

Lösningar tenta SF1679 DISKRET MATEMATIK, F3 m.fl.

12 januari 2017

Tryckfel kan förekomma.

1) Vi söker (a, 1p) det minsta (om något finns) $k \in \mathbb{Z}_+$ med $2^k \equiv_{1989} 1$ och (b, 2p) det största $k \in \mathbb{Z}_+$ som för något $x \in \mathbb{Z}$ är det minsta med $x^k \equiv_{1989} 1$ och ett motsvarande x .

Lösning:

Enligt kinesiska restsatsen är $x^k \equiv_{1989} 1$ omm $x^k = 1$ i $\mathbb{Z}_9, \mathbb{Z}_{13}$ och $\mathbb{Z}_{17}$.

a. Potenser av $[2]_9, [2]_{13}, [2]_{17}$:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	
2^k	2	4	8	7	5	1	...							$i \mathbb{Z}_9$
2^k	2	4	8	3	6	12	11	9	5	10	7	1	...	$i \mathbb{Z}_{13}$
2^k	2	4	8	16	15	13	9	1	...					$i \mathbb{Z}_{17}$

Det visar att $2^k \equiv_{1989} 1$ omm $k \mid 6, 12, 8$, dvs omm $k \mid \text{mgm}(6, 12, 8) = 24$.

Det minsta sådana $k \in \mathbb{Z}_+$ är alltså $k = 24$.

b. $x^k = 1$ i $\mathbb{Z}_{1989}$ omm $x \in U_{1989} \approx U_9 \times U_{13} \times U_{17}$ ($U_m = U(\mathbb{Z}_m)$, de inverterbara elementen i $\mathbb{Z}_m$) och $o_m(x) \mid k$ för $m = 9, 13, 17$ (o_m : multiplikativa ordningen i U_m). Det minsta sådana k är alltså $\text{mgm}(o_9(x), o_{13}(x), o_{17}(x))$.

Vi såg ovan att 2 har maximal ordning i $\mathbb{Z}_9$ och $\mathbb{Z}_{13}$ (nämligen $|U_9| = 6$ och $|U_{13}| = 12$), men $o_{17}(2) = 8 < |U_{17}| = 16$. Prövning ger att $o_{17}(3) = 16$.

Alltså är det sökta maximala $k = \text{mgm}(6, 12, 16) = 48$ och $x \equiv_9 2, \equiv_{13} 2, \equiv_{17} 3$ ger ett motsvarande x . De två första ger $x = 2 + 9 \cdot 13t$, $t \in \mathbb{Z}$. Även den sista uppfylls om $(m) 9 \cdot 13t \equiv_{17} 1$, så $t \equiv_{17} 2 \cdot 4 = 8$ (ty $9^{-1} = 2, 13^{-1} = 4$ i $\mathbb{Z}_{17}$) och $t = 8 + 17u$, $x = 2 + 9 \cdot 13 \cdot 8 + 9 \cdot 13 \cdot 17u = 938 + 1989u$, $u \in \mathbb{Z}$ godtyckligt.

Svar a: $k = 24$, b: $k = 48$, ett möjligt x är 938 (andra är 5, 7 och 10).

(Enklare: $o_{17}(3^n) = 16$ om $\text{sgd}(n, 16) = 1$. Om $x \equiv_{17} 3^n$ och $x \in U_9, U_{13}$ och dessutom $3 \mid o_9(x)$ eller $3 \mid o_{13}(x)$ är x "motsvarande". $n = 5$ ger $3^n \equiv_{17} 5$ och $o_9(5) = 6, o_{13}(5) = 4$ etc.)

2) (3p) En binär linjär kod $\mathcal{C}$ har $|\mathcal{C}| = 8$ och 101010, 111001, 110111 $\in \mathcal{C}$.

Vi söker en kontrollmatris H för $\mathcal{C}$ och skall avgöra om $\mathcal{C}$ rättar ett fel.

