**KTH Matematik**, B.Ek

**Lösningar extratentan SF1610(/5B1118) DISKRET MATEMATIK, CL m.fl., 29 maj 2010**

Tryckfel kan förekomma.

**1)** (3p) Finn alla heltal $x$ så att $35 \mid (22x-7)$, dvs $22x - 7 \equiv 0 \pmod{35}$.

---

**Lösning:** $35 \mid (22x-7)$ betyder precis $22x + 35k = 7$ för något $k$. Euklides algoritm:

$$\begin{cases} 35 = 1 \cdot 22 + 13, \\ 22 = 1 \cdot 13 + 9, \\ 13 = 1 \cdot 9 + 4, \\ 9 = 2 \cdot 4 + 1, \end{cases}$$

$1 = 9 - 2 \cdot 4 = 9 - 2(13-9) = -2 \cdot 13 + 3 \cdot 9 =$
$-2 \cdot 13 + 3(22-13) = 3 \cdot 22 - 5 \cdot 13 =$
$3 \cdot 22 - 5(35-22) = -5 \cdot 35 + 8 \cdot 22$
så $22 \cdot 56 - 35 \cdot 35 = 7$
$22(56-35) - 35(35-22) = 22 \cdot 21 - 35 \cdot 11 = 7.$

$x = 21$ är alltså en lösning och som vanligt ($\text{sgd}(22, 35) = 1$) fås den allmänna lösningen
**Svar: Alla lösningar ges av $x = 21 + 35n$, där $n \in \mathbb{Z}$.**

---

**2)** (3p) 24 barn, 12 flickor och 12 pojkar, skall ställa sig i två led med 12 barn i varje led. På hur många sätt kan det ske om leden inte får vara enkönade?
(Svaret får innehålla heltal, potenser, fakulteter och de fyra vanliga räknesätten.)

---

**Lösning:** Det finns lika många sätt att göra de två leden som att göra ett långt led, 24!. Från det skall dras antalet sätt skapa enkönade led, $2 \cdot (12!)^2$ (led 1 eller led 2 med bara flickor, varje led ordnas på 12! sätt)
**Svar: Leden kan bildas på $24! - 2 \cdot (12!)^2 (= 620447942848173834240000)$ sätt.**

---

**3)** (3p) En grupp $G$ har delgrupperna $H$ och $K$ med 24 respektive 35 element, dvs $|H| = 24$, $|K| = 35$. Finn alla möjliga värden för $|H \cap K|$, dvs hur många element som kan ligga i både $H$ och $K$.

---

**Lösning:** Om $g \in H$ gäller för $g$:s ordning $o(g) \mid |H| = 24$ och om $g \in K$ måste $o(g) \mid 35$. Om $g \in H \cap K$ gäller alltså $o(g) \mid \text{sgd}(24, 35) = 1$, dvs $g$ måste vara 1, identitetselementet. Alltid gäller $1 \in H \cap K$, så **Svar: Enda möjligheten är $|H \cap K| = 1$.**

---

**4)** (3p) Ett RSA-kryptosystem har $n = 221 (= 13 \cdot 17)$. Meddelandet 7 krypteras som 11 och meddelandet 8 som 60. Vad krypteras meddelandet 56 som? Glöm inte att motivera.

---

**Lösning:** Vi vet att $E(7) = 11$, dvs $7^e \equiv 11 \pmod{221}$ och p.s.s. $E(8) = 60 \equiv 8^e \pmod{221}$. Det ger $E(56) \equiv 56^e = 7^e 8^e \equiv 11 \cdot 60 = 660 \equiv 218 \pmod{221}$.
**Svar: 56 krypteras som 218.**

---

**5)** (3p) I en plan sammanhängande graf $G = (V, E)$ har precis hälften av hörnen valens (grad) 3 och hälften har valens 4. Grafen delar in planet i 47 ytor (fasetter) (inklusive den yttre, oändliga ytan). Hur många hörn och hur många kanter har $G$?

---

**Lösning:** Om en plan sammanhängande graf har $v$ hörn, $e$ kanter och $r$ ytor gäller $v - e + r = 2$. Med $v = 2a$ fås $3a + 4a = \sum_{x \in V} \delta(x) = 2e$. $r = 47$ ger $2a - \frac{7}{2}a + 47 = 2$, så $a = 30$ och $v = 60$, $e = \frac{7}{2}30 = 105$. **Svar: Grafen har 60 hörn och 105 kanter.**

---

**6)** (4p) Finn en kontrollmatris $H$ för en linjär binär kod $\mathcal{C}$ med $|\mathcal{C}| = 16$, $11011011 \in \mathcal{C}$, $00111000 \notin \mathcal{C}$, som rättar ett fel.

