Lösningar för tenta i TMV200 Diskret matematik 2019-08-30 kl. 14:00–18:00

1. Antag att alla hypoteserna är sanna samtidigt som slutsatsen är falsk. Lyckas vi hitta värden på variablerna så att detta gäller har vi ett motexempel som visar att argumentet inte är giltigt, och om det visar sig att det inte finns något motexempel så har vi istället gjort ett motsägelsebevis som visar att argumentet är giltigt.

Enligt antagandet är slutsatsen falsk, dvs minst en av de tre variablerna har sanningsvärdet F. Låt oss säga att $r = F$. Då blir tredje hypotesen automatiskt uppfylld, eftersom implikationen $F \to x$ är sann för alla x.

Första hypotesen kan förenklas till $p \to q$ och andra hypotesen till $q \to p$, dvs tillsammans blir de $p \leftrightarrow q$. Detta är sant precis då p och q har samma sanningsvärde. Sätter vi $p = q = S$ blir fjärde hypotesen sann, och vi har alltså hittat ett motexempel. Argumentet är därör inte giltigt.

Svar: Argumentet är inte giltigt. Ett motexempel ges av $p = q = S$ och $r = F$. (Även $p = r = S$ och $q = F$ fungerar, liksom $q = r = S$ och $p = F$).

2. Vi gör ett induktionsbevis. För detta är det lämpligt att införa beteckningarna

$$\mathrm{VL}(n) = \sum_{k=1}^{n} F(k)^2 \qquad \text{och} \qquad \mathrm{HL}(n) = F(n)F(n+1).$$

Basfall: Eftersom $F(2) = F(1) + F(0) = 1 + 0 = 1$ och

$$\mathrm{VL}(1) = \sum_{k=1}^{1} F(k)^2 = F(1)^2 = 1$$
$$\mathrm{HL}(1) = F(1)F(2) = 1 \cdot 1 = 1$$

har vi ett giltigt basfall.

Induktionssteget: Antag att $\mathrm{VL}(p) = \mathrm{HL}(p)$ för något visst $p \in \mathbb{Z}_+$. Då är

$$\begin{aligned}\mathrm{VL}(p+1) &= \sum_{k=1}^{p+1} F(k)^2 = F(p+1)^2 + \sum_{k=1}^{p} F(k)^2 = F(p+1)^2 + \mathrm{VL}(p) = \\ &= F(p+1)^2 + \mathrm{HL}(p) = F(p+1)^2 + F(p)F(p+1) = \\ &= F(p+1)\underbrace{\big(F(p+1) + F(p)\big)}_{=F(p+2)} = F(p+1)F(p+2) = \mathrm{HL}(p+1),\end{aligned}$$

där de syrenfärgade delarna är lika enligt antagandet ovan. Det gäller alltså att $\mathrm{VL}(p) = \mathrm{HL}(p) \Rightarrow \mathrm{VL}(p+1) = \mathrm{HL}(p+1)$.

Med ett giltigt basfall och ett giltigt induktionssteg ger *induktionsprincipen* att

$$\sum_{k=1}^{n} F(k)^2 = F(n)F(n+1)$$

för alla $n \in \mathbb{Z}_+$.

3. (a) Eftersom nollan $0 = \pm\sqrt{0} \in S$ är identitet för addition för alla reella tal fungerar den även i S, dvs $x + 0 = x$ för alla $x \in S$.

Svar: Ja, 0 är identitet för addition i S.

(b) Antag att S är sluten under addition. Eftersom både $\sqrt{2} \in S$ och $\sqrt{3} \in S$ skall då även $\sqrt{2} + \sqrt{3} \in S$, dvs det finns ett naturligt tal n sådant att

$$\sqrt{2} + \sqrt{3} = \sqrt{n} \quad \Rightarrow \quad 2 + 2\sqrt{6} + 3 = n,$$

vilket uppenbart inte gäller om $n \in \mathbb{N}$. Vi har fått en motsägelse, och S är alltså *inte* sluten under addition.

Svar: Nej, S är inte sluten under addition.

(c) Vi såg tidigare att det finns en identitet för addition i S, vilket ju är ett krav för att det skall kunna finnas additiva inverser. Direkt ur definition av S ser vi att $x \in S \Leftrightarrow -x \in S$, och eftersom $x + (-x) = 0$ har alla element en additiv invers.

