

Lösningsförslag 2024-10-26

11 Svar: (ii) och (iv) är tautologier.

Lösning: Kan här: en tautologi är en sammansatt utsaga där sanningsvärdet är 1 oavsett sanningsvärdena för de ingående $\mathcal{B}$ och de variablerna (här p, q, r).

Vi kan göra sanningsbatter, med 8 fall i rader, men kan också komma till svaret mer direkt. En implikation är alltid sann om hypotesen är falsk, varför fall med hypotesen sann är de intressanta att undersöka.

Fall (i): Tag p, q sanns. Då gäller att $(p \rightarrow q) \wedge q$ är sann, men

$\neg p$ är falsk. Då hypotesen sann
men slutsatsen falsk $\Rightarrow$ inte en
tautologi.

Fall (i): Hypotesen sann innebär att

$\neg r$ är sann $\Rightarrow r$ falsk.

För att $p \rightarrow r$ ska vara sann måste lösningen
vara p vara falsk.

Då slutsatsen $\neg p$ är sann, verkar (i) är
en tautologi.

Fall (ii): Hypotesen inkluderar $r \wedge \neg r$,
vilket förstås är falskt. Då, hypotesen
alltså sann, verkar implikationen
alltså är sann; uttrycket är en
tautologi.

2)

a) Svar: 96.

Antalet som söker är $\Phi(195)$. Eftersom $195 = 3 \cdot 5 \cdot 13$

$$\begin{aligned}\text{har vi } \Phi(195) &= \Phi(3 \cdot 5 \cdot 13) = \Phi(3) \Phi(5) \Phi(13) \\ &= 2 \cdot 4 \cdot 12 = \underline{\underline{96}}.\end{aligned}$$

b) Svar: $\text{sgd}(273, 756) = 21$.

Via Euklides algoritmen har vi:

$$756 = \underbrace{2 \cdot 273}_{546} + 210$$

$$273 = 1 \cdot 210 + 63$$

$$210 = 3 \cdot 63 + 21$$

$$63 = 3 \cdot 21 + 0$$

$$\Rightarrow \text{sgd}(756, 273) = 21$$

31

a) Svar: $W_n = \begin{cases} 3^n, & n \text{ udda} \\ 0, & n \text{ jämnt} \end{cases}$

Lösning: Om n är ett jämnt tal finns det 0 vägar, d.e. vi måste vara tillbaka på samma sida av $H_{3,3}$ som vi startade (dvs, en nod med samma "färg" som n).

För n udda finns det i alla steg utan det sista 3 val på noden att gå till, i det sista steget måste vi sedan gå till n .

$$\Rightarrow \underbrace{3 \cdot 3 \cdot \dots \cdot 3}_{n-1 \text{ steg}} \cdot 1 = 3^{n-1} \text{ olika vägar.}$$

b) Svar: 80

Lösning: För en 8-bits sträng som startar med 1011 finns det fyra "fria" platser med två möjliga val (0 & 1) för varje $\Rightarrow 2^4 = 16$ möjliga strängar enligt multiplikationsprincipen.

På samma sätt, om strängen startar med 01 finns det $2^6 = 64$ möjliga 8-bits strängar.

Additionsprincipen ger nu totalt $16 + 64 = 80$ strängar.

c) Svar: 37.

Lösning: Antal 8-bits strängar med exakt 6 1:or

$$\text{är } \binom{8}{6} = \frac{8!}{6!(8-6)!} = \frac{8 \cdot 7}{1 \cdot 2} = 28$$

Anzahl ~~8~~ bits strings weil exakt 7 $1-w: \binom{8}{7} = 8,$

_____ 1 _____ 8 $1-w: 1$

$\Rightarrow$ Anzahl strings weil ~~set~~ either 1-w or

disjunct $28 + 8 + 1 = \underline{\underline{37}}$

4) Ekvationssystemet: $x \equiv 1 \pmod{7}$

$$2x \equiv 1 \pmod{9}$$

$$4x \equiv 1 \pmod{11}$$

Visa att $\text{sgd}(7,9) = \text{sgd}(7,11) = \text{sgd}(9,11) = 1$ så vi vet att systemet har lösningar.

Vi börjar med att sluta av så att vi endast har x i vänsterledet: $\text{sgd}(2,9) = 1$ så invers finns.

