MAT1140 — Strukturer og argumenter

Obligatorisk oppgavesett nr. 1 (av 2)

Løsningsforslag

Oppgave 1. For $a, b \in \mathbb{N}^*$ la $d \in \mathbb{N}^*$ være det mindste naturlige tall som kan skrives som

$$d = ax + by \tag{1}$$

med $x, y \in \mathbb{Z}$. Vis at d er den største tall som deler a og b.

Vi giver her to mulige løsninger til opgave 1:

Løsning. Bemærk at a kan skrives som $a = a \cdot 1 + b \cdot 0$. Så da d er det mindste tal i $\mathbb{N}^*$ som kan kan skrives på formen i likning (1) følger at $d \leq a$. Vi kan nu benytte Euklid's algoritme til at skrive $a = qd + r$, for passende $q, r \in \mathbb{Z}$ med $0 \leq r < d$. Vi kan da skrive r således:

$$r = a - qd = a \cdot (1 - qx) + b \cdot (-qy).$$

Så da $r < d$, og d er det mindste tal i $\mathbb{N}^*$ som kan kan skrives på formen i likning (1), får vi at $r = 0$. Altså er $a = qd$. Med andre ord er d en divisor i a. Samme argument med b i stedet for a viser at d også er en divisor i b. Vi har altså vist at d er en fælles divisor for a og b

La $c \in \mathbb{N}^*$ være en anden fælles divisor for a og b. Da kan vi finde n og m i $\mathbb{Z}$ sådan at $a = cn$ og $b = cm$. Vi indsætter dette i likning (1):

$$d = cnx + cmy = c \cdot (nx + my).$$

Altså er c divisor i d, så specielt er $c \leq d$. Det viser at d er den største fælles divisor.

Løsning. La $d_0 = \gcd(a, b)$. Vi kan da skrive $a = d_0 n$ og $b = d_0 m$ for passende $n, m \in \mathbb{N}^*$. Nu er $d_0 \cdot \gcd(n, m)$ en fælles divisor for a og b, så da d_0 er den største fælles divisor er $\gcd(n, m) = 1$. Pr. Bezout's identitet (fra forelæsningerne) findes $x, y \in \mathbb{Z}$ slik at $1 = nx + my$. Vi ganger med d_0 på begge sider og får at

$$d_0 = d_0 nx + d_0 my = ax + by.$$

Da d er det mindste tall som kan skrives sådan følger det at $d \leq d_0$.

La nu $x, y \in \mathbb{Z}$ være så $d = ax + by$. Vi indsætter $a = d_0 n$ og $b = d_0 m$ i denne likning:

$$d = ax + by = d_0 nx + d_0 my = d_0 \cdot (nx + my).$$

Altså er d_0 en divisor i d og specielt er da $d_0 \leq d$. Samlet set har vi nu vist at $d \leq d_0 \leq d$. Men så må $d_0 = d$.

Oppgave 2. Vis at for alle $N \in \mathbb{N}$ har vi $\sum_{k=0}^{N} 2^k = 2^{N+1} - 1$.

Løsning. Lad $S = \sum_{k=0}^{N} 2^k$. Da er

$$2S = 2 \cdot \sum_{k=0}^{N} 2^k = \sum_{k=0}^{N} 2^{k+1} = \sum_{k=1}^{N+1} 2^k.$$

Det følger at

$$S = 2S - S = \sum_{k=1}^{N+1} 2^k - \sum_{k=0}^{N} 2^k = 2^{N+1} - 1.$$

Oppgave 3. Vis de følgende påstand på to måter, en gang med induksjon og en annen gang uten induksjon: For hvert $n \in \mathbb{N}$ er $n^3 - n$ et multiplum av 6.

Løsning.

Bevis med induksjon. For $n = 0$ har vi $0^3 - 0 = 0$ hvilket er et multiplum av 6. Anta nu at $n^3 - n$ er et multiplum av 6, for et $n \in \mathbb{N}$. Vi har at

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = (n^3 - n) + 3n(n+1).$$

Da n og $n+1$ er to påfølgende tal må mindst ét av dem være et partall. Altså indgår 2 som faktor i $n(n+1)$ og da ser vi at $3n(n+1)$ er et multiplum av 6. Induksjonshypotesen giver os nu at $(n+1)^3 - (n+1)$ er summen av to tall som begge er multiplum av 6. Da er $(n+1)^3 - (n+1)$ selv et multiplum av 6. Pr. induksjon følger at $n^3 - n$ er et multiplum av 6, for alle $n \in \mathbb{N}$. □

Bevis uten induksjon. For hvert $n \in \mathbb{N}$ kan vi skrive:

$$n^3 - n = (n-1)n(n+1).$$

Da $n - 1$, n og $n + 1$ er 3 påfølgende tall er ét av dem et multiplum av 3 og mindst ét av dem et multiplum av 2. Altså er $n^3 - n$ et multiplum av 6. □

Oppgave 4. La P og Q være utsagn. Vis at følgende utsagn er en tautologi:

$$(P \implies (P \implies Q)) \iff (P \implies Q).$$

Løsning. Vi laver en sandhedstabel:

P	Q	$P \implies Q$	$P \implies (P \implies Q)$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Fra sandhedstabellen ser vi at $(P \implies Q)$ og $(P \implies (P \implies Q))$ har samme sandhedsværdi for hvert par av mulige sandhedsværdier for P og Q. Det følger at $(P \implies (P \implies Q)) \iff (P \implies Q)$ er en tautologi.