Svar: Ja, varje element $x \in S$ har en additiv invers $-x \in S$.

(d) Eftersom $1 = \sqrt{1} \in S$ uppfyller $1 \cdot x = x \cdot 1 = x$ för alla $x \in S$ är 1 identitet för multiplikation i S.

Svar: Ja, $1 \in S$ är identitet för multiplikation.

(e) Om $x, y \in S$ så finns det tal $m, n \in \mathbb{N}$ sådana att $x^2 = m$ och $y^2 = n$. Om nu $z = xy$ så är $z^2 = mn \in \mathbb{N}$, så att $z = \sqrt{mn} \in S$ eller $z = -\sqrt{mn} \in S$.

Svar: Ja, S är sluten under multiplikation.

4. Låt x vara antalet praliner som beställdes. Enligt texten i uppgiften skall då

$$\begin{cases} x \equiv 12 \mod 90 \\ x \equiv 47 \mod 83. \end{cases}$$

Eftersom 83 är ett primtal som inte delar 90 är $\operatorname{sgd}(90, 83) = 1$, så Kinesiska restsatsen garanterar att det finns lösningar till systemet.

Första kongruensen ger oss $x = 12 + 90s$ för något heltal s. Insatt i andra kongruensen ger detta

$$12 + 90s \equiv 47 \mod 83 \quad \Leftrightarrow \quad 90s \equiv 35 \mod 83 \quad \Leftrightarrow \quad 7s \equiv 7 \cdot 5 \mod 83.$$

Eftersom $\operatorname{sgd}(83, 7) = 1$ har 7 en multiplikativ invers modulo 83, och om vi multiplicerar med den på båda sidor får vi $s \equiv 5 \mod 83$, dvs $s = 5 + 83t$ för något heltal t. (Vi behöver inte ta reda på inversen till 7 i det här fallet, men det går att göra med Euklides algoritm, och den är 12.)

Vi har nu

$$x = 12 + 90s = 12 + 90(5 + 83t) = 12 + 450 + 90 \cdot 83t = 462 + 7470t.$$

Enda lösningen där $0 \leq x < 1000$ är då $t = 0$, dvs $x = 462$.

Svar: Det beställdes $x = 462$ praliner.

5. (a) Relationen $\mathcal{R}$ ger upphov till en partition av de naturliga talen, dvs unionen av de disjunkta delmängderna

$$\begin{aligned} A_0 &= \{0\} \\ A_1 &= \{x : 1^2 \leq x < 2^2\} \\ A_2 &= \{x : 2^2 \leq x < 3^2\} \\ A_3 &= \{x : 3^2 \leq x < 4^2\} \\ &\vdots \end{aligned}$$

ger mängden av alla naturliga tal.

För alla $x \in A_k$ gäller att $Q(x) = k$, dvs alla tal i A_k är relaterade med varandra men inte med något tal i någon av de andra mängderna. Relationen är alltså en ekvivalensrelation.

(b) Lite experimenterande ger till exempel att $1\mathcal{R}2$ (och såklart även $2\mathcal{R}1$) eftersom $Q(1) = 1 = Q(2)$, men det gäller förstås *inte* att $1 = 2$. Relationen är alltså inte antisymmetrisk.

Svar: Nej, relationen $\mathcal{R}$ är inte antisymmetrisk.

(c) Eftersom $Q(40) = 6$ är $[40] = \underbrace{\{x : 6^2 \leq x < 7^2\}}_{= A_6 \text{ från (a)}}$. Primtalen i den ekvivalensklassen är 37, 41, 43, och 47.

Svar: Primtalen i ekvivalensklassen är 37, 41, 43, och 47.

6. (a) Det finns tre st A, och dessa kan placeras på $\binom{5}{3} = 10$ sätt i ordet, och det återstår att sätta in två andra bokstäver. Om de två bokstäverna är lika måste de vara R, N, eller G, dvs tre möjligheter. Om de två bokstäverna är olika skall vi välja ut två av fem (R, N, G, E, och M) med hänsyn till ordning, vilket kan ske på 20 olika sätt. Sammantaget finns det alltså $\binom{5}{3}(3 + 20) = 230$ "ord" som uppfyller kravet.

