Matematik, KTH
B.Ek

Lösningar tentan 19 augusti 2015
SF1662 DISKRET MATEMATIK, för CL, SIMTEK, E, m.fl.
Trynfel kan förekomma.

1) (3p) Vi söker $\text{sgd}(1794, 806)$ och $a, b \in \mathbb{Z}$ med $\text{sgd}(1794, 806) = 1794a + 806b$.

Lösning: Euklides algoritm:

$$\begin{cases} 1794 = 2 \cdot 806 + 182, \\ 806 = 4 \cdot 182 + 78, \\ 182 = 2 \cdot 78 + 26, \\ 78 = 3 \cdot 26, \end{cases} \quad \begin{matrix} \text{så} \\ \text{sgd}(1794, 806) = 26 \\ \text{och} \end{matrix} \quad \begin{cases} 26 = 182 - 2 \cdot 78 = 182 - 2(806 - 4 \cdot 182) = \\ = -2 \cdot 806 + 9 \cdot 182 = \\ = -2 \cdot 806 + 9(1794 - 2 \cdot 806) = \\ = 9 \cdot 1794 - 20 \cdot 806 \end{cases}$$

Svar: $\text{sgd}(1794, 806) = 26$ och ett par sådana tal är $a = 9$, $b = -20$.
(Alla lösningar ges av $a = 9 + 31k$, $b = -20 - 69k$, $k \in \mathbb{Z}$. ($69 = \frac{1794}{26}$, $31 = \frac{806}{26}$.))

---

2) (3p) $a_0 = 0$, $a_1 = 6$ och $a_{n+2} = a_{n+1} + 6a_n + 2^{n+2}$ för $n \in \mathbb{N}$.
Vi skall visa att $a_n = 2 \cdot 3^n - (1 + (-1)^n) \cdot 2^n$ för alla $n \in \mathbb{N}$.

Lösning: Vi låter P_n vara påståendet att den önskade likheten är sann för n och för $n + 1$ och visar med induktion P_n för alla $n \in \mathbb{N}$.
Bas: P_0 är sant, ty $a_0 = 0 = 2 \cdot 3^0 - (1 + (-1)^0) \cdot 2^0$ och $a_1 = 6 = 2 \cdot 3^1 - (1 + (-1)^1) \cdot 2^1$.
Steg: Antag (IA) P_r för ett godtyckligt $r \in \mathbb{N}$, dvs antag
$a_r = 2 \cdot 3^r - (1 + (-1)^r) \cdot 2^r$ och $a_{r+1} = 2 \cdot 3^{r+1} - (1 + (-1)^{r+1}) \cdot 2^{r+1}$.
Då "fås" dels $a_{r+1} = 2 \cdot 3^{r+1} - (1 + (-1)^{r+1}) \cdot 2^{r+1}$ (antogs ju) och dels (med rekursionsformeln)
$a_{r+2} = a_{r+1} + 6a_r + 2^{r+2} = 2 \cdot 3^{r+1} - (1 + (-1)^{r+1}) \cdot 2^{r+1} + 6 \cdot 2 \cdot 3^r - 6(1 + (-1)^r) \cdot 2^r + 2^{r+2} =$
$= (6 + 12)3^r - (2 + (-1)^{r+1} \cdot 2 + 6 + 6 \cdot (-1)^r - 4) \cdot 2^r = 18 \cdot 3^r - (4 + (-1)^r 4) \cdot 2^r =$
$= 2 \cdot 3^{r+2} - (1 + (-1)^{r+2}) \cdot 2^{r+2}$, så båda tillsammans ger P_{r+1}.
Så P_0 är sant och om P_r är sant är P_{r+1} sant. **Saken är klar (induktionsprincipen).**

---

3) (3p) 17 (särskiljbara) stolar skall besättas av (en del av) 12 flickor och 15 pojkar. Vi söker antalet sätt det går (särskiljbara personer), då alla flickor får sitta.

