Lösningar för tenta i TMV200 Diskret matematik 2019-04-25 kl. 14:00–18:00

1. Om argumentet *inte* är giltigt går det att hitta ett motexempel, dvs en uppsättning sanningsvärden för vilka alla hypoteserna är sanna medan slutsatsen är falsk. Vi försöker konstruera ett motsägelsebevis, och om det inte går så är argumentet giltigt. Vi gör därför antagandet att alla hypoteserna är sanna och att slutsatsen är falsk, och ser vad det leder till.

Slutsatsen består av en implikation, och enda fallet där en implikation är falsk är fallet $S \to F$, så för att göra slutsatsen falsk måste $p = F$ och $r = S$. Med dessa sanningsvärden blir första hypotesen och tredje hypotesen uppfyllda.

Enda sättet att få fjärde hypotesen sann är att sätta $q = S$.

I andra hypotesen är $(r \wedge \neg p) = S$, och hypotesen blir alltså sann med de tilldelade sanningsvärdena. Vi har alltså hittat ett motexempel, som gör hypoteserna sanna med slutsatsen falsk ($p = F$ och $q = r = S$).

Svar: Argumentet är inte giltigt, och ett motexempel är $p = F$ och $q = r = S$.

2. Vi visar detta genom induktion. Inför beteckningarna

$$VL(n) = \sum_{k=1}^{n} \frac{4}{k(k+1)(k+2)} \qquad \text{och} \qquad HL(n) = \frac{n(n+3)}{(n+1)(n+2)},$$

och låt $U(n)$ vara utsagan (påståendet) att $VL(n) = HL(n)$.

Eftersom

$$VL(1) = \sum_{k=1}^{1} \frac{4}{k(k+1)(k+2)} = \frac{4}{1(1+1)(1+2)} = \frac{4}{6} = \frac{2}{3}$$

och

$$HL(1) = \frac{1(1+3)}{(1+1)(1+2)} = \frac{4}{6} = \frac{2}{3}$$

är $U(1)$ sann, och vi har alltså ett giltigt *basfall*.

Vi skall nu visa *induktionssteget*, dvs att $U(p) \Rightarrow U(p+1)$. Antag därför att $U(p)$ är sann för något visst p, dvs att $VL(p) = HL(p)$. Det gäller nu att

$$\begin{aligned}
VL(p+1) &= \sum_{k=1}^{p+1} \frac{4}{k(k+1)(k+2)} \\
&= \frac{4}{(p+1)(p+1+1)(p+1+2)} + \sum_{k=1}^{p+1} \frac{4}{k(k+1)(k+2)} \\
&= \frac{4}{(p+1)(p+2)(p+3)} + VL(p) = \frac{4}{(p+1)(p+2)(p+3)} + HL(p) \\
&= \frac{4}{(p+1)(p+2)(p+3)} + \frac{p(p+3)}{(p+1)(p+2)} \\
&= \frac{4}{(p+1)(p+2)(p+3)} + \frac{p(p+3)^2}{(p+1)(p+2)(p+3)} \\
&= \frac{4 + p(p^2+6p+9)}{(p+1)(p+2)(p+3)} = \frac{p^3+6p^2+9p+4}{(p+1)(p+2)(p+3)} \\
&= \frac{(p+1)^2(p+4)}{(p+1)(p+2)(p+3)} = \frac{(p+1)(p+4)}{(p+2)(p+3)} = HL(p+1),
\end{aligned}$$

där de karmosinröda uttrycken ovan är lika enligt antagandet att $U(p)$ är sann. Vi har nu funnit att $U(p+1)$ är sann så fort $U(p)$ är sann, dvs induktionssteget $U(p) \Rightarrow U(p+1)$ gäller.

Vi har ett giltigt basfall och ett induktionssteg, och *induktionsprincipen* ger därför att $U(n)$ är sann för alla heltal $n \geq 1$.

3. (a) Om $u = a + b\sqrt{3}$ så är $u^2 = (a + b\sqrt{3})^2 = a^2 + 2ab\sqrt{3} + 3b^2$. Är detta ett heltal måste $ab = 0$, dvs $a = 0$ eller $b = 0$. Om $a = 0$ så är $u\sqrt{3} = b\sqrt{3}\sqrt{3} = 3b$ ett heltal, och om $b = 0$ så är $u = a$ ett heltal.

(b) Om $u = a + b\sqrt{3}$ och $v = c + d\sqrt{3}$ så blir

$$uv = (a + b\sqrt{3})(c + d\sqrt{3}) = ac + ad\sqrt{3} + bc\sqrt{3} + 3bd,$$

som kan skrivas $s + t\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ med heltalen $s = ac + 3bd$ och $t = ad + bc$.

Svar: Ja, $\mathbb{Z}[\sqrt{3}]$ är sluten under multiplikation.