Oppgave 5. For $n = 2^{20} + 1$ regne ut 2^{n-1} modulo n. Kan vi konkludere fra svaret om n er et primtall eller ikke? Begrunn svaret dit.

Løsning. Vi viser først et nyttigt lemma:

Lemma 1. *For hvert $k, \ell \in \mathbb{N}$ er*

$$2^k \equiv 2^{k \textit{ mod } 2\ell} \textit{ mod } (2^\ell + 1).$$

Bevis. Bemærk at $2^\ell \equiv -1 \bmod 2^\ell + 1$. Derfor er $2^{2\ell} \equiv 1 \bmod 2^\ell + 1$. La $\hat{k} \in \{0, 1, \ldots, 2^\ell + 1\}$ være standardrepresentanten for k modulo 2ℓ. Da finnes $q \in \mathbb{Z}$ slik at $k = 2\ell q + \hat{k}$. Nu er

$$2^k = 2^{\hat{k}+2\ell q} = 2^{\hat{k}}(2^{2\ell})^q \equiv 2^{\hat{k}} \bmod (2^\ell + 1). \qquad \square$$

Vi skal benytte Lemma 1 ovenfor med $\ell = 20$ og $k = 2^{20}$. Vi regner først ut 2^{20} mod 40:

$$2^{20} = (2^5)^4 \equiv (-8)^4 \bmod 40 \equiv (2^3)^4 \bmod 40 \equiv 16^3 \bmod 40.$$

Bemærk at $16 \cdot 16 = 256 \equiv 16 \bmod 40$. Sætter vi dette ind i likningen ovenfor ser vi at

$$2^{20} \equiv 16 \bmod 40.$$

Pr. Lemma 1 med $\ell = 20$ og $k = 2^{20}$ får vi da

$$2^{2^{20}} \equiv 2^{2^{20} \bmod 40} \bmod (2^{20} + 1) \equiv 2^{16} \bmod (2^{20} + 1)$$

Da dette ikke er kongruent med 1 modulo $2^{20} + 1$ følger det av Fermats lille teorem at n ikke er et primtall.

Oppgave 6. La $n \in \mathbb{N}$ og $n \geq 2$. Vis at n er et primtall hvis og kun hvis

$$(n-1)! \equiv -1 \bmod n.$$

Løsning. Anta at n er et primtall. For hvert naturligt tall $1 \leq k \leq n-1$ er da $\gcd(k, n) = 1$. Pr. teoremet på side 9 i forelæsning 3 finnes da et $\ell \in \mathbb{Z}$ slik at $k\ell \equiv 1 \bmod n$. Det er klart at vi kan vælge ℓ slik at $1 \leq \ell \leq n-1$, og at der for hvert $1 \leq k \leq n-1$ findes præcist ét $1 \leq \ell \leq n-1$ slik at $k\ell \equiv 1 \bmod n$.

Lemma 2. *La p være et primtal og la $1 \leq k \leq p-1$ være et naturligt tall. Hvis $k^2 \equiv 1$ mod p så er enten $k = 1$ eller $k = p-1$.*

Bevis av Lemma. Vi har $k^2 - 1 = (k+1)(k-1)$. Da p er et primtal følger, at hvis $k^2 - 1 \equiv 0 \mod p$ så må p være en divisor i enten $k+1$ eller $k-1$. I første tilfælde følger at $k = p-1$ og i siste tilfælde følger at $k = 1$. $\square$

Fra lemmaet ser vi, at av tallene $1, 2, \ldots, n-1$ er det bare 1 og $n-1$ som er sin egen multiplikative invers modulo n. De resterende tall $2, \ldots, n-2$ kan parres to og to sådan at produktet av hvert par er lik 1 mod n. Vi får da,

$$[(n-1)!]_n = ([2]_n \cdot [3]_n \cdot \cdots \cdot [n-2]_n) \cdot [n-1]_n = [1]_n \cdot [n-1]_n = [-1]_n$$

Med andre ord er $(n-1)! \equiv -1 \mod n$, som vi ville vise.

Vi giver her 3 forskellige beviser for den modsatte implikasjon. I enhver løsning er det naturligvis kun nødvendigt at give ét bevis.