Lösning: Varje placering beskrivs fullständigt genom att först ange vilken stol varje flicka skall sitta på (det kan göras på $(17)_{12} = \frac{17!}{5!}$ sätt (injektion 12-mängd→17-mängd)) och sedan för varje återstående stol (5 st) välja en pojke för den (det kan p.s.s. göras på $(15)_5 = \frac{15!}{10!}$ sätt). Multiplikationsprincipen ger svaret $\frac{17!}{5!} \cdot \frac{15!}{10!} = \frac{17! \cdot 15!}{5! \cdot 10!}$.

Svar: Antalet sådana placeringar är $\frac{17! \cdot 15!}{5! \cdot 10!}$ (= 1 068 129 346 572 288 000).

---

4) Vi skall (a, 1p) finna alla element i U_{36} (de inverterbara elementen i $\mathbb{Z}_{36}$) och (b, 2p) finna ordningen för $5 \in U_{36}$.

Lösning: a. $x \in U_{36}$ omm $x \in \mathbb{Z}_{36}$ och $\text{sgd}(x, 36) = 1$, så
$U_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.
b. Ordningen för elementen i U_{36} är delare till 12 ($= |U_{36}|$), så möjliga värden är 1, 2, 3, 4, 6, 12. $5^1 = 5$, $5^2 = 25$, $5^3 = 125 = 17$, $5^4 = 5 \cdot 17 = 85 = 13$, $5^6 = 25 \cdot 13 = 325 = 9 \cdot 36 + 1 = 1$, så $o(5) = 6$.

Svar a: $U_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$, b: $o(5) = 6$.

---

5) (3p) Grafen $G = (V, E)$ är sammanhängande och ritad utan korsande kanter på en sfär. Den har 5 gånger så många hörn av valens 3 som av valens 5 och inga andra hörn finns. G har 10 hörn mer än dualgrafen $G^\perp$. Vi söker antalet kanter.

Lösning: Om antalet hörn med valens 5 är x är antalet med valens 3 $5x$ och $v = |V| = 6x$. Valensernas summa är $2e = \sum_{x \in V} \delta(x)$ ("handslagslemmat"), så $e = \frac{1}{2}(5x \cdot 3 + x \cdot 5) = 10x$. r, antalet ytor (fasetter), är lika med antalet hörn i $G^\perp$, så $r = v - 10 = 6x - 10$. Eulers polyederformel (G plan, sammanhängande) ger $v - e + r = 6x - 10x + (6x - 10) = 2$, så $x = 6$ och $e = 10 \cdot 6 = 60$. **Svar: Antalet kanter i G är 60.**

---

6) (4p) Vi söker $k \in \mathbb{N}$ sådant att $y \equiv x^{585} \pmod{667} \Rightarrow x \equiv y^k \pmod{667}$ för alla $x, y \in \mathbb{Z}$. $[667 = 23 \cdot 29]$.

Lösning: Vi känner igen ett RSA-system med $n = 667 = 23 \cdot 29$, $e = 585$ och söker d.
$n = 23 \cdot 29$ ger $m = 22 \cdot 28 = 616$, så d bestäms av att $e \cdot d \equiv_{616} 1$.
Vi använder Euklides algoritm.

$616 = 1 \cdot 585 + 31$
$585 = 18 \cdot 31 + 27$ så
$31 = 1 \cdot 27 + 4$
$27 = 6 \cdot 4 + 3$
$4 = 1 \cdot 3 + 1$

$1 = 4 - 3 = 4 - (27 - 6 \cdot 4) = -27 + 7 \cdot 4 =$
$= -27 + 7(31 - 27) = 7 \cdot 31 - 8 \cdot 27 =$
$= 7 \cdot 31 - 8(585 - 18 \cdot 31) = -8 \cdot 585 + 151 \cdot 31 =$
$= -8 \cdot 585 + 151 \cdot (616 - 585) = 151 \cdot 616 - 159 \cdot 585 =$
$= (151 - 585) \cdot 616 - (159 - 616) \cdot 585 = -434 \cdot 616 + 457 \cdot 585.$

Så $457 \cdot 585 \equiv_{667} 1$, dvs vi kan ta d, som i lydelsen kallades k, som 457.