---

**Lösning:** Koden har tydligen längd 8 och dimension 4 ($16 = 2^4$), så $H$:s rang skall vara 4. Vi tar alltså $H$ som en $4 \times 8$-matris med alla kolonner olika och $\neq \mathbf{0}$.
$11011011 \in \mathcal{C}$ ger att summan av kolonnerna 1, 2, 4, 5, 7 och 8 är $= \mathbf{0} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, man kan t.ex. ta (summan av 1, 2 och 4)=(summan av 5, 7 och 8) $= \mathbf{0}$.
$00111000 \notin \mathcal{C}$ ger att (summan av kolonnerna 3, 4 och 5) $\neq \mathbf{0}$.
**Svar: Man kan t.ex. ta $H = \begin{bmatrix} 1&0&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0&0 \\ 0&0&1&0&1&0&0&1 \\ 0&0&0&0&0&1&1&1 \end{bmatrix}$.**

---

**7)** Låt som vanligt fibonaccitalen $F_n$, $n \in \mathbb{N}$, definieras av $F_0 = 0$, $F_1 = 1$ och $F_{n+2} = F_{n+1} + F_n$ för alla $n \in \mathbb{N}$.
**a)** (2p) Visa att $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^n = \left(\begin{smallmatrix}F_{n+1}&F_n\\F_n&F_{n-1}\end{smallmatrix}\right)$ för $n = 1, 2, 3, \ldots$
**b)** (2p) Visa att $F_n^2 + F_{n+1}^2 = F_{2n+1}$ för alla $n \in \mathbb{N}$.
(I b) får a) användas även om man inte gjort den.)

---

**Lösning:** a) Induktionsbevis. Bas: $\mathrm{VL}_1 = \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}F_2&F_1\\F_1&F_0\end{smallmatrix}\right) = \mathrm{HL}_1$, ok.
Steg: Antag att påståendet stämmer för $n = k$, dvs $\mathrm{VL}_k = \mathrm{HL}_k$. Då fås $\mathrm{VL}_{k+1} = \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^{k+1} = \mathrm{VL}_k \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) \overset{\text{IA}}{=} \mathrm{HL}_k \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}F_{k+1}&F_k\\F_k&F_{k-1}\end{smallmatrix}\right)\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}F_{k+1}+F_k&F_{k+1}\\F_k+F_{k-1}&F_k\end{smallmatrix}\right) = \left(\begin{smallmatrix}F_{k+2}&F_{k+1}\\F_{k+1}&F_k\end{smallmatrix}\right) = \mathrm{HL}_{k+1}$. Steget också ok, så induktionsprincipen ger att **saken är klar**.
b) Eftersom $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^{2n} = \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^n \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)^n$ ger a) att $\left(\begin{smallmatrix}F_{2n+1}&F_{2n}\\F_{2n}&F_{2n-1}\end{smallmatrix}\right) = \left(\begin{smallmatrix}F_{n+1}&F_n\\F_n&F_{n-1}\end{smallmatrix}\right)\left(\begin{smallmatrix}F_{n+1}&F_n\\F_n&F_{n-1}\end{smallmatrix}\right)$. 11-elementet är $F_{2n+1} = F_{n+1}^2 + F_n^2$, **saken är klar**.

---

**8)** Permutationen $\pi \in S_9$ ges av att $\pi(1) = 7$, $\pi(2) = 1$, $\pi(3) = 9$, $\pi(4) = 4$, $\pi(5) = 3$, $\pi(6) = 8$, $\pi(7) = 2$, $\pi(8) = 5$, $\pi(9) = 6$.
**a)** (1p) Uttryck $\pi$ i cykelnotation.
**b)** (3p) Finn $\pi$:s ordning $o(\pi)$ och ett $\sigma \in S_9$ så att $o(\sigma\pi) > o(\pi)$.

---

**Lösning:** a) Eftersom $\pi(1) = 7$, $\pi(7) = 2$, $\pi(2) = 1$ etc, fås $\pi = (1\,7\,2)(3\,9\,6\,8\,5)(4)$.
b) $o(\pi) = \mathrm{mgm}(3, 5, 1) = 15$. Om $\sigma\pi$ har cykelstrukturen 45 är $o(\sigma\pi) = \mathrm{mgm}(4, 5) = 20 > 15$. Valet $\sigma\pi = (1\,7\,2\,4)(3\,9\,6\,8\,5)$ ger $\sigma = \sigma\pi\pi^{-1} = (1\,7\,2\,4)(3\,9\,6\,8\,5)(1\,2\,7)(3\,5\,8\,6\,9) = (1\,4)$.
**Svar: a) $\pi = (1\,7\,2)(3\,9\,6\,8\,5)(4)$, b) $o(\pi) = 15$, t.ex. $\sigma = (1\,4)$.**

---

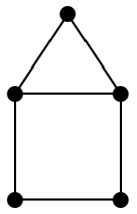
**9a)** (2p) Visa att för alla $r$, $s \in \mathbb{N}$ gäller $2^r - 1 \mid 2^{rs} - 1$.
**b)** (3p) Visa att om $m \in \mathbb{N}$ är udda gäller $m \mid 2^n - 1$ för något $n = 1, 2, \ldots, m$.