Bevis for "$\Leftarrow$" (direkte). Anta at $(n-1)! \equiv -1 \mod n$. Vi kan da finde et $q \in \mathbb{Z}$ slik at $(n-1)! = qn + (n-1)$. Hvis vi omorganiserer har vi altså at $(n-1)! - qn = n - 1$. Så hvis et naturligt tall $1 \leq d < n$ er en divisor i n så er d også en divisor i $n-1$. Men så er d også en divisor i $1 = n - (n-1)$. Altså må vi ha $d = 1$. De eneste (ikke-negative) divisorer i n er derfor 1 og n. Med andre ord er n et primtall. $\square$

Bevis for "$\Leftarrow$" (kontrapositon). Anta at n *ikke* er et primtall. Vi har nu 2 muligheder: enten kan vi skrive $n = a \cdot b$ for naturlige tall $1 < a, b < n$ slik at $a \neq b$ eller så er $n = a^2$ for et naturligt tall $a > 1$. Vi skal behandle disse to tilfælde hver for sig. Desuden må tilfældet $n = 4$ behandles separat.

(1) Anta at $n = a \cdot b$ for naturlige tall $1 < a, b < n$ slik at $a \neq b$. Vi ser at a og b optræder separat i produktet $(n-1)! = 2 \cdot 3 \cdot \cdots \cdot (n-1)$. Altså er n en divisor i $(n-1)!$ og dermed er $(n-1)! \equiv 0 \mod n$.

(2) Anta at $n = a^2$ for et naturligt tall $a > 2$. Vi har da at $1 < a, 2a < n$ så a og $2a$ optræder separat i produktet $(n-1)! = 2 \cdot 3 \cdot \cdots \cdot (n-1)$. Altså er $2n = (2a) \cdot a$ en divisor i $(n-1)!$. Da n er en divisor i $2n$ får vi da at n er en divisor i $(n-1)!$ og dermed er $(n-1)! \equiv 0 \mod n$.

(3) For $n = 4$ har vi at $(4-1)! = 6$ og videre at $6 \equiv 2 \mod 4$. Men $2 \not\equiv -1 \mod 4$.

I alle 3 tilfælde er $(n-1) \not\equiv -1 \mod n$, hvilket var hvad vi ville vise. $\square$

Bevis for "$\Leftarrow$" (motstrid). Anta for motstrid at $(n-1)! \equiv -1 \mod n$ *og* at n er et sammensat tall. Vi kan da skrive $n = a \cdot b$, for passende naturlige tall $1 < a, b < n$. Da $(n-1)!$ er produktet av alle naturlige tall fra 1 till og med $n-1$ ser vi at a må være en faktor i $(n-1)!$. Da er n en faktor i $b \cdot (n-1)!$, så vi ser at $b \cdot (n-1)! \equiv 0 \mod n$. Men $(n-1)! \equiv -1 \mod n$, så samtidigt er $b \cdot (n-1)! \equiv -b \mod n$. Vi får altså at $b \equiv 0 \mod n$ og dermed at $n \leq b$. Men nu er $n \leq b < n$, hvilket er en motstrid $\lightning$. $\square$

Oppgave 7. La A og B være mengder.

1. Vis at $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
2. Vis at $\mathcal{P}(A \cup B) \supseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.

Er der mengder A og B hvor $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$?

Løsning. La C være en mengde. Pr. definition av potensmengden er $C \in \mathcal{P}(A \cap B)$ hvis og bare hvis $C \subseteq A \cap B$. Pr. definition av snittet av to mengder er dette tilfældet hvis og bare hvis $C \subseteq A$ og $C \subseteq B$. Dette er tilfældet hvis og bare $C \in \mathcal{P}(A)$ og at $C \in \mathcal{P}(B)$, pr. definition av potensmengden. Til slut er dette tilfældet hvis og bare hvis $C \in \mathcal{P}(A) \cap \mathcal{P}(B)$, hvor vi igen benytter definitionen av snittet.

La nu $C \in \mathcal{P}(A) \cup \mathcal{P}(B)$. Pr. definition av unionen av to mengder er da $C \in \mathcal{P}(A)$ eller $C \in \mathcal{P}(B)$. Pr. definition av potensmengden er i det første tilfælde $C \subseteq A$ og i det andet tilfælde $C \subseteq B$. Nu er både $A \subset A \cup B$ og $B \subset A \cup B$ pr. definition av unionen. Så i begge tilfælde er $C \subset A \cup B$ hvorfra vi slutter at $C \in \mathcal{P}(A \cup B)$ pr. definition av potensmengden.

Ja, der er mengder A og B hvor $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$. Et eksempel er $A = \{0\}$ og $B = \{1\}$. Her er mængden $A \cup B = \{0, 1\}$ et element i $\mathcal{P}(A \cup B)$ men ikke i $\mathcal{P}(A) \cup \mathcal{P}(B)$.