Svar: Ett sådant k är 457.

---

7) $\pi \in S_9$ har $\pi(1)=3$, $\pi(2)=2$, $\pi(3)=4$, $\pi(4)=1$, $\pi(5)=8$, $\pi(6)=5$, $\pi(7)=9$, $\pi(8)=6$, $\pi(9) = 7$. Vi skall (a, 1p) skriva π i cykelnotation, (b, 2p) visa att $H = \{\tau \in S_9 \mid i \in \{1,2,3,4\} \Rightarrow \tau(i) \in \{1,2,3,4\}\}$ är en delgrupp till S_9 och (c, 1p) finna $(S_9 : H)$, H:s index i S_9.

Lösning: a. $\pi(1) = 3$, $\pi(3) = 4$, $\pi(4) = 1$, $\pi(2) = 2$, $\pi(5) = 8, \ldots$ ger att
$\pi = (1\,3\,4)(2)(5\,8\,6)(7\,9) = (1\,3\,4)(5\,8\,6)(7\,9)$.
b. Eftersom S_9 är en ändlig grupp är H en delgrupp om $H \neq \varnothing$ och $\sigma, \tau \in H \Rightarrow \sigma\tau \in H$ (känd sats). $id \in H$, så $H \neq \varnothing$ och om $\sigma, \tau \in H$, $i \in \{1, 2, \ldots, 4\}$ så $\tau(i) \in \{1, \ldots, 4\}$ så $(\sigma\tau)(i) = \sigma(\tau(i)) \in \{1, \ldots, 4\}$, så $\sigma\tau \in H$. **b-Saken är klar.**
c. Eftersom S_9 är en ändlig grupp är $(S_9 : H) = \frac{|S_9|}{|H|}$ (ty varje sidoklass har precis $|H|$ element). $|S_9| = 9!$ (antalet permutationer av en 9-mängd) och $|H| = 4! \cdot 5!$ (permutationer av en 4-mängd och en 5-mängd väljs oberoende), så $(S_9 : H) = \frac{9!}{4! \cdot 5!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4 \cdot 3 \cdot 2 \cdot 1} = 9 \cdot 7 \cdot 2 = 126 (= \binom{9}{4})$.
Svar a: $\pi = (1\,3\,4)(5\,8\,6)(7\,9)$, b: Visat ovan, c: $(S_9 : H) = 126$.

---

8) (4p) $X = \{1, 2, \ldots, 9, 10\}$. Vi söker antalet bijektioner $f : X \to X$ sådana att det finns $x, y \in X$ med x och $f(x)$ båda udda och $y \leq 4$ och $f(y) \geq 6$ (eventuellt $x = y$).

Lösning: Låt S_X vara mängden av alla bijektioner $X \to X$,
$A = \{f \in S_X \mid f(x)$ jämn för alla udda $x \in X\}$ och
$B = \{f \in S_X \mid f(y) \leq 5$ för alla $y \in X$ med $y \leq 4\}$.
Sökt är då $|S_X \setminus (A \cup B)|$, dvs (inklusion/exklusion, $A, B \subseteq S_X$) $|S_X| - |A| - |B| + |A \cap B|$.
$|S_X| = 10!$ (antalet permutationer av en 10-mängd), $|A| = 5! \cdot 5!$ (5! bijektioner udda→jämna, 5! jämna→udda),
$|B| = (5)_4 \cdot 6! = 5! \cdot 6!$ ($y = 1, \ldots, 4$ tar olika $f(y) \leq 5$, resten bijektion 6-mängd→6-mängd),
$|A \cap B| = 2! \cdot (3)_2 \cdot 3! \cdot 3! = 2 \cdot (3!)^3$ ($\{f(1), f(3)\} = \{2, 4\}$, $f(2), f(4) \in \{1, 3, 5\}$, olika, övriga udda och jämna tas var för sig bijektivt 3-mängd→3-mängd).
Det sökta antalet är alltså $10! - (5!)^2 - 5! \cdot 6! + 2 \cdot (3!)^3 = 10! - 7 \cdot (5!)^2 + 2 \cdot 6^3$.
Svar: Det finns $10! - 7 \cdot (5!)^2 + 2 \cdot 6^3 (= 3\,528\,432)$ olika sådana bijektioner.