Lösning:

Längd 6 och $|\mathcal{C}| = 8 = 2^3$ ger att $\text{rank } H = 6 - 3 = 3$, så alla H med 3 linjärt oberoende rader som uppfyller Hc_i^T för $c_{1,2,3}$ de givna elementen i $\mathcal{C}$ är kontrollmatriser för $\mathcal{C}$.

H 's rader är alltså linjärt oberoende lösningar till det homogena systemet med koefficienter $\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1 \text{ t.}, 2, 3} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{2 \text{ t.}, 3} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \xrightarrow{3 \text{ t.}, 1} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$.

Genom att välja de sista bitarna som 100, 010, 001 fås raderna 101100, 011010, 010001, så $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$. Den har lika kolonner, så $\mathcal{C}$ rättar inte ett fel, ex. 000000, 100100 $\in \mathcal{C}$ ger båda 100000 med ett fel.

Svar: En möjlig kontrollmatris är $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$, $\mathcal{C}$ rättar inte (säkert) ett fel.

3) (3p) Vi söker antalet sätt att fördela 31 dagar mellan diskret matte, romaner och spel.

Det skall vara totalt 9 dagar spel, aldrig två i rad, och fler dagar diskret än romaner.

Lösning:

Antalet dagar utan spel är $31 - 9 = 22$. De kan fördelas mellan diskret och romaner på 2^{22} sätt, varav $\binom{22}{11}$ har lika många dagar av varje. Hälften av övriga, $\frac{1}{2}(2^{22} - \binom{22}{11})$ st, är de fördelningar som har fler dagar med diskret matte än romaner.

Av de 23 mellanrummen/ytterplatserna mellan dem kan 9 fyllas med speldagar på $\binom{23}{9}$ sätt.

Multiplikationsprincipen ger antalet fördelningar som uppfyller förutsättningarna,

$$\binom{23}{9} \cdot \frac{1}{2}(2^{22} - \binom{22}{11}) = \frac{23!}{9!14!} \cdot (2^{21} - \frac{22!}{2 \cdot (11!)^2}).$$

Svar: Didrik kan fördela dagarna på $\frac{23!}{9!14!} \cdot (2^{21} - \frac{22!}{2 \cdot (11!)^2}) (= 1\,425\,535\,654\,840)$ sätt.

4) $(G, \cdot)$ är en grupp och vi har ekvationerna $a = b^2$, $b = c^2$, $c = a^2$ för $a, b, c \in G$. Vi söker (a, 1p) alla lösningar med minst två av a, b, c lika och skall (b, 2p) visa att det om $|G| = 1467$ inte finns några lösningar med alla a, b, c olika.

Lösning:

a. Låt a, b, c uppfylla ekvationerna och $b = a$ ($c = b$ och $a = c$ analoga). Då är $a = b^2 = a^2$, så $a = 1$, G 's identitets-element (multiplicera med a^{-1}). Det ger också $b = a = 1$ och $c = a^2 = 1$.
b. Ekvationerna ger $a = b^2 = (c^2)^2 = c^4 = (a^2)^4 = a^8$ och således $a^7 = 1$. Det betyder att $o(a) \mid 7$, så $o(a) = 1$ eller 7. $o(a) = 1$ ger $a = 1$ och därmed $b = c = 1$ (så de är inte olika), medan $o(a) = 7$ är omöjligt eftersom $o(a) \mid |G|$ och $7 \nmid 1467$. **Saken är klar.**

Svar a: Enda möjligheten är $a = b = c = 1$, b: Visat ovan.

5) (3p) I en plan, sammanhängande graf har 2 hörn valens 3, de övriga valens 4. 4 ytor begränsas av 4 kanter, de övriga av 3 kanter. Vi söker antalen hörn, kanter och ytor i grafen.

Lösning:

Låt (som vanligt) v , e , r vara antalen hörn, kanter och ytor i grafen.

