Matematik, KTH
B.Ek

Lösningar tentan SF1610(/5B1118) DISKRET MATEMATIK, CL m.fl., 30 maj 2011

Tryckfel kan förekomma.

1) (3p) Vi söker alla heltal x så att $12x + 13 \equiv 10 \pmod{51}$.

Lösning: $12x + 13 \equiv 10 \pmod{51} \Leftrightarrow 12x \equiv -3 \equiv 48 \pmod{51} \Leftrightarrow 4x \equiv 16 \pmod{17}$ (det sista eftersom $12x - 48 = 51k \Leftrightarrow 4x - 16 = 17k$). Eftersom $4 \cdot 13 = 52 \equiv 1 \pmod{17}$ (kan äv. fås med Euklides algoritm) och $\text{sgd}(13, 17) = 1$ är ekvationen $\Leftrightarrow 13 \cdot 4x \equiv x \equiv 13 \cdot 16 \equiv -13 \equiv 4 \pmod{17}$.
Svar: Alla sådana x är $x = 4 + 17k$, $k \in \mathbb{Z}$.

---

2) (3p) Bland 10 (särskiljbara) barn skall 23 små (identiska) bullar och två stora (särskiljbara) alla fördelas så att varje barn får minst en bulle.
På hur många sätt kan bullarna fördelas om Lisa får en stor bulle (men inte två)?

Lösning: Lisas stora bulle kan väljas på 2 sätt och barnet som får den andra stora på 9 sätt. Efter att övriga 8 barn fått varsin liten finns 15 små bullar kvar att fördela bland de 10 barnen. Det kan göras på $\binom{15+9}{9} = \frac{24!}{9!\,15!}$ sätt (9 väggar bland 15 + 9 väggbarn.) Multiplikationsprincipen ger svaret $2 \cdot 9 \cdot \frac{24!}{9!\,15!}$. **Svar: De kan fördelas på $\frac{2 \cdot 24!}{8!\,15!}$ (= 23535072) sätt.**

---

3) Permutationen $\pi \in S_9$ ges av $\pi(1) = 7$, $\pi(2) = 8$, $\pi(3) = 9$, $\pi(4) = 6$, $\pi(5) = 3$, $\pi(6) = 2$, $\pi(7) = 1$, $\pi(8) = 4$, $\pi(9) = 5$. Vi söker (a, 2p) π:s och π^2:s cykelformer och ordningar och (b, 1p) ett $\sigma \in S_{10}$ med maximal ordning, samt σ:s ordning.

Lösning: Eftersom $\pi(1) = 7$, $\pi(7) = 1$, $\pi(2) = 8$, $\pi(8) = 4$ etc fås $\pi = (1\,7)(2\,8\,4\,6)(3\,9\,5)$. Multiplikation ger $\pi^2 = (2\,4)(3\,5\,9)(6\,8)$. Deras ordningar ges av mgm av cykellängderna, så $o(\pi) = 12$, $o(\pi^2) = 6$. I b) söks maximum av $\text{mgm}(k_1, k_2, \dots)$ med $k_i \geq 1$, $k_1 + k_2 + \ldots = 10$. Prövning (t.ex. efter största cykellängd) ger att cykler av längd 2, 3, 5 ger maximal ordning, 30.
Svar: a) $\pi = (1\,7)(2\,8\,4\,6)(3\,9\,5)$, $\pi^2 = (2\,4)(3\,5\,9)(6\,8)$, $o(\pi) = 12$, $o(\pi^2) = 6$,
b) t.ex. $\sigma = (1\,2\,3\,4\,5)(6\,7\,8)(9\,10)$ ger maximal ordning 30.

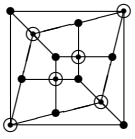
---

4) En linjär binär kod ges av kontrollmatrisen (checkmatrisen) $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$.
Vi söker dels (a, 1p) ett kodord som med högst ett fel kan bli 010110
och dels (b, 2p) ett ord som inte kan uppstå med högst ett fel i ett kodord.

Lösning: $H(010110)^T = (010)^T = H$:s kolonn 3, så bit 3 fel, det sökta ordet är 011110.
Ord av den sökta typen är precis sådana som inte kan rättas som i a), dvs $H(\dots)^T$ är inte en kolonn i H (dvs är $(011)^T$). Exempel är 100001, 010100, 001010, 110010, 111111.
Svar: a) Det sökta kodordet är 011110, b) ett sådant ord är 100001.