---

9) (5p) $G_i = (V_i, E_i)$, $i = 1, 2$, är enkla grafer och vi skall visa att $\overline{G_1[G_2]} = \overline{G}_1[\overline{G}_2]$, där $G_1[G_2] = (V_1 \times V_2, E_L)$, $E_L = \{\{(u_1, u_2), (v_1, v_2)\} \mid \{u_1, v_1\} \in E_1 \vee (u_1 = v_1 \wedge \{u_2, v_2\} \in E_2)\}$. $\overline{G}$ betecknar komplementgrafen till G ($\overline{G} = (V, \overline{E})$ med $\overline{E} = \{\{u, v\} \mid u, v \in V,\ u \neq v,\ \{u, v\} \notin E\}$).

Lösning: $\overline{G_1[G_2]}$ och $\overline{G}_1[\overline{G}_2]$ har båda hörnmängden $V_1 \times V_2$, så det gäller att visa att deras respektive kantmängder E_{VL} och E_{HL} är lika.
Det finns precis nio olika fall för $e = \{(u_1, u_2), (v_1, v_2)\}$, svarande mot rutorna i tabellen:

	$u_2 = v_2$	$\{u_2, v_2\} \in E_2$	$\{u_2, v_2\} \in \overline{E}_2$
$u_1 = v_1$		$\circ$	$*$
$\{u_1, v_1\} \in E_1$	$\circ$	$\circ$	$\circ$
$\{u_1, v_1\} \in \overline{E}_1$	$*$	$*$	$*$

Enligt definitionen av $G_1[G_2]$ gäller $e \in E_L$ precis i fallen markerade med $\circ$. $\overline{G}_i$ i stället för G_i (dvs $\overline{E}_i$ i stället för E_i) ger att $e \in E_{\text{HL}}$ precis i fallen markerade med $*$.
Men $e \in E_{\text{VL}}$ precis om $(u_1, u_2) \neq (v_1, v_2)$ och $e \notin E_L$ (enligt definitionen av komplementgrafen), dvs precis i fallen med $*$. Således $e \in E_{\text{VL}} \Leftrightarrow e \in E_{\text{HL}}$, så $E_{\text{VL}} = E_{\text{HL}}$. **Saken är klar.**

---

10) Relationen $\mathcal{R}$ på S_7 definieras av att $\sigma_1 \mathcal{R} \sigma_2 \Leftrightarrow \pi\sigma_1 = \sigma_2\pi$ för något $\pi \in S_3$. Vi skall (a, 2p) visa att $\mathcal{R}$ är en ekvivalensrelation och (b, 3p) finna antalet $\mathcal{R}$-ekvivalensklasser.
(Element i S_3 identifieras med motsvarande permutationer i S_7.)