---

**Lösning:** a) $2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \ldots + 2^r + 1)$, **klart** (Alt. induktion över $s$).
b) Antag motsatsen, att division av $2^n - 1$ med $m$ ger rest $\neq 0$ för alla $n = 1, 2, 3, \ldots, m$. Då finns (postfacksprincipen) två lika rester, säg för $2^s - 1$ och $2^t - 1$, där $1 \leq s < t \leq m$, så $m \mid (2^t - 1) - (2^s - 1) = 2^t - 2^s = 2^s(2^{t-s} - 1)$, så ($m$ är udda) $m \mid 2^{t-s} - 1$. Men $1 \leq t - s < m$, så det motsäger antagandet. Så påståendet gäller, **saken är klar**.

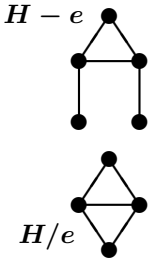
---

**10a)** (2p) Finn det kromatiska polynomet för vidstående graf. På hur många sätt kan grafen hörnfärgas med högst 5 färger?
**b)** (2p) Låt en graf $G$ ha det kromatiska polynomet $P_G(\lambda)$ och kromatiska talet $\chi(G) = 3$. På hur många sätt kan $G$ hörnfärgas med precis 5 färger (dvs så att alla färger används)?
**c)** (1p) Kontrollera resultatet i b) med grafen härintill.



---

**Lösning:** a) Kalla grafen $H$ och den understa kanten $e$. Rekursionsformeln ger $P_H(\lambda) = P_{H-e}(\lambda) - P_{H/e}(\lambda)$. Från figurerna fås $P_{H-e}(\lambda) = \lambda(\lambda-1)(\lambda-2)(\lambda-1)^2$ (sedan triangeln färgats kan de "hängande" hörnen vardera få $\lambda - 1$ olika färger) och $P_{H/e}(\lambda) = \lambda(\lambda-1)(\lambda-2)(\lambda-2)$. Så $P_H(\lambda) = \lambda(\lambda-1)(\lambda-2)((\lambda-1)^2 - (\lambda-2)) = \lambda(\lambda-1)(\lambda-2)(\lambda^2 - 3\lambda + 3)$.
Med högst 5 färger kan grafen färgas på $P_H(5) = 5 \cdot 4 \cdot 3 \cdot 13 = 780$ sätt.




b) Låt $X$ vara mängden av alla tillåtna färgningar av $G$ och $A_i$ vara mängden av färgningar där färgen "$i$" inte används. Vi söker $|X \setminus (A_1 \cup A_2 \cup \cdots \cup A_5)|$, som enligt principen om inklusion och exklusion är $|X| - (|A_1| + |A_2| + \cdots + |A_5|) + (|A_{12}| + |A_{13}| + \cdots + |A_{45}|)$ (där $A_{12}$ betecknar $A_1 \cap A_2$ och motsvarande). $\chi(G) = 3$ ger ju att $|A_1 \cap A_2 \cap A_3|$ etc. $= 0$. $|X|$ är antalet sätt att färga med högst 5 färger, dvs $P_G(5)$ och p.s.s. $|A_1| = \cdots = P_G(4)$ och $|A_{12}| = \cdots = P_G(3)$. Antalen av de olika termerna är 1, 5, $\binom{5}{2} = 10$, så det sökta antalet är $P_G(5) - 5P_G(4) + 10P_G(3)$.
c) Enligt a) är $P_H(5) = 780$, $P_H(4) = 168$, $P_H(3) = 18$, så enligt b) är antalet sätt att färga grafen med precis 5 färger $780 - 5 \cdot 168 + 10 \cdot 18 = 120$, vilket förstås **stämmer** (5 hörn färgas med 5 olika färger, totalt $5! = 120$ sätt).
**Svar: a) Polynomet: $\lambda(\lambda-1)(\lambda-2)(\lambda^2-3\lambda+3)$, 780 sätt.**
**b) På $P_G(5) - 5P_G(4) + 10P_G(3)$ sätt.**