---

5) (3p) Vi skall avgöra om grafen i figuren har någon hamiltonstig.



Lösning: Grafen är enligt figuren bipartit. I en hamiltonstig kan antalet X-hörn och antalet Y-hörn skilja sig med högst 1 (de ligger vartannat), men i vår graf är skillnaden 2. **Svar: Grafen har ingen hamiltonstig.**

---

6) (4p) Vi skall avgöra (a, 1p) vilka primtal ≤ 5000 som inte är möjliga och (b, 3p) hur många olika värden som är möjliga för e, $1 < e \leq 5000$, i ett RSA-system med $n = 5917 = 61 \cdot 97$.

Lösning: $n = 61 \cdot 97$ ger $m = 60 \cdot 96 = 2^7 \cdot 3^2 \cdot 5$. Villkoret på e att $\text{sgd}(e, m) = 1$ ger att de omöjliga primtalen är 2, 3, 5. Möjliga e är precis de som inte är delbara med 2, 3 eller 5. Antalet fås med principen om inklusion och exklusion. Med $X = \{x \in \mathbb{N} \mid 1 < x \leq 5000\}$ och $A_i = \{x \in X \mid i \nmid x\}$ söks $|X \setminus (A_2 \cup A_3 \cup A_5)| = |X| - |A_2| - |A_3| - |A_5| + |A_6| + |A_{10}| + |A_{15}| - |A_{30}| = 4999 - 2500 - 1666 - 1000 + 833 + 500 + 333 - 166 = 1333$, där vi använt att $A_i \cap A_j = A_{\text{mgm}(i,j)}$ och att $|A_i|$ är heltalsdelen av $\frac{5000}{i}$ (om $i > 1$).
Svar: a) De omöjliga primtalen är 2, 3 och 5, b) antalet möjliga e är 1333.

---

7) Med Fibonacci-talen $\{F_n\}_{n=0}^{\infty}$ givna av $F_0=0,\ F_1=1,\ F_{n+2}=F_{n+1}+F_n$ för $n=0,1,2,\ldots$ skall vi visa $F_0F_1 + F_1F_2 + F_2F_3 + F_3F_4 + \cdots + F_{2n-1}F_{2n} = (F_{2n})^2$ för $n = 1, 2, 3, \ldots$

Lösning: Induktionsbevis över n.
Bas: $VL_1 = F_0F_1 + F_1F_2 = 0 \cdot 1 + 1 \cdot 1 = 1 = (F_2)^2 = HL_1$, så det stämmer för $n = 1$.
Steg: Antag (IA) att påståendet stämmer för $n = k$. Då fås $VL_{k+1} = F_0F_1 + F_1F_2 + \cdots + F_{2k-1}F_{2k} + F_{2k}F_{2k+1} + F_{2k+1}F_{2k+2} = VL_k + F_{2k}F_{2k+1} + F_{2k+1}F_{2k+2} \overset{\text{IA}}{=} HL_k + F_{2k}F_{2k+1} + F_{2k+1}F_{2k+2} = (F_{2k})^2 + F_{2k}F_{2k+1} + F_{2k+1}F_{2k+2} = F_{2k}(F_{2k} + F_{2k+1}) + F_{2k+1}F_{2k+2} = F_{2k}F_{2k+2} + F_{2k+1}F_{2k+2} = (F_{2k} + F_{2k+1})F_{2k+2} = (F_{2k+2})^2 = HL_{k+1}$, så om påståendet stämmer för $n = k$ gör det det också för $n = k + 1$, steget är klart.
Enligt induktionsprincipen är påståendet visat för $n = 1, 2, \ldots$ **Saken är klar.**

---

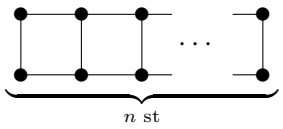
8) (4p) Vi skall visa att det finns ett heltal $n \geq 1$ så att 147^n (skrivet i bas 10) slutar på 0000000001, dvs så att $10^{10} \mid (147^n - 1)$.