(c) Vi söker ett element $a + b\sqrt{3}$ sådant att $(a + b\sqrt{3})(7 + 4\sqrt{3}) = 1$. Detta kräver att koefficienten framför $\sqrt{3}$ är noll och det "ensamma" heltalet är ett. Med hjälp av räkningarna i (b) ser vi att det sker då

$$\begin{cases} 7a + 12b = 1 \\ 4a + 7b = 0 \end{cases} \Leftrightarrow \begin{cases} 7a + 12b = 1 \\ -b = 4 \end{cases} \Leftrightarrow \begin{cases} a = 7 \\ b = -4. \end{cases}$$

Ekvationssystemet lösning gav heltal, dvs vi har hittat elementet vi sökte. En enkel kontroll visar också att $(7 - 4\sqrt{3})(7 + 4\sqrt{3}) = 7^2 - 3 \cdot 4^2 = 1$, som önskat.

Svar: Ja, $7 - 4\sqrt{3}$ är invers till $7 + 4\sqrt{3}$.

(d) Antag att $a + b\sqrt{3}$ har den multiplikativa inversen $c + d\sqrt{3}$. Om

$$(a + b\sqrt{3})(c + d\sqrt{3}) = ac + ad\sqrt{3} + bc\sqrt{3} + 3bd = 1$$

så måste $ac + 3bd = 1$. Om $d = \text{sgd}(a, b)$ så gäller att $d | ac + 3bd$, och då måste även $d | 1$. De enda talen som delar 1 är ± 1, och eftersom $d = \text{sgd}(a, b) > 0$ måste $d = 1$, vilket skulle visas.

4. Låt x beteckna antalet krusbärspajer. Då söker vi den minsta positiva lösningen till kongruenssystemet

$$\begin{cases} 3x \equiv 1 \mod 71 \\ x \equiv 28 \mod 70 \end{cases} \Leftrightarrow \begin{cases} x \equiv g \mod 71 \\ x \equiv 28 \mod 70, \end{cases}$$

där g är den multiplikativa inversen till 3 modulo 71 (det finns garanterat en sådan, då $\text{sgd}(3, 71) = 1$). Eftersom $\text{sgd}(70, 71) = 1$ lovar kinesiska restsatsen att systemet är lösbart.

Vi börjar med att bestämma g. Euklides algoritm ger

$$\begin{aligned} 71 &= 23 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1, \end{aligned}$$

så att $1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (71 - 23 \cdot 3) = 24 \cdot 3 - 71$. Detta ger oss att $g = 24$ duger som invers.

Första kongruensen ger nu att $x = 24 + 71s$ för något heltal s. Insättning av detta i andra kongruensen ger

$$24 + 71s \equiv 28 \mod 70 \quad \Leftrightarrow \quad s \equiv 4.$$

Detta innebär att $s = 4 + 70t$ för något heltal t.

Eftersom $x = 24 + 71s$ får vi

$$x = 24 + 71s = 24 + 71(4 + 70t) = 24 + 71 \cdot 4 + 4970t = 308 + 4970t,$$

där t är ett godtyckligt heltal. Minsta positiva lösningen blir $x = 308$.

Svar: Minsta positiva lösningen är $x = 308$.

5. (a) Vi kontrollerar att $\mathcal{R}$ är *reflexiv*:

$$a\mathcal{R}a \quad \Leftrightarrow \quad D(a) = D(a),$$

symmetrisk:

$$a\mathcal{R}b \quad \Leftrightarrow \quad D(a) = D(b) \quad \Leftrightarrow \quad D(b) = D(a) \quad \Leftrightarrow \quad b\mathcal{R}a,$$

och *transitiv*:

$$\begin{cases} a\mathcal{R}b \\ b\mathcal{R}c \end{cases} \Leftrightarrow \quad \begin{cases} D(a) = D(b) \\ D(b) = D(c) \end{cases} \Rightarrow \quad D(a) = D(c) \quad \Leftrightarrow \quad a\mathcal{R}c.$$

(b) Eftersom $98 = 2 \cdot 7^2$ är $D(98) = 7^2$.

Antag att x uppfyller $D(x) = 7^2$. Då måste $x = k \cdot 7^2$ för mågot heltal $k > 1$. Vi kan inte ha $k > 7$, eftersom då blir $D(x) = 7k \neq 7^2$, så $2 \leq k \leq 7$. Dessutom måste k vara ett primtal, för om $k = mn$ med $m \geq n > 1$ blir $D(x) = D(mn \cdot 7^2) \geq m \cdot 7^2 \neq 7^2$.

Svar: Ekvivalensklassen som innehåller 98 är $\{98, 147, 245, 343\}$.

6. (a) Bokstäverna M, U, och R finns i dubbel uppsättning, medan E, L, D, och J endast finns i vardera ett exemplar.

