. Mulighetene er da

$$(r_c, r_d) \in \{(1,2),(2,1),(0,0)\}.$$

<u>Lemma</u>

Ingen kvadrattall har rest 2 (mod 3).

<u>Bevis</u>

Anta at $n \in \mathbb{Z}$. Vi har at n er delelig med 3 hvis og bare hvis n^2 er det.

Vi har

$$m = Q_1 \cdot 3 + r_1 \,,\; 0 \le r_1 < 3 \,,$$
$$m^2 = Q_2 \cdot 3 + r_2 \,,\; 0 \le r_2 < 3 .$$

Videre er

$$m^2 = (Q_1 \cdot 3 + r_1)^2$$
$$= Q_1^2 \cdot 3^2 + 2Q_1 \cdot 3 + r_1^2$$
$$= (3Q_1^2 + 2Q_1) \cdot 3 + r_1^2 .$$

Vi har at $r_1 = 0$, $r_1 = 1$ eller $r_1 = 2$.

~~Dermed er~~

$$\begin{array}{ccc} \Downarrow & \Downarrow & \Downarrow \\ r_1^2 = 0 & r_1^2 = 1 & r_1^2 = 4 \\ \Downarrow & \Downarrow & \Downarrow \\ r_2 = 0 & r_2 = 1 & r_2 = 1 . \end{array}$$

$\boxtimes$

Det følger at

$$(r_c, r_d) \in \{(0,0), (0,1), (1,0), (1,1)\} .$$

Dermed er

$$(r_c, r_d) = (0,0) .$$

Mer om relasjoner.

Seksjon 1

2. En ordning på $X = \{1,2,3,4,5\}$ er gitt ved

$$\leq \; = \{\cancel{(1,1)}, (1,2), (1,3), (1,4), (1,5), \cancel{(2,2)}, (2,4), \cancel{(3,3)}, (3,4), \cancel{(4,4)}, \cancel{(5,5)}\}.$$

Tegn et Hasse-diagram.

Vi ser at $(1,4)$ må være i $\leq$ pga. at $(1,3), (3,4) \in \leq$. Dermed er

$$\begin{tikzcd}
3 \arrow[rr] & & 4 \\
& 5 & \\
1 \arrow[uu] \arrow[ur] \arrow[rr] & & 2 \arrow[uu]
\end{tikzcd}$$

et ok Hasse-diagram.

Seksjon 1. — Mer om relasjoner

4. La X være mengden av funksjoner

$$f : \{1,2,3\} \to \{1,2\}$$

og definer en relasjon på X ved

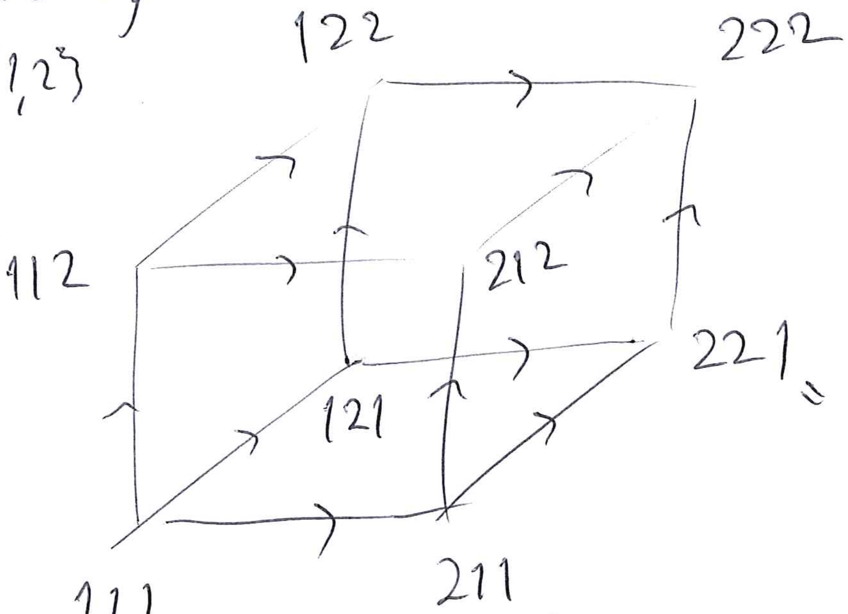
$$f \le g \iff f(i) \le g(i)$$

for alle $i \in \{1,2,3\}$. Tegn et Hasse-diagram.