Svar: Det finns 230 "ord" som uppfyller kravet.

(b) Eftersom vi skall välja fyra olika bokstäver måste vi använda precis en dubblett och tre andra bokstäver. Dubbletten måste väljas som A, R, N, eller G, dvs det finns fyra möjligheter. När vi har valt dubbletten finns det fem olika bokstäver kvar, och vi kan välja tre av dem på $\binom{5}{3} = 10$ sätt. Sammanlagt finns det alltså $4 \cdot 10 \cdot \frac{5!}{2!} = 2400$ olika "ord" enligt specifikationerna (2! i nämnaren på grund av dubbletten).

Svar: Det finns 900 "ord" som uppfyller kraven.

(c) Vi kan sätta ihop RE till en ny symbol $\mathcal{R}$, och välja ut ytterligare tre bokstäver bland dem som är kvar. Följande fall finns för att välja ut bokstäverna:

- Vi väljer tre st A, och bildar sedan $\frac{4!}{3!} = 4$ "ord".
- Vi väljer en dubblett (A, N, eller G) och ytterligare en bokstav (bland fyra möjliga). Det blir då $3 \cdot 4 \cdot \frac{4!}{2!} = 144$ "ord".
- Vi väljer tre olika bokstäver, vilket sker på $\binom{5}{3} = 10$ sätt. Detta fallet ger oss $10 \cdot 4! = 240$ "ord".

Sammanlagt blir det $4 + 144 + 240 = 388$ "ord".

Svar: Det kan bildas 388 "ord" med RE i.

7. (a) Enligt känd sats finns en Eulercykel i en sammanhängande gram om och endast om alla noder har ett jämnt gradtal. I grafen finns fyra noder med udda gradtal, och vi kan inte ge alla noder ett jämnt gradtal genom att dra en enda ny kant.

Svar: Nej, det går inte.

(b) Enligt definitionen är ett träd en sammanhängande graf utan cykler. Grafen är sammanhängande och har två cykler, och genom att bryta upp cyklerna genom att ta bort en kant från vardera cykel får vi ett träd med sju noder. Detta går att göra på $3 \cdot 3 = 9$ sätt.

Svar: Nio delgrafer till H är träd med sju noder.

(c) I en bipartit graf kan det inte finnas cykler av udda längd, vilket det gör i H. Vi behöver alltså ta bort minst en kant i vardera cykel, och oavsett hur vi gör det kommer vi att få en bipartit graf. Vi behöver alltså inte lägga till några kanter, utan det räcker att ta bort två.

Svar: Två kanter är det minsta antalet som behöver plockas bort (och inga behöver läggas till).

8. (a) Vi noterar att $\Phi(x)$ är ett jämnt tal för alla $x \in \mathbb{Z}_+$ förutom $x = 1$ och $x = 2$. Det beror på att om p^k (där $p \geq 2$ är ett primtal och $k \geq 1$) är en faktor i x så är $\Phi(p^k) = p^{k-1}(p-1)$ en faktor i $\Phi(x)$. Om $\text{sgd}(m,n) = 1$ måste alltså ett av talen, säg m, vara antingen $m = 1$ eller $m = 2$. Då blir $\text{sgd}(m,n) \leq 2$, dvs $\text{sgd}(m,n) = 1$ eller $\text{sgd}(m,n) = 2$.

(b) Primtalsfaktorisering ger $352 = 2^5 \cdot 11$, så

$$\Phi(352) = \Phi(2^5)\Phi(11) = 2^4(2-1)(11-1) = 16 \cdot 10 = 160.$$

Svar: $\Phi(352) = 160$.

(c) Eftersom $\text{sgd}(352, 7) = 1$ garanterar Eulers sats att $7^{\Phi(352)} \equiv 1 \mod 352$. Enligt divisionsalgoritmen är $7042 = 44 \cdot 160 + 2$, så

$$7^{7042} \equiv 7^{44 \cdot 160 + 2} \equiv (7^{\Phi(352)})^{44} \cdot 7^2 \equiv 1^{44} \cdot 49 \equiv 49 \mod 352.$$

Svar: Det sökta talet är $x = 49$.