Lösning: a. $\mathcal{R}$ är en ekvivalensrelation omm den är reflexiv, symmetrisk och transitiv.
$\mathcal{R}$ är **reflexiv**, dvs $\sigma \mathcal{R} \sigma$ för alla $\sigma \in S_7$, ty $id\,\sigma = \sigma\, id$.
$\mathcal{R}$ är **symmetrisk**, dvs $\sigma_1 \mathcal{R} \sigma_2 \Rightarrow \sigma_2 \mathcal{R} \sigma_1$ för alla $\sigma_1, \sigma_2 \in S_7$, ty $\pi\sigma_1 = \sigma_2\pi \Rightarrow \pi^{-1}\sigma_2 = \sigma_1\pi^{-1}$.
$\mathcal{R}$ är **transitiv**, dvs ($\sigma_1 \mathcal{R} \sigma_2$ och $\sigma_2 \mathcal{R} \sigma_3$) $\Rightarrow \sigma_1 \mathcal{R} \sigma_3$ för alla $\sigma_1, \sigma_2, \sigma_3 \in S_7$,
ty ($\pi_1\sigma_1 = \sigma_2\pi_1$ och $\pi_2\sigma_2 = \sigma_3\pi_2$) $\Rightarrow \pi_2\pi_1\sigma_1 = \pi_2\sigma_2\pi_1 = \sigma_3\pi_2\pi_1$.
a-saken är klar. (Vi har använt att identitetspermutationen $id \in S_3$ och $\pi, \pi_1, \pi_2 \in S_3 \Rightarrow \pi^{-1}, \pi_2\pi_1 \in S_3$.)
b. Ekvivalensklasserna för $\mathcal{R}$ är banorna då S_3 verkar på S_7 med konjugering,
dvs $\pi(\sigma) = \pi\sigma\pi^{-1}$ för $\pi \in S_3$, $\sigma \in S_7$ (ty $\pi\sigma_1 = \sigma_2\pi \Leftrightarrow \sigma_2 = \pi\sigma_1\pi^{-1}$).
(Konjugeringen är en gruppverkan, ty $\pi_1(\pi_2(\sigma)) = (\pi_1\pi_2)\sigma(\pi_1\pi_2)^{-1} = (\pi_1\pi_2)(\sigma)$ och $id(\sigma) = \sigma$.)
Vi använder Burnsides lemma för att bestämma antalet banor.
För att få våra vanliga beteckningar låter vi $G = S_3$ och $X = S_7$.
Vi har $|G| = |S_3| = 3! = 6$ och behöver $|X_\pi|$, antalet $\sigma \in X$ med $\sigma = \pi\sigma\pi^{-1}$, för $\pi \in G$.
Om $\pi(i) = i$ (t.ex. om $i \in \{4, \ldots, 7\}$) och $\sigma \in X_\pi$ (så $\sigma\pi = \pi\sigma$) är $\pi(\sigma(i)) = \sigma(\pi(i)) = \sigma(i)$, så om en σ-cykel med i innehåller j är $\pi(j) = j$. Det hjälper när vi söker X_π:
Tabellen:

π:s typ	antal π	$\lvert X_\pi \rvert$	
id	1	$\lvert X \rvert = \lvert S_7 \rvert = 7!$	alla $\sigma \in X$ invarianta
[21]	3	$2 \cdot 5!$	$\pi = (i\,j)$ bevarar dels $(i\,j)\ldots$, dels $(i)(j)\ldots$ med $\ldots$ godtyckliga permutationer av en 5-mängd
[3]	2	$3 \cdot 4!$	$\pi = (i\,j\,k)$ bevarar $(1\,2\,3)\ldots$, $(1\,3\,2)\ldots$ och $(1)(2)(3)\ldots$ med $\ldots$ permutationer av en 4-mängd

Så det sökta antalet = antalet banor under G:s verkan =
$= \frac{1}{|G|} \sum_{\pi \in G} |X_\pi| = \frac{1}{6}(1 \cdot 7! + 3 \cdot 2 \cdot 5! + 2 \cdot 3 \cdot 4!) = \frac{4!}{6}(7 \cdot 6 \cdot 5 + 3 \cdot 2 \cdot 5 + 2 \cdot 3) = 4(210 + 30 + 6) =$
$= 4 \cdot 246 = 984.$

Svar: Antalet ekvivalensklasser för $\mathcal{R}$ är 984.