För att hitta inversen till 2 i $\mathbb{Z}_9$ använder vi Euklides alg.:

$$\left. \begin{array}{l} 9 = 4 \cdot 2 + 1 \\ 2 = 2 \cdot 1 + 0 \end{array} \right\} \Rightarrow 1 = 9 - 4 \cdot 2$$

$$\text{där } [2]^{-1} = [-4] \text{ i } \mathbb{Z}_9, \text{ så } [2]^{-1} = [5] \text{ i } \mathbb{Z}_9$$

$$\Rightarrow x \equiv 5 \pmod{9}$$

På samma sätt hittar vi inversen till 4 i $\mathbb{Z}_{11}$:

$$\left. \begin{array}{l} 11 = 2 \cdot 4 + 3 \\ 4 = 1 \cdot 3 + 1 \\ 3 = 3 \cdot 1 + 0 \end{array} \right\} \Rightarrow \begin{array}{l} 1 = 4 - 3 = 4 - (11 - 2 \cdot 4) \\ \quad \quad \quad = 3 \cdot 4 - 11 \end{array}$$

$$\Rightarrow [4]^{-1} = [3] \text{ i } \mathbb{Z}_{11}$$

(Notera att här kan vi relativt enkelt se att $[2]^{-1} \in \mathbb{Z}_9$ & $[4]^{-1} \in \mathbb{Z}_{11}$ utan att använda Euklides alg.)

$\Rightarrow$ sätter vi in lösningarna i systemet så får vi $x \equiv 3 \pmod{11}$.

"Kongruens" system:

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 5 \pmod{9} \\ x \equiv 3 \pmod{11} \end{cases}$$

Lösar med substitutionsmetoden:

Sätt $x = 1 + k \cdot 7$, sätt in i andra ekvationen:

$$1 + k \cdot 7 \equiv 5 \pmod{9}$$

$$\Leftrightarrow 7k \equiv 4 \pmod{9} \quad [\text{sgd}(7,9)=1]$$

Hitta inversen till 7 i $\mathbb{Z}_9$: $[7]^{-1} = [13] = [4]$ i $\mathbb{Z}_9$

$$\Rightarrow k \equiv 4 \cdot 4 \equiv 16 \equiv 7 \pmod{9}$$

Sätt $k = 7 + 9y$, $y \in \mathbb{Z}$.

$$\begin{aligned} \Rightarrow x &= 1 + 7k \\ &= 1 + 7(7 + 9y) \\ &= 1 + 49 + 63y \\ &= 50 + 63y \end{aligned}$$

Sätt in i 3:e ekvationen ($x \equiv 3 \pmod{11}$)

$$\overbrace{50 + 63y}^x \equiv 3 \pmod{11}$$

$$\Leftrightarrow 6 + 8y \equiv 3 \pmod{11}$$

$$\Leftrightarrow 8y \equiv -3 \pmod{11}$$

$$\Leftrightarrow 8y \equiv 8 \pmod{11}$$

Eftersom $\text{sgd}(8,11)=1$ har vi att den är invertibel med
 $y \equiv 1 \pmod{11}$

$$\Rightarrow y = 1 + 11z, z \in \mathbb{Z}$$

Satt in i uttrykket for x :

$$\begin{aligned} x &= 50 + 63y = 50 + 63(1 + 11z) \\ &= 50 + 63 + 693z \\ &= \underline{113 + 693z}, z \in \mathbb{Z}. \end{aligned}$$

(Noter: $693 = 7 \cdot 9 \cdot 11$)

Minste positive heltall som oppfyller likningssystemet er
dermed $x_0 = 113$ (dvs veli $z=0$ oven).

Svar: $x_0 = 113$.

5)

a) Se föreläsninganteckningarna eller boken.

b) En Bannoni ges av

$a \rightarrow B$

$b \rightarrow A$

$c \rightarrow C$

$d \rightarrow E$

$e \rightarrow G$

$f \rightarrow D$

$g \rightarrow F$

c) Gradtal:

v	d_v
a	2
b	4
c	4
d	5
e	1
f	4
g	2

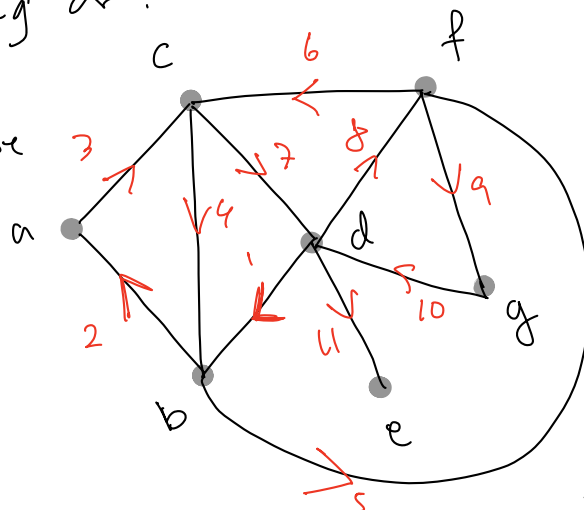
$\Rightarrow$ alla utom d & e har ett jämnt gradtal.