- Det finns endast ett sätt att välja ut sju *olika* bokstäver, och sedan kan vi bilda 7! olika ”ord” med dem.
- Om vi vill använda precis en bokstav två gånger kan vi välja bokstäverna på $\binom{3}{1} \cdot \binom{6}{5} = 3 \cdot 6 = 18$ olika sätt, och vi kan sedan bilda $\frac{7!}{2!}$ olika ”ord” med dem. Det ger $9 \cdot 7!$ olika ”ord”.
- Om vi vill använda precis två bokstäver två gånger kan vi välja bokstäverna på $\binom{3}{2} \cdot \binom{5}{3} = 3 \cdot 10 = 30$ sätt, och sedan kan vi bilda $\frac{7!}{2! \cdot 2!}$ ”ord” med dem. Det ger $15 \cdot \frac{7!}{2!}$ olika ”ord”.
- Om vi vill använda alla dubbletterna kan vi välja den sista bokstaven på fyra sätt, och sedan kan $\frac{7!}{2! \cdot 2! \cdot 2!}$ olika ”ord” bildas. Det ger $\frac{7!}{2!}$ olika ”ord”.

Sammanlagt får vi $7! + 9 \cdot 7! + 15 \cdot \frac{7!}{2!} + \frac{7!}{2!} = 18 \cdot 7!$ ”ord”.

Svar: Det kan bildas $18 \cdot 7!$ ”ord”.

(b) Vi delar upp i samma typ av fall som i (a).

- Använder vi sju olika bokstäver får vi 7! olika ”ord” precis som tidigare.
- Om vi använder precis en bokstav två gånger får vi $18 \cdot 6!$ ”ord”.

- Om vi använder precis två bokstäver två gånger får vi $30 \cdot 5!$ ”ord”.
- Om vi använder alla dubbletterna får vi $4 \cdot 4!$ ”ord”.

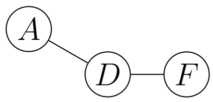
Sammanlagt får vi $7! + 18 \cdot 6! + 30 \cdot 5! + 4 \cdot 4!$ ”ord”.

Svar: Det kan bildas $7! + 18 \cdot 6! + 30 \cdot 5! + 4 \cdot 4!$ ”ord”.

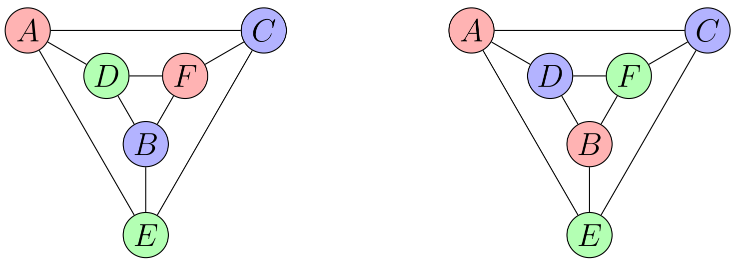
(c) Sätt ihop LEMUR till symbolen $\mathcal{L}$. Vi har då ”bokstäverna” $\mathcal{L}$MURDJ att använda. Vi måste använda $\mathcal{L}$ och två av de fem övriga, vilket ger $\binom{5}{2} \cdot 3! = \frac{5!}{2!} = 60$ ”ord”.

Svar: Det kan bildas 60 sådana ”ord”.

7. (a) **Svar:** Ett exempel fås genom att ta bort noderna B, C, och E:



(b) Noderna A, C, och E måste uppenbarligen vara i olika nodmängder. På samma sätt måste D, F, och B också vara i olika nodmängder. Vi ser att det finns precis två indelningar:



Svar: Det finns två sådana indelningar.

(c) Grafen är sammanhängande och består av sex noder med gradtal tre. För att det skall finnas en Eulerväg får grafen innehålla högst två noder med udda gradtal. Detta går inte att åstadkomma genom att ta bort endast en kant, men det går om vi tar bort två kanter (exempelvis kanten C till F och kanten B till E).

Svar: Minsta antalet kanter som behöver plockas bort för att grafen skall få en Eulerväg är två.

(d) För att grafen skall få en Eulercykel behöver vi se till så att alla nodernas gradtal är jämna. Vi måste lägga till minst tre kanter för att lyckas ändra gradtalet på alla sex noderna. Det visar sig också att tre kanter räcker; lägg exempelvis till kanter från A till B, från C till D, och från E till F (jämför med de tripartita indelningarna ovan).

Svar: Minsta antalet kanter som behöver läggas till för att grafen skall få en Eulercykel är tre.

8. (a) Vi börjar med att faktorisera $980 = 2^2 \cdot 5 \cdot 7^2$, och vi får sedan

$$\Phi(980) = \Phi(2^2) \cdot \Phi(5) \cdot \Phi(7^2) = 2^1(2-1) \cdot (5-1) \cdot 7^1(7-1) = 336.$$

Svar: $\Phi(980) = 336$.

(b) Eulers sats ger oss $3^{\Phi(980)} \equiv 3^{336} \equiv 1 \mod 980$, eftersom $\operatorname{sgd}(3, 980) = 1$ enligt faktoriseringen i (a). Vi får

$$x \equiv 3^{2019} \equiv 3^{6 \cdot 336 + 3} \equiv (3^{336})^6 \cdot 3^3 \equiv 1^6 \cdot 3^3 \equiv 27 \mod 980.$$

Svar: Det minsta positiva sådana talet är $x = 27$.