Løsning:

$\{1,2,3\} \to \{1,2\}$
$1 \mapsto 2$
$2 \mapsto 2$
$3 \mapsto 2$
$\shortparallel$

$\{1,2,3\} \to \{1,2\}$
$1 \mapsto 1$
$2 \mapsto 1$
$3 \mapsto 2$
$\shortparallel$



$\shortparallel$
$\{1,2,3\} \to \{1,2\}$
$1 \mapsto 2$
$2 \mapsto 2$
$3 \mapsto 1$

$\shortparallel$
$\{1,2,3\} \to \{1,2\}$
$1 \mapsto 1$
$2 \mapsto 1$
$3 \mapsto 1$

$\shortparallel$
$\{1,2,3\} \to \{1,2\}$
$1 \mapsto 2$
$2 \mapsto 1$
$3 \mapsto 1$

Mer om relasjoner – Seksjon 1

8. Anta at $\leq$ er en partiell ordning på en mengde X. Anta at A er en ikke-tom delmengde av X og la $\leq_A$ være relasjonen på A definert ved

$$x \leq_A y \iff x, y \in A \text{ og } x \leq y.$$

Vis at $\leq_A$ er en partiell ordning på A.

<u>Løsning</u>

~~Reffl~~

(i) Refleksivitet: Anta at ~~x∈A~~ $x \in A$. Da er $x \in X$. Vi har $x \leq x$ fordi $\leq$ er refleksiv. Dermed er $x \leq_A x$.

(ii) ~~Antsy~~ Antisymmetri: Anta at $x, y \in A$ og at $x \leq_A y$ og $y \leq_A x$. Da er $x, y \in X$ og $x \leq y$ og $y \leq x$. Siden $\leq$ er antisymmetrisk, er $x = y$.

(iii) Transitivitet: Anta at $x, y, z \in A$ og at $x \leq_A y$ og $y \leq_A z$. Da er $x \leq y$ og $y \leq z$ i $(X, \leq)$. Siden $\leq$ er transitiv er $x \leq z$, så $x \leq_A z$.

Mer om relasjoner — Seksjon 2

2. Gjennomfør beviset for Setning 5 for minste/minimale elementer.

La $(X, \leq)$ være en partielt ordnet mengde. Vi ønsker å vise implikasjonen

$$a \text{ minste element} \Rightarrow a \text{ minimalt}$$

som er ekvivalent med den kontrapositive

$$a \text{ ikke minste} \Leftarrow a \text{ ikke minimalt.}$$

Anta at a ikke er minimalt. Da er det en $b \in X$ med $b < a$ i følge def. av "minimalt". I følge def. av "minste" er det umiddelbart at a ikke er et minste element.

Mer om relasjoner – Seksjon 2

3. (a) Finn en partiell ordning på en mengde som ikke har den minste øvre skranke-egenskapen.

La $(X, \leq) = \{c > a < b\}$.
Delmengden $\{a\} \subset X$ har både b og c som øvre skranker, men verken b eller c er en minste øvre skranke siden ~~$c < b$ og $b < c$~~ verken $b < c$ eller $c < b$.

(b) Vis at enhver totalt ordnet ~~mengde~~ endelig mengde har ~~minste~~ minste øvre skranke-egenskapen.

På grunn av at to elementer i en totalt ordnet mengde kan vi, for eksempel ved induksjon på antall elementer, vise at elementene kan skrives i en liste

$$x_1 < x_2 < \dots < x_n,$$ Dette er oppg. 9 fra Seksjon 1.

der $n = |X|$ er antallet elementer i den totalt ordnede mengden $(X, \leq)$.

Dermed kan vi veldefinerte funksjoner

min, max : $P(X) - \{\emptyset\} \to X$

som plukker ut henholdsvis det minste og det største elementet til den ikke-tomme delmengden av X.

La $(X, \leq)$ være totalt ordnet, endelig. Anta at A er en oppad begrenset delmengde (~~Ent~~ med den induserte ordningen $\leq_A$). (Enhver delmengde er for øvrig oppad begrenset.)

Vi påstår at

$$b = \min B,$$

der B er mengden av øvre skranker til A, er en minste øvre skranke.

Vel, B er totalt ordnet og $\min B$ er veldefinert nettopp på grunn av at B er totalt ordnet og endelig. Vi har at ~~c > b~~ $b < c$ for alle $c \in B$ med $c \neq b$.

Mer om relasjoner – Sesjon 2

4. La X være en mengde. Vis at

$$(\mathcal{P}(X), \subseteq)$$

har ~~den~~ minste øvre skranke-egenskapen.

Den oppad begrensede delmengden $\{\emptyset\} \subseteq \mathcal{P}(X)$ har for eksempel $\emptyset$ som minste øvre skranke.

Anta at $A \subseteq \mathcal{P}(X)$ er ikke-tom og oppad begrenset. Forøvrig er alle delmengder av $\mathcal{P}(X)$ oppad begrenset av X selv.