Därför finns ingen Eulerskyl, men det finns en

Eulerstig mellan d & e .

Exempel på en sådan väg är:

$d \rightarrow b \rightarrow a \rightarrow c \rightarrow b \rightarrow f \rightarrow c \rightarrow d \rightarrow f \rightarrow g \rightarrow d \rightarrow e$
 1 2 3 4 5 6 7 8 9 10 11



bl. 1) Ett första bevis ges av binomialformeln: För x, y har vi

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

$$\text{Sätt } x=y=1 \Rightarrow 2^n = \sum_{k=0}^n \binom{n}{k} //$$

ii) Vi kan använda oss av tolkningen av $\binom{n}{k}$:

Ur en mängd med n element, på hur många sätt kan vi plocka ut k av dem. $\binom{n}{k}$ är därmed antalet delmängder ur, t.ex., $\{1, 2, \dots, n\}$ med k element.

$$\Rightarrow \sum_{k=0}^n \binom{n}{k} \text{ är totalt antalet delmängder till}$$

$$\{1, 2, \dots, n\}.$$

Det senare är precis strukturen av potensmängder

$$\mathcal{P}(\{1, 2, \dots, n\}), \text{ som vi vet är } 2^n. \left[\text{Allt: } n \text{ oberoende val,} \right. \\ \left. \text{med 2 möjligheter} \right]$$

iii) Vi visar påståendet via induktion.

För basfallet $n=1$ har vi

$$\left. \begin{array}{l} \text{V.h.} = \binom{1}{0} + \binom{1}{1} = 1+1=2 \\ \text{H.h.} = 2^1 = 2 \end{array} \right\} \text{V.h.} = \text{H.h.}, \text{ så ok.}$$

Antag nu att påståendet gäller för $n \geq 2$.

Betrakta fallet $n+1$:

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \binom{n+1}{n+1} + \sum_{k=0}^n \binom{n+1}{k}$$

$$= 1 + \sum_{k=0}^n \binom{n+1}{k}$$

Betrakta nu summan ovan: Grått är allmänt att

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

$$\begin{aligned} \Rightarrow \sum_{k=0}^n \binom{n+1}{k} &= \binom{n+1}{0} + \sum_{k=1}^n \binom{n+1}{k} \\ &= 1 + \sum_{k=1}^n \left(\binom{n}{k-1} + \binom{n}{k} \right) \\ &= 1 + \sum_{k=1}^n \binom{n}{k-1} + \sum_{k=1}^n \binom{n}{k} \quad (*) \end{aligned}$$

Grått att

$$\begin{aligned} \sum_{k=1}^n \binom{n}{k-1} &= \sum_{k=0}^{n-1} \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} - \binom{n}{n} \\ &= \sum_{k=0}^n \binom{n}{k} - 1 \end{aligned}$$

Hilande: $\sum_{k=1}^n \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} - \binom{n}{0} = \sum_{k=0}^n \binom{n}{k} - 1$

Sätt in i (*):

$$\begin{aligned} 1 + \sum_{k=1}^n \binom{n}{k-1} + \sum_{k=1}^n \binom{n}{k} &= 1 + \left(\sum_{k=0}^n \binom{n}{k} - 1 \right) + \left(\sum_{k=0}^n \binom{n}{k} - 1 \right) \\ &= 2 \sum_{k=0}^n \binom{n}{k} - 1 \end{aligned}$$

Från induktionsantagandet:

$$2 \cdot \sum_{k=0}^n \binom{n}{k} = 2 \cdot 2^n = 2^{n+1}$$

$\forall i$ har det med rest , med induktionsbegreppet, att

$$\begin{aligned}\sum_{k=0}^{n+1} \binom{n+1}{k} &= \binom{n+1}{n+1} + \sum_{k=0}^n \binom{n+1}{k} \\ &= 1 + \sum_{k=0}^n \binom{n+1}{k} \\ &= 1 + 2^{n+1} - 1 \\ &= \underline{\underline{2^{n+1}}}\end{aligned}$$

De påstående som gäller även för $n=0$ ger induktionsprincipen
nu att det är sant för samtliga $n \geq 1$, dvs:

$$\text{för heltal } n \geq 1 \text{ gäller } \sum_{k=0}^n \binom{n}{k} = \underline{\underline{2^n}}$$

7)

a) Behöver visa att R är reflexiv, symmetrisk & transitiv.