Lösning: Betrakta $147^n \pmod{10^{10}}$ för $n = 2, 3, \ldots$ Eftersom bara 10^{10} olika värden är möjliga, finns enligt postfacksprincipen $r > s$ med $147^r \equiv 147^s \pmod{10^{10}}$, så $10^{10} \mid (147^r - 147^s) = 147^s(147^{r-s} - 1)$. Eftersom $\text{sgd}(147, 10) = 1$ ger det med $n = r - s(\geq 1)$ att $10^{10} \mid (147^n - 1)$. **Saken är klar.**

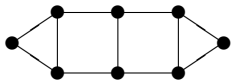
Alt. $\text{sgd}(147, 10^{10}) = 1$, så 147 är inverterbart i $\mathbb{Z}_{10^{10}}$, dvs ligger i den ändliga gruppen $G = U(\mathbb{Z}_{10^{10}})$ som har identitetselementet 1. Om n är 147:s ordning i G gäller $147^n = 1$ i G, dvs $147^n \equiv 1 \pmod{10^{10}}$.

---

9) G_n är den övre grafen och $P_n(\lambda)$ dess kromatiska polynom. Vi söker (a, 2p) $P_1(\lambda)$ och $P_2(\lambda)$, (b, 2p) $P_n(\lambda)$ för godtyckligt $n = 1, 2, \ldots$ och (c, 1p) antalet sätt att (hörn)färga den undre grafen med högst 4 färger.



Lösning: G_1 består av två hörn med en kant mellan dem. Det första hörnet kan färgas på λ sätt och sedan det andra på $\lambda - 1$ sätt, så $P_1(\lambda) = \lambda(\lambda - 1)$.



Rekursionsformeln för kromatiska polynom, $P_G(\lambda) = P_{G-e}(\lambda) - P_{G/e}(\lambda)$, med den högraste kanten som e, ger $P_{k+1}(\lambda) = P_k(\lambda)(\lambda - 1)^2 - P_k(\lambda)(\lambda - 2)$ (2 extra hörn med varsin granne ger faktorn $(\lambda - 1)^2$ och 1 hörn med 2 grannar med olika färg ger $(\lambda - 2)$), så $P_{k+1}(\lambda) = P_k(\lambda)(\lambda^2 - 3\lambda + 3)$. Med uttrycket för $P_1(\lambda)$ ger det $P_n(\lambda) = \lambda(\lambda - 1)(\lambda^2 - 3\lambda + 3)^{n-1}$.
Den undre grafen består av en G_3 med 2 extra hörn, vardera med 2 olikfärgade grannar, så dess kromatiska polynom är $P(\lambda) = P_3(\lambda)(\lambda - 2)^2$. Antalet sätt att färga grafen med högst 4 färger är alltså $P(4) = 4(4 - 1)(4^2 - 3 \cdot 4 + 3)^2(4 - 2)^2 = 4 \cdot 3 \cdot 7^2 \cdot 2^2 = 2352$.
Svar a): $P_1(\lambda) = \lambda(\lambda - 1)$, $P_2(\lambda) = \lambda(\lambda - 1)(\lambda^2 - 3\lambda + 3)$,
b): $P_n(\lambda) = \lambda(\lambda - 1)(\lambda^2 - 3\lambda + 3)^{n-1}$, c): Antalet sätt är 2352.

---

10) Gruppen G har ordning $|G| = 143 (= 11 \cdot 13)$. Vi skall (a, 1p) ange möjliga värden för elementens i G ordningar $o(g)$ och (b, 4p) visa (utan Cauchys sats) att det finns $g, h \in G$ med ordningar $o(g) = 11,\ o(h) = 13$.

Lösning: För alla $g \in G$ gäller $o(g) \mid |G|$, så $o(g)$ måste vara en av 1, 11, 13 och 143.
Svar: a): Möjliga $o(g)$ är 1, 11, 13, 143.
Antag att inget $g \in G$ har ordning 13.
Om något $a \in G$ har $o(a) = 143$ gäller $o(a^{11}) = 13$, så alla element måste ha ordning 11 eller 1 (bara enhetselementet). Varje element av ordning 11 genererar en delgrupp av ordning 11, dvs innehåller precis 10 element av ordning 11. De 10 genererar alla samma delgrupp (11 är primtal), så de 142 elementen av ordning 11 partitioneras i mängder med precis 10 element i varje (de som är potenser av varandra). Det går inte (ty $10 \nmid 142$), så antagandet att inget element hade ordning 13 ledde till motsägelse.
På samma sätt leder antagandet att inget element har ordning 11 till att de 142 elementen av ordning 13 skall partitioneras i mängder med precis 12 element i varje. Motsägelse (ty $12 \nmid 142$). **Saken i b) är klar.**