La $B \subseteq \mathcal{P}(X)$ være mengden av øvre skranker til A. Legg merke til at

$$c = \bigcap_{b \in B} b$$

er et element i B: Anta at $b \in B$. Da er

$$a \leq b$$

for alle $a \in A$. Dermed er

$$\bigcup_{a \in A} a \subseteq b.$$

Elementet b var vilkårlig, så

$$\bigcup_{a \in A} a \subseteq \bigcap_{b \in B} b = c \Rightarrow c \in B$$

Mer om relasjoner — Seksjon 5

5. La X være en uendelig mengde og $\mathcal{F}(X)$ familien av endelige delmengder av X. Vis at inklusjonsordningen på $\mathcal{F}(X)$ ikke har maksimale elementer.

Vi ønsker å vise at ~~the~~ ingen elementer i $\mathcal{F}(X)$ er maksimale. Anta at $a \in \mathcal{F}(X)$. Velg en $x \in X - a$. Da er $b = a \cup \{x\} \in \mathcal{F}(X)$ og $a < b$, så a ~~er~~ ikke maksimalt og a var vilkårlig valgt.

Mer om relasjoner – Seksjon 2

8. $\mathcal{F}$ er mengden av funksjoner $f : \mathbb{R} \to \mathbb{R}$.
Vi definerer en relasjon $\preceq$ på $\mathcal{F}$
ved
$$f \preceq g \iff f(x) \leq g(x) \text{ for alle } x \in \mathbb{R}.$$

(a) Vis at $\preceq$ er en partiell ordning.

$\preceq$ Refl: $f \preceq f \Longleftarrow f(x) = f(x)$ for alle x

$\preceq$ antisymm.: $f \preceq g$ og $g \preceq f$

$$\Rightarrow f(x) \leq g(x) \text{ og } g(x) \leq f(x) \text{ for alle } x \in \mathbb{R}$$
$$\Rightarrow f(x) = g(x) \text{ for alle } x \in \mathbb{R}$$
$$\Rightarrow f = g.$$

$\preceq$ transitiv: $f \preceq g$ og $g \preceq h$

$$\Rightarrow f(x) \leq g(x) \text{ og } g(x) \leq h(x) \text{ for alle } x$$
$$\Rightarrow f(x) \leq h(x) \text{ for alle } x$$
$$\Rightarrow f \preceq h.$$

b) Vis at $\lesssim$ verken har et største eller et minste element.

Gitt f kan vi definere

$$g_x : \mathbb{R} \to \mathbb{R}$$

ved

$$g_x(y) = \begin{cases} f(y), & y \neq x \\ f(x) - 1, & y = x. \end{cases}$$

Da er $g_x < f$, så det vilkårlig valgte elementet f er ikke minimalt. Tilsvarende for maksimalt.

c) Vis at mengden $\{f, g\} \subseteq \mathcal{F}$ har en minste øvre skranke. Funksjonen

$$h : \mathbb{R} \to \mathbb{R}$$

$$h(x) = \max\{f(x), g(x)\}$$

er en minste øvre skranke. En øvre skranke h' for $\{f, g\}$ må være gitt ved

$$h'(x) \geq \max\{f(x), g(x)\},$$

så $h \leq h'$.

En delmengde $\mathcal{G} \subseteq \mathcal{F}$ er "punktvis begrenset" hvis det for hver $a \in \mathbb{R}$ er en konstant $M_a \in \mathbb{R}$ s.a.

$$|g(a)| \leq M_a$$

for alle $g \in \mathcal{G}$.

(d) Vis at ~~en~~ delmengde $\mathcal{G} \subseteq \mathcal{F}$ har en minste övre ~~og~~ og största nedre skranke hvis og bare hvis den er punktvis begrenset.

Vi begynner med implikasjonen

$\mathcal{G}$ har minste ~~og~~ övre og största nedre skranke $\Rightarrow$ $\mathcal{G}$ er punktvis begrenset

$\Updownarrow$

$\mathcal{G}$ har ikke både minste ~~og~~ övre skranke og största nedre skranke. $\Leftarrow$ $\mathcal{G}$ er ikke punktvis begrenset

Den andre muligheten er tilsvarende.

Anta at G ikke er punktvis begrenset, f.eks. at $a \in \mathbb{R}$ er slik at vi gitt en $N \in \mathbb{N} \subset \mathbb{R}$ kan finne en $g \in G$ med $g(a) > N$. Da har ikke G en gang en øvre skranke, ~~langt mindre en~~ og derfor ikke en minste øvre.

~~Vi~~ Vi viser

G har minste øvre og største nedre $\Longleftarrow$ G er punktvis begrenset.

Anta at G er punktvis begrenset. Ta ~~største~~ minste øvre-tilfellet. I og med at $\mathbb{R}$ har minste øvre skranke-egenskapen kan vi definere $f : \mathbb{R} \to \mathbb{R}$ ved

$$f(a) = \sup_{g \in G} \{ g(a) \}.$$

Det er klart at enhver øvre skranke f' for G må tilfredsstille

$$f'(a) \geq \sup_{g \in G} \{ g(a) \}.$$

$\Rightarrow$ f er minste øvre skranke.