Eulers polyederformel ger $v - e + r = 2$. Summan av valenserna är $2e$, så $3 \cdot 2 + 4(v - 2) = 2e$. Motsvarande för den duala grafen ($v^\perp = r$, $r^\perp = v$) ger $4 \cdot 4 + 3(r - 4) = 2e$. Vi får systemet

$$\begin{cases} v - e + r = 2 \\ 2v - e = 1 \\ 2e - 3r = 4 \end{cases} \quad \text{med lösning} \quad \begin{cases} v = 9 \\ e = 17 \\ r = 10. \end{cases}$$

Svar: Grafen har 9 hörn, 17 kanter och 10 ytor.

6) $(G, *)$ är en grupp och $A \subseteq G$, $A \neq \emptyset$. Vi skall (a, 2p) visa att $|G_A| \leq |A|$ då $G_A = \{g \in G \mid a \in A \Rightarrow g * a \in A\}$, (b, 1p) visa att G_A är en delgrupp till G om A är ändlig och (c, 1p) ge exempel på G och A där G_A inte är en grupp.

Lösning:

a. följer av att $g \in G_A$ bestäms helt av sin verkan på ett enda $a \in A$:

Tag ett $a_0 \in A$ (finns, ty $A \neq \emptyset$). Om $g_1, g_2 \in G$ och $g_1 * a_0 = g_2 * a_0$ är $g_1 = g_2$ (ty $a_0 \in G$, multiplicera med a_0^{-1} från höger). Det betyder att $f_0: G_A \rightarrow A$ som ges av $f_0(g) = g * a_0$ är en injektion, så $|G_A| \leq |A|$ (postfacksprincipen; definitionen av $\leq$ om G_A inte är ändlig).

b. $a \in A \Rightarrow 1 * a \in A$, så $1 \in G_A$ och $G_A \neq \emptyset$.

$g_1, g_2 \in G_A \Rightarrow (a \in A \Rightarrow g_2 * a \in A \Rightarrow g_1 * (g_2 * a) = (g_1 * g_2) * a \in A) \Rightarrow g_1 * g_2 \in G_A$.

A ändlig ger G_A ändlig, så (känd sats) G_A är en delgrupp till G .

c. Med $(G, *) = (\mathbb{Z}, +)$ och $A = \mathbb{N}$ är $G_A = \mathbb{N}$, som inte är en grupp under addition.

Svar a,b: Visade ovan, c: $(G, *) = (\mathbb{Z}, +)$ och $A = \mathbb{N}$ utgör ett sådant exempel.

7) (4p) Vi skall för $m, n \in \mathbb{Z}_+$ visa att $\phi(d)\phi(mn) = d\phi(m)\phi(n)$, där $d = \text{sgd}(m, n)$ och ϕ är Eulers ϕ -funktion.

Lösning:

Låt, för $k \in \mathbb{Z}_+$, $P_k = \{p : p \text{ primtal}, p \mid k\}$. Då är $\phi(k) = k \cdot \prod_{p \in P_k} (1 - \frac{1}{p})$ (känd sats).

Så (för $m, n \in \mathbb{Z}_+$) $\phi(d)\phi(mn) = dmn \cdot \prod_{p \in P_d} (1 - \frac{1}{p}) \prod_{p \in P_{mn}} (1 - \frac{1}{p})$ och

$d\phi(m)\phi(n) = dmn \cdot \prod_{p \in P_m} (1 - \frac{1}{p}) \prod_{p \in P_n} (1 - \frac{1}{p})$.

Eftersom $P_{mn} = P_m \cup P_n$, $P_d = P_m \cap P_n$ är båda uttrycken dmn gånger faktorer $(1 - \frac{1}{p})^2$ för p i både P_m och P_n och faktorer $(1 - \frac{1}{p})$ för p i precis en av P_m och P_n , så de är lika.

Saken är klar.

$$8) \text{ (4p) } \sigma \in S_{13} \text{ ges av: } \frac{i}{\sigma(i)} \begin{array}{c|cccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ \hline 11 & 8 & 1 & 9 & 4 & 12 & 5 & 13 & 7 & 6 & 3 & 10 & 2 \end{array}.$$

Vi söker antalet $\pi \in S_{13}$ med $\pi\sigma = \sigma^{-1}\pi$.

Lösning:

På cykelform är $\sigma = (1 \ 11 \ 3)(2 \ 8 \ 13)(4 \ 9 \ 7 \ 5)(6 \ 12 \ 10)$ (ty $\sigma(1) = 11$, $\sigma(11) = 3$, $\sigma(3) = 1, \dots$).

$\pi\sigma = \sigma^{-1}\pi \Leftrightarrow \pi\sigma\pi^{-1} = \sigma^{-1}$. $\sigma^{-1} = (3 \ 11 \ 1)(13 \ 8 \ 2)(5 \ 7 \ 9 \ 4)(10 \ 12 \ 6)$ och

$\pi\sigma\pi^{-1} = (\pi(1) \ \pi(11) \ \pi(3))(\pi(2) \ \pi(8) \ \pi(13))(\pi(4) \ \pi(9) \ \pi(7) \ \pi(5))(\pi(6) \ \pi(12) \ \pi(10))$.

De är lika omm 3-cyklerna i den ena motsvarar 3-cyklerna i den andra och 4-cyklerna motsvarar varandra.

$\pi(1)$ kan vara vilket element som helst av de 9 i σ^{-1} :s 3-cykler, det bestämmer $\pi(11)$, $\pi(3)$,

$\pi(2)$ kan sedan väljas bland 6 element (2 st 3-cykler kvar), det bestämmer $\pi(8)$, $\pi(13)$,

$\pi(6)$ kan då väljas bland 3 element, det bestämmer $\pi(12)$, $\pi(10)$ och till sist kan

$\pi(4)$ väljas som vilket som helst i σ^{-1} :s 4-cykel, det bestämmer $\pi(9)$, $\pi(7)$, $\pi(5)$.

Totalt blir det (multiplikationsprincipen) $9 \cdot 6 \cdot 3 \cdot 4 = 648$ möjliga π .

Svar: Det finns 648 olika sådana π .

9) (5p) Om $G = (V_G, E_G)$ är en graf, $\mathcal{R}$ en ekvivalensrelation på V_G med ekvivalensklasser $\mathcal{V}_i$, $i \in I$, ges kvotgrafan $G/\mathcal{R} = (V_{G/\mathcal{R}}, E_{G/\mathcal{R}})$ av $V_{G/\mathcal{R}} = \{\mathcal{V}_i \mid i \in I\}$ och $E_{G/\mathcal{R}} = \{\{\mathcal{V}_i, \mathcal{V}_j\} \mid \text{det finns } v_i \in \mathcal{V}_i, v_j \in \mathcal{V}_j \text{ med } \{v_i, v_j\} \in E_G\}$.

Vi skall visa att om $H = (V_H, E_H)$ är en sammanhängande graf, så finns ett träd $T = (V_T, E_T)$ och en ekvivalensrelation $\mathcal{R}$ på V_T , sådana att $H \approx T/\mathcal{R}$ och $|E_H| = |E_T|$.

Lösning:

Induktion över $|V_H|$.

Bas: Om $|V_H| = 0$ eller 1 kan man ta $T = (V_H, \emptyset)$, $\mathcal{R}$ likhetsrelationen.

Steg: Antag att påståendet är sant för alla sammanhängande grafer med färre hörn än H .

Låt $|V_H| \geq 2$. Då finns $x \in V_H$ sådant att $H' = (V_{H'}, E_{H'})$, bildad genom att ta bort x och dess kanter från H , är sammanhängande (x kan vara ett löv i ