Matematik, KTH
B.Ek

Lösningar tentan TEN1 SF1631(/SF1630) DISKRET MATEMATIK, D3 m.fl., 31 maj 2013

Tryckfel kan förekomma.

1) (4p) $G = (V, E)$ är plan och sammanhängande. Dess valenser är: 5 st 3, 2 st 4, 1 st 5 och 1 st 6. Varje begränsad yta har precis 3 kanter. Vi söker antalet kanter kring den obegränsade ytan.

Lösning: $2|E| = \sum_{x\in V}\delta(x) = 5\cdot 3 + 2\cdot 4 + 5 + 6 = 34$, så $|E| = 17$. Antalet hörn $|V| = 5+2+1+1 = 9$. Eftersom G är plan och sammanhängande ger Eulers polyederformel att antalet ytor $r = 2 - |V| + |E| = 2 - 9 + 17 = 10$, så det finns 9 begränsade ytor. Om antalet kanter kring den obegränsade ytan är k får man $3\cdot 9 + k = 2\cdot 17$ (varje kant ingår i två ytor (eller två gånger i en)), så $k = 7$.

Svar: Den obegränsade ytan har 7 kanter.

---

2) (4p) Vi söker alla lösningar $x, y \in \mathbb{Z}$ till ekvationen $165x + 121y = 99$.

Lösning: Euklides algoritm ger $165 = 1\cdot 121 + 44$, $121 = 2\cdot 44 + 33$, $44 = 1\cdot 33 + 11$, $33 = 3\cdot 11 + 0$ så $\text{sgd}(165, 121) = 11$ och $11 = 44 - 33 = 44 - (121 - 2\cdot 44) = -121 + 3\cdot 44 = -121 + 3(165 - 121) = 3\cdot 165 - 4\cdot 121$.
Multiplikation med 9 ger $165\cdot 27 + 121\cdot(-36) = 99$, så $\begin{cases} x_0 = 27 \\ y_0 = -36 \end{cases}$ löser ekvationen.
(x, y) uppfyller då ekvationen precis om $165(x - 27) + 121(y + 36) = 0$, dvs (dividera med $\text{sgd}(165, 121) = 11$) $15(x - 27) = -11(y + 36)$, där $\text{sgd}(15, 11) = 1$. Så (entydig faktorisering) $x - 27 = 11q$, $y + 36 = -15q$, för något $q \in \mathbb{Z}$. Varje $q \in \mathbb{Z}$ ger också en lösning. $k = q + 2$ ger en lite enklare form.
Svar: Alla de sökta lösningarna är $\begin{cases} \boldsymbol{x = 5 + 11k} \\ \boldsymbol{y = -6 - 15k}, \end{cases}$ $\boldsymbol{k \in \mathbb{Z}}$ **godtyckligt.**

---

3) (4p) Vi söker antalet sätt att ordna en kortlek med klöver-, ruter- och hjärterkorten vardera i rätt inbördes ordning och inga spaderkort intill varandra.

Lösning: Ordningen mellan de 39 klöver-, ruter- och hjärterkorten bestäms entydigt av vilka av de 39 som har varje färg. Det finns alltså $\binom{39}{13,13,13} = \frac{39!}{13!\cdot 13!\cdot 13!}$ olika tillåtna ordningar. För varje sådan ordning kan spaderkorten placeras i de 40 platserna före, mellan och efter dem (högst ett på varje plats) på $(40)_{13} = \frac{40!}{(40-13)!}$ sätt (injektion 13-mängd→40-mängd). Multiplikationsprincipen ger totala antalet som produkten av dem.
Svar: Antalet ordningar är $\boldsymbol{\frac{39!\cdot 40!}{(13!)^3\cdot 27!}}$ **(=** $\boldsymbol{6330039278294248158284276259225600000}$**).**

---

4) (4p) H är en delgrupp till G. Vi skall visa att H är en delgrupp till K som är en delgrupp till G om $K = \{g \in G \mid gH = Hg\}$.

Lösning: Eftersom $hH = Hh = H$ för alla $h \in H$ är $H \subseteq K \subseteq G$ och det räcker att visa att K är en grupp. Enligt känd sats är det tillräckligt att visa att $a, b \in K \Rightarrow ab, a^{-1} \in K$. $aH = Ha$, $bH = Hb$ betyder att för varje $h \in H$ finns $h_1, h_2 \in H$ med $bh = h_1 b$, $ah_1 = h_2 a$, så $(ab)h = a(bh) = a(h_1 b) = (ah_1)b = (h_2 a)b = h_2(ab)$, så $abH \subseteq Hab$ och "p.s.s." visas $Hab \subseteq abH$, så $a, b \in K \Rightarrow ab \in K$. $ha = ah_3 \Leftrightarrow a^{-1}h = h_3 a^{-1}$, så $Ha = aH \Rightarrow a^{-1}H \subseteq Ha^{-1}$ och "p.s.s." $Ha^{-1} \subseteq a^{-1}H$, så $a \in K \Rightarrow a^{-1} \in K$. **Saken är klar.**

---

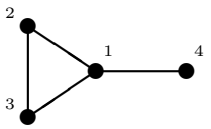
5) (4p) Vi söker alla lösningar till $x^2 = x$ i $\mathbb{Z}_{341}$ och i $\mathbb{Z}_{431}$.

Lösning: $x^2 = x \Leftrightarrow x(x-1) = 0$. Eftersom 431 är ett primtal är $\mathbb{Z}_{431}$ en kropp och de enda lösningarna där är $x = 0$ och $x = 1$ ($431 \mid x(x-1) \Leftrightarrow 431 \mid x$ eller $431 \mid (x-1)$).
$341 = 11 \cdot 31$, så $341 \mid x(x-1) \Leftrightarrow 11 \mid x(x-1)$ och $31 \mid x(x-1)$, dvs $x \equiv_{11} 0, 1$ och $x \equiv_{31} 0, 1$.
Om $x \equiv_{11} 0$ är $x = 11k$ för något $k \in \mathbb{Z}$ och $x \equiv_{31} 0$ ger $k \equiv_{31} 0$, så $x \equiv_{341} 0$, medan $x \equiv_{31} 1$ ger $11k \equiv_{31} 1 \Leftrightarrow 33k \equiv_{31} 3$ (ty $\text{sgd}(3, 31) = 1$) $\Leftrightarrow 2k \equiv_{31} 3 \Leftrightarrow 32k \equiv_{31} 48$ (ty $\text{sgd}(16, 31) = 1$) $\Leftrightarrow k \equiv_{31} 17$, så $x \equiv_{341} 11 \cdot 17 = 187$.
Om $x \equiv_{11} 1$ är $x = 11k + 1$ för något $k \in \mathbb{Z}$ och $x \equiv_{31} 1$ ger $k \equiv_{31} 0$, så $x \equiv_{341} 1$, medan $x \equiv_{31} 0$ ger $11k \equiv_{31} -1 \Leftrightarrow 33k \equiv_{31} -3$ (ty $\text{sgd}(3, 31) = 1$) $\Leftrightarrow 2k \equiv_{31} -3 \Leftrightarrow 32k \equiv_{31} -48$ (ty $\text{sgd}(16, 31) = 1$) $\Leftrightarrow k \equiv_{31} 14$, så $x \equiv_{341} 11 \cdot 14 + 1 = 155$.

Svar: Alla lösningar är $x = 0, 1, 155, 187$ i $\mathbb{Z}_{341}$ och $x = 0, 1$ i $\mathbb{Z}_{431}$.

---

6) $G = (V, E)$ är en enkel graf och A dess grannmatris. Vi söker A^2 och $\text{tr}\, A^3$ för (a, 2p) grafen härintill och (b, 3p) i allmänhet.



Lösning:
a) Man finner $A = \begin{pmatrix} 0&1&1&1 \\ 1&0&1&0 \\ 1&1&0&0 \\ 1&0&0&0 \end{pmatrix}$, $A^2 = \begin{pmatrix} 3&1&1&0 \\ 1&2&1&1 \\ 1&1&2&1 \\ 0&1&1&1 \end{pmatrix}$ och $A^3 = \begin{pmatrix} 2&4&4&3 \\ 4&2&3&1 \\ 4&3&2&1 \\ 3&1&1&0 \end{pmatrix}$, så $\text{tr}\, A^3 = 6$.
b) ij-elementet i A^2 är $\sum_{k \in V} a_{ik} a_{kj}$ = (additions- och multiplikationsprinciperna) om $i \neq j$: antalet vägar av längd 2 från i till j, om $i = j$: valensen för hörnet i. P.s.s. är ij-elementet i A^3 antalet sätt man kan komma från i till j i 3 steg (eventuellt med upprepade kanter), speciellt om $i = j$: dubbla antalet 3-cykler i ingår i (dubbla, ty man kan gå åt två håll). I $\text{tr}\, A^3$ räknas varje 3-cykel sex gånger, två för varje hörn i den. (Man ser f.ö. också att $\text{tr}\, A^2 = 2|E|$.)

Svar a: $A^2 = \begin{pmatrix} \mathbf{3}&\mathbf{1}&\mathbf{1}&\mathbf{0} \\ \mathbf{1}&\mathbf{2}&\mathbf{1}&\mathbf{1} \\ \mathbf{1}&\mathbf{1}&\mathbf{2}&\mathbf{1} \\ \mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1} \end{pmatrix}$, $\text{tr}\, A^3 = 6$, b: i A^2 är ii-elementet hörn i:s valens och ij-elementet ($i \neq j$) antalet vägar av längd 2 från i till j, $\text{tr}\, A^3$ är 6·(antalet 3-cykler i G).

---

7) (a, 2p) $\pi_1, \pi_2 \in S_9$ ges av $\pi_1 = \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 7&9&8&1&5&3&4&2&6 \end{smallmatrix}\right)$, $\pi_2 = \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&8&9&1&7&6&2&5&4 \end{smallmatrix}\right)$. Vi skall för $i = 1, 2$ avgöra om π_i är konjugerad med $(\pi_i)^2$.
(b, 3p) Vi söker ett nödvändigt och tillräckligt villkor på cyklernas längder i $\pi \in S_n$ för att π skall vara konjugerad med π^k ($n, k \in \mathbb{Z}_+$).

Lösning: $\pi, \sigma \in S_n$ är konjugerade omm för varje k, antalet k-cykler i π och σ är lika.
a) På cykelform är $\pi_1 = (1\,7\,4)(2\,9\,6\,3\,8)(5)$ och $\pi_2 = (1\,3\,9\,4)(2\,8\,5\,7)(6)$. Kvadrering ger $(\pi_1)^2 = (1\,4\,7)(2\,6\,8\,9\,3)(5)$ och $(\pi_2)^2 = (1\,9)(3\,4)(2\,5)(7\,8)(6)$. Tydligen är π_1 och $(\pi_1)^2$, men inte π_2 och $(\pi_2)^2$, konjugerade (lika respektive olika cykelstruktur).
b) Det sökta villkoret skall uttrycka att för varje cykel $\alpha = (a_1\, a_2\, \ldots\, a_m)$ i π gäller att α^k också är en cykel (olika cykler i π kan ju inte "blandas ihop" i π^k). Detta är uppfyllt omm $\text{sgd}(k, m) = 1$, vilket vi ser som följer. Om $d \mid m$ har α^d inga cykler längre än $\frac{m}{d}$ (ty $(\alpha^d)^{\frac{m}{d}} = \alpha^m = id$), så om också $d \mid k$ gäller detsamma för $\alpha^k = (\alpha^d)^{\frac{k}{d}}$. Om $1 = \text{sgd}(k, m) = ak + bm$ blir $\alpha = \alpha^{ak+bm} = (\alpha^k)^a (\alpha^m)^b = (\alpha^k)^a$, så α^k är en m-cykel.

Svar a: π_1 och $(\pi_1)^2$, men inte π_2 och $(\pi_2)^2$, är konjugerade,
b: π och π^k är konjugerade omm alla π:s cykellängder är relativt prima med k.

---

8) (4p) $m \in \mathbb{Z}_+$ och $(G, \cdot)$ är en abelsk grupp med $|G| = n \in \mathbb{Z}_+$.
Vi skall visa att $\phi(g) = g^m$ definierar en automorfi av G om $\text{sgd}(n, m) = 1$.

Lösning: ϕ är en automorfi precis om: 1. $\phi(gh) = \phi(g)\phi(h)$ för alla $g, h \in G$ (strukturen bevaras) och 2. $\phi : G \to G$ är en bijektion.
Eftersom G är abelsk är $\phi(gh) = (gh)^m = g^m h^m = \phi(g)\phi(h)$ (oberoende av $\text{sgd}(n, m)$).
G är ändlig, så för att visa att ϕ är en bijektion räcker det att visa att det är en injektion (att $\phi(g) \in G$ för alla $g \in G$ är ju klart). Antag alltså att $g, h \in G$ och $\phi(g) = \phi(h)$. Vi är klara om vi visar att $g = h$ (det visar ju injektiviteten). $g^m = h^m \Rightarrow (gh^{-1})^m = 1$ (där vi använt att G är abelsk), så $o(gh^{-1}) \mid m$. Men $gh^{-1} \in G$, så $o(gh^{-1}) \mid |G| = n$. Eftersom $\text{sgd}(n, m) = 1$ ger de att $o(gh^{-1}) = 1$, så $gh^{-1} = 1$ och $g = h$. Som sagt, det räcker. **Saken är klar.**
(I själva verket är $\text{sgd}(n, m) = 1$ nödvändigt och tillräckligt för isomorfi. Följer av att $p \mid |G|$, p primtal, ger att G har element av ordning p.)

---

9) (6p) $a, b, c \in \mathbb{Z}_+$ är parvis relativt prima. Vi visar att $(ab)^{\phi(c)} + (bc)^{\phi(a)} + (ca)^{\phi(b)} \equiv_{abc} 1$.

Lösning: Eftersom a, b, c är parvis relativt prima gäller för alla $n \in \mathbb{Z}$ att $abc \mid n$ omm ($a \mid n$, $b \mid n$ och $c \mid n$). Det räcker alltså att visa att a, b och c alla delar $(ab)^{\phi(c)} + (bc)^{\phi(a)} + (ca)^{\phi(b)} - 1$.
$a \mid (ab)^{\phi(c)}$, $(ca)^{\phi(b)}$, ty $\phi(c), \phi(b) \geq 1$. $\text{sgd}(a, bc) = 1$, så enligt Eulers sats (en av dem) gäller $a \mid ((bc)^{\phi(a)} - 1)$. Det följer att $a \mid ((ab)^{\phi(c)} + (bc)^{\phi(a)} + (ca)^{\phi(b)} - 1)$.
Att b, $c \mid ((ab)^{\phi(c)} + (bc)^{\phi(a)} + (ca)^{\phi(b)} - 1)$ visas p.s.s. **Saken är klar.**

---

10) Vi skall visa att (a, 3p) om $g(x), h(x) \in \mathbb{Z}[x]$ och alla koefficienter i $g(x)h(x)$ är delbara med primtalet p, är alla koefficienterna i minst en av $g(x)$ och $h(x)$ också det och (b, 3p) att om $f(x) \in \mathbb{Z}[x]$ är reducibel i $\mathbb{Q}[x]$ så är den reducibel i $\mathbb{Z}[x]$.

Lösning: a) Låt $g(x) = a_m x^m + \cdots + a_1 x + a_0$, $h(x) = b_n x^n + \cdots + b_1 x + b_0$ och antag att p varken delar alla a_i:na eller alla b_j:na. Om r är minst så att $p \nmid a_r$, men $p \mid a_i$ för alla $i < r$ och s är minst så att $p \nmid b_s$, men $p \mid b_j$ för alla $j < s$, gäller att p inte delar koefficienten för x^{r+s} i $g(x)h(x)$, $a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s} b_0$, ($p$ delar ju alla termer i summan utom $a_r b_s$). Det ger påståendet. **a)-saken är klar.**
b) Låt $f(x) \in \mathbb{Z}[x]$ och $f(x) = \varphi(x)\psi(x)$, där $\varphi(x), \psi(x) \in \mathbb{Q}[x]$. Om k är en gemensam multipel till alla nämnarna i $\varphi(x)$:s koefficienter gäller att $k\varphi(x) \in \mathbb{Z}[x]$. Vi kallar den $g(x)$ och p.s.s. låter vi $h(x) = l\psi(x) \in \mathbb{Z}[x]$. Då är $kl \cdot f(x) = g(x)h(x)$ en faktorisering i $\mathbb{Z}[x]$ och vi kan, enligt a), förkorta med en primfaktor i kl i taget, tills vi får en faktorisering av $f(x)$ i $\mathbb{Z}[x]$. Faktorerna i den har samma grader som $\varphi(x)$, $\psi(x)$, så om $f(x)$ är reducibel i $\mathbb{Q}[x]$ är den det också i $\mathbb{Z}[x]$. **b)-saken är också klar.**