Reflexiv: $aRa \Leftrightarrow a * a^{-1} \in H$.

Men $e \in H$ och $a * a^{-1} = e$, därför aRa .

Symmetri: Tag $a, b \in G$ och antag aRb .

$aRb \Leftrightarrow a * b^{-1} \in H$. Kalla motsvarande element i H för x_{ab} :

$$a * b^{-1} = x_{ab} \in H$$

Betrakta $b * a^{-1}$. Gäller att $b * a^{-1} \in G$ och vi kan därför beräkna

$$\begin{aligned} (b * a^{-1}) * x_{ab} &= b * (a^{-1} * x_{ab}) && \text{Associativ} \\ \left. \begin{array}{l} \text{def. av} \\ x_{ab} \end{array} \right\} &= b * (a^{-1} * (a * b^{-1})) \\ \left. \begin{array}{l} * \\ \text{associativ} \end{array} \right\} &= b * ((a^{-1} * a) * b^{-1}) \\ \left. \begin{array}{l} a^{-1} \text{ invers till } a \\ \text{m.a.p. } * \end{array} \right\} &= b * (e * b^{-1}) \\ \left. \begin{array}{l} e \\ \text{identitet} \end{array} \right\} &= b * b^{-1} = e \end{aligned}$$

Det vill säga $b * a^{-1}$ är en invers till $x_{ab} = a * b^{-1}$.

Eftersom $*$ är associativ finns det som mest en invers till ett element i $G \Rightarrow b * a^{-1}$ är enda inversen till $a * b^{-1}$.

Men $a * b^{-1} \in H$, därför även $b * a^{-1} \in H$ (H delgrupp)
 $\Rightarrow bRa$.

Vi har alltså visat att för $a, b \in G$ gäller

$$aRb \Rightarrow bRa,$$

dvs R är symmetrisk.

Transitiv: Tag $a, b, c \in G$ och antag aRb , bRc .

$$\Rightarrow a * b^{-1} \in H, \quad b * c^{-1} \in H.$$

$*$ en operator på H

$$\Rightarrow (a * b^{-1}) * (b * c^{-1}) \in H$$

$$\begin{aligned} \text{Från } * \text{ associativitet: } (a * b^{-1}) * (b * c^{-1}) &= a * (\underbrace{b^{-1} * b}_{=e}) * c^{-1} \\ &= a * e * c^{-1} \\ &= a * c^{-1} \end{aligned}$$

$$\Rightarrow a * c^{-1} \in H$$

Alltså gäller aRc ; R är transitiv.

Ovan visar tillsammans att R är en ekvivalensrelation.

$$b) H_N = \{ k \in \mathbb{Z} : N | k \}, \quad N \in \mathbb{Z}_+.$$

i) $(\mathbb{Z}, +)$ en grupp: Vi behöver verifiera villkoren för en grupp.

$+$ är en associativ operator, med identitet $0 \in \mathbb{Z}$.

Vidare har varje element $n \in \mathbb{Z}$ invers $-n$ m.p. $\mathbb{Z}$.

$\Rightarrow \mathbb{Z}$ med addition är en grupp.

ii) Behöver nu visa att H_N är en delgrupp.

Först gäller att för två element $g, h \in H_N$ att

$$g+h \in H_N, \text{ ty } N|g, N|h \Rightarrow N|g+h.$$

Alltså är $+$ en operator på H_N och den är uppenbart associativ. Vidare gäller $0 \in H_N$ för alla N , är identiteten (för $+$) finns i H_N .

Slutligen ser vi att för ett $g \in H_N$ (säger också) inversen $g^{-1} \in H_N$, ty $N|g \Rightarrow N|(g-g)$.

Alltså är H_N en delgrupp till $\mathbb{Z}$.

4) Tag $G = \mathbb{Z}$, addition som operator och $H = H_N$.

R definieras som, för $a, b \in \mathbb{Z}$,

$$aRb \Leftrightarrow a-b \in H,$$

Vilket här betyder

$$a + (-b) \in H$$

$$\Leftrightarrow N|a-b$$

Det vill säga $aRb \Leftrightarrow \overline{a \equiv b \pmod{N}}$

Svar: R är relationen "kongruens modulo N ".