KTH Matematik
B.Ek

Lösningar tentan SF1610(/5B1118) DISKRET MATEMATIK, CL (m.fl.), 20 augusti 2008

Tryckfel kan förekomma.

1) Vi visar med induktion att $F_1 + F_3 + F_5 + \ldots + F_{2n+1} = F_{2n+2}$ för $n = 0, 1, 2, \ldots$, där fibonaccitalen $\{F_n\}_{n=0}^{\infty}$ ges av $F_0 = 0,\ F_1 = 1$ och $F_{n+2} = F_{n+1} + F_n,$ för $n = 0, 1, 2, \ldots$
Bas: $VL_0 = F_1 = 1,\ HL_0 = F_2 = F_1 + F_0 = 1 + 0 = 1$, så **påståendet är sant för $n = 0$.**
Steg: Antag att påståendet är sant för $n = k$, något $k = 0, 1, 2, \ldots$
Då fås $VL_{k+1} = F_1 + F_3 + \ldots + F_{2k+1} + F_{2k+3} = VL_k + F_{2k+3} \overset{\text{ind.ant.}}{=} HL_k + F_{2k+3} = F_{2k+2} + F_{2k+3} = F_{2k+4} = F_{2(k+1)+2} = HL_{k+1}$,
så **om påståendet är sant för $n = k$ är det sant för $n = k + 1$.**
Enligt induktionsprincipen är det sant för alla $n = 0, 1, 2, \ldots$ **Saken är klar.**

2) Antalet injektioner $f : \{a, b, c, d\} \to \{1, 2, 3, 4, 5, 6, 7\}$ som antar minst ett jämnt värde är det totala antalet injektioner minus antalet injektioner som bara tar udda värden, dvs $7 \cdot 6 \cdot 5 \cdot 4 - 4 \cdot 3 \cdot 2 \cdot 1 = 840 - 24 = 816$ (känt uttryck för antalet injektioner eller multiplikationsprincipen).
Svar: Det sökta antalet funktioner är 816.

3) För att finna alla lösningar i $\mathbb{Z}_{14}$ till ekvationen $x^2 = x + 6$ beräknar vi båda leden för alla element i $\mathbb{Z}_{14}$ och jämför:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
x^2	0	1	4	9	2	11	8	7	8	11	2	9	4	1
$x+6$	6	7	8	9	10	11	12	13	0	1	2	3	4	5

Den givna andragradsekvationen har tydligen fyra lösningar. Tabellen ger:
Svar: Ekvationens samtliga lösningar är $x = 3,\ 5,\ 10$ och 12.

4) $f(x, y, z, w) = xzw + \bar{x}yz + \bar{x}y\bar{z}\bar{w} + \bar{x}\bar{y}zw + y\bar{z}w$
ger karnaughdiagrammet härintill.
Genom att, som i fig., täcka 1:orna med så stora rektanglar som möjligt med sidlängder 1, 2 eller 4, får vi att $f(x, y, z, w)$ är ekvivalent med $\bar{x}y + yw + zw$.
Det är den sökta minimala disjunktiva formen.
Svar: Uttrycket blir $f(x, y, z, w) = \bar{x}y + yw + zw$.

xy \ zw	00	01	11	10
00	0	0	1	0
01	1	1	1	1
11	0	1	1	0
10	0	0	1	0

5) Om grafens ena komponent (den fullständiga) har x hörn, har den $\frac{1}{2}x(x-1)$ kanter (2·(antalet kanter)=summan av valenserna). Den andra komponenten har då $10 - x$ hörn (totalt var det 10 hörn) och $10 - x - 1 = 9 - x$ kanter (eftersom det var ett träd). Totala antalet kanter (som var 18) blir $\frac{1}{2}x(x-1) + 9 - x = 18$, så $x^2 - 3x - 18 = 0$, med lösningar $x = 6, -3$. Antalet hörn i en komponent är positivt, så
Svar: Den fullständiga komponenten har 6 hörn och den andra har 4 hörn.

6) Vi söker heltalslösningar till $(i)\ 111x + 84y = 15$ och $(ii)\ 84x + 111y = 16$.
Euklides algoritm ger $111 = 1 \cdot 84 + 27$, $84 = 3 \cdot 27 + 3$, $27 = 9 \cdot 3 + 0$ så **$\mathbf{sgd(111, 84) = 3}$** och $3 = 84 - 3 \cdot 27 = 84 - 3(111 - 84) = -3 \cdot 111 + 4 \cdot 84$.
För x och y heltal delar 3 talet $84x + 111y$ men inte 16, så **(ii) saknar heltalslösningar**.
$111 \cdot (-3) + 84 \cdot 4 = 3$, så $111 \cdot (-15) + 84 \cdot 20 = 15$ och $\begin{cases} x_0 = -15 \\ y_0 = 20 \end{cases}$ är en lösning till (i).
(x, y) uppfyller då (i) precis om $111(x - x_0) + 84(y - y_0) = 0$, dvs $37(x - x_0) = 28(y_0 - y)$, så (entydig faktorisering) $x - x_0 = 28k$, godtyckligt $k \in \mathbb{Z}$ och därur $y = y_0 - 37k$.
Svar: (i) har lösningarna $\begin{cases} x = -15 + 28k \\ y = 20 - 37k \end{cases}$, $k \in \mathbb{Z}$. (ii) saknar heltalslösningar.

7) Grafen G är sammanhängande och har $e = 107$ kanter och $v = 66$ hörn. Vi vet också att ingen cykel i G har längd < 5.
Antag att grafen kan ritas plan. Då har var och en av de r ytorna (fasetterna) minst 5 kanter, så summan av antalet kanter i ytorna är $\geq 5r$, men den är också $= 2e$ (varje kant räknas två gånger). Vi har alltså $2e \geq 5r$, så $r \leq \frac{2}{5}e$ och enligt Eulers formel för sammanhängande plana grafer $2 = v - e + r \leq v - \frac{3}{5}e$, så $e \leq \frac{5}{3}(v-2) = \frac{5}{3}(66-2) = 106\frac{2}{3}$. Men $e = 107$, motsägelse, så **Svar: Nej grafen kan inte vara planär.**

($v = 66$, $e = 106$ är däremot möjligt i en planär graf (t.ex. 4 dodekaedrar hopklistrade i rad längs sidoytor + ett extra hörn med en kant).)

8) Vi söker det minsta $n \in \mathbb{N}$ så att för alla $x, y \in \mathbb{Z}$ gäller $y \equiv x^{107} \pmod{1271} \Rightarrow$
$y^n \equiv x \pmod{1271}$, dvs $x^{107n} \equiv x \pmod{1271}$ för alla $x \in \mathbb{Z}$.
(Så det handlar om ett RSA-system med n' (vanligen kallat n) $= 1271 = 31 \cdot 41, e = 107, m = (31-1)(41-1) = 1200$. Vårt sökta n är det som brukar kallas d.)
Enligt RSA räcker $107\,n \equiv 1 \pmod{1200}$. Det ger med Euklides algoritm etc att $\boldsymbol{n = 1043}$ **duger** (för 3p), men mindre n finns.
Kravet på n är ju precis att $x^{107n} \equiv x \pmod{31}$ **och** 41) (ty sgd$(31, 41) = 1$), dvs $107n \equiv 1 \pmod{30}$ **och** 40) (ty 31 och 41 är primtal). (mod 30) ger med Euklides algoritm att $1 = -7 \cdot 107 + 25 \cdot 30 = (30k-7)107 + (25-107k)30$, så (som i 6) ovan) $n = 30k - 7$ för något $k \in \mathbb{Z}$.
Möjliga k ges av villkoret $107n \equiv 1 \pmod{40}$, dvs $30 \cdot 107k = 3210k \equiv 10k \equiv 1 + 7 \cdot 107 = 750 \equiv 30 \pmod{40}$, så $k \equiv 3 \pmod 4$ och $k = 3 + 4i$, $n = 90 + 120i - 7 = 83 + 120i$ för godtyckligt $i \in \mathbb{N}$.
Svar: Möjliga är $\boldsymbol{n = 83 + 120i}$, $\boldsymbol{i = 0, 1, 2, \ldots}$ Minsta möjliga är $\boldsymbol{n = 83}$.

9) Vi har $\pi(1)=7$, $\pi(2)=10$, $\pi(3)=9$, $\pi(4)=2$, $\pi(5)=5$, $\pi(6)=8$, $\pi(7)=1$,
$\pi(8)=6$, $\pi(9)=3$, $\pi(10)=4$.
a) På cykelform: $\pi = (1\,7)\,(2\,10\,4)\,(3\,9)\,(5)\,(6\,8)$, ty $\pi(1) = 7$, $\pi(7) = 1$ etc. Ordningen för en permutation (den lägsta positiva potensen av den som är identitetspermutationen) är minsta gemensamma multipeln av cyklernas längder, dvs $o(\pi) = \text{mgm}(2, 3, 2, 1, 2) = 6$.
Svar: $\boldsymbol{\pi}$ är på cykelform (1 7) (2 10 4) (3 9) (5) (6 8). Dess ordning är 6.
b) $\sigma\pi\sigma^{-1}$:s cykelform är $(\sigma(1)\,\sigma(7))\,(\sigma(2)\,\sigma(10)\,\sigma(4))\,(\sigma(3)\,\sigma(9))\,(\sigma(5))\,(\sigma(6)\,\sigma(8))$, ty σ^{-1} tar t.ex. $\sigma(1)$ till 1, som π tar till 7, som σ tar till $\sigma(7)$ osv.
Svar: $\boldsymbol{\sigma\pi\sigma^{-1}}$ är $\boldsymbol{(\sigma(1)\,\sigma(7))\,(\sigma(2)\,\sigma(10)\,\sigma(4))\,(\sigma(3)\,\sigma(9))\,(\sigma(5))\,(\sigma(6)\,\sigma(8))}$.
c) σ kommuterar med π precis om $\sigma\pi\sigma^{-1} = \pi$, dvs om cykelformerna i svaren ovan är lika.
Cykeln $(\sigma(2)\,\sigma(10)\,\sigma(4))$ måste då vara samma som $(2\,10\,4)$ och $\sigma(2)$ kan vara 2, 10 eller 4. $\sigma(10)$ och $\sigma(4)$ bestäms entydigt av valet av $\sigma(2)$. **3 möjligheter.**
Cykeln $(\sigma(1)\,\sigma(7))$ måste vara en av $(1\,7)$, $(3\,9)$ och $(6\,8)$, så $\sigma(1)$ kan vara 1, 7, 3, 9, 6 eller 8. $\sigma(7)$ bestäms entydigt av valet av $\sigma(1)$. **6 möjligheter.**
Cykeln $(\sigma(3)\,\sigma(9))$ måste då vara en av de två återstående 2-cyklerna, så $\sigma(3)$ kan ta ett av 4 värden. $\sigma(9)$ bestäms entydigt av valet av $\sigma(3)$. **4 möjligheter.**
Cykeln $(\sigma(6)\,\sigma(8))$ måste då vara den återstående 2-cykeln, så $\sigma(6)$ kan ta ett av 2 värden. $\sigma(8)$ bestäms entydigt av valet av $\sigma(6)$. **2 möjligheter.**
$\sigma(5)$ måste vara 5 (den enda 1-cykeln).
Multiplikationsprincipen ger det sökta antalet som $3 \cdot 6 \cdot 4 \cdot 2 = 144$.
Svar: 144 olika $\boldsymbol{\sigma \in S_{10}}$ kommuterar med det givna $\boldsymbol{\pi}$.

10) G är en ändlig grupp. H, K och L är delgrupper till G.
a) $H \cap K \neq \varnothing$, ty identiteten I tillhör båda. $x, y \in H \cap K \Rightarrow (x, y \in H$ och $x, y \in K) \Rightarrow (xy \in H$ och $xy \in K) \Rightarrow xy \in H \cap K$. Eftersom G, och därmed $H \cap K$, är ändlig, ger en känd sats att $H \cap K$ är en delgrupp till G. **Saken är klar.**
b) Med $G = (\mathbb{Z}_6, +)$ och $H = \{0, 2, 4\}$, $K = \{0, 3\}$ är H, K delgrupper till G, men inte $H \cup K = \{0, 2, 3, 4\}$, ty $2, 3 \in H \cup K$, men $2 + 3 = 5 \notin H \cup K$. **Saken är klar.**
c) Enligt a) är $H \cap K$ och L delgrupper till G, så enligt a) igen är $H \cap K \cap L$ också det. Den är alltså delgrupp till alla grupperna H, K, L, $H \cap K$, $H \cap L$, $K \cap L$. Enligt Lagranges sats är $H \cap K \cap L$:s ordning en delare till alla dessa gruppers ordningar.
Enligt satsen om inklusion och exklusion är $|H \cup K \cup L| = |H| + |K| + |L| - (|H \cap K| + |H \cap L| + |K \cap L|) + |H \cap K \cap L|$ och eftersom alla termer i HL är delbara med $|H \cap K \cap L|$, är också VL det. **Saken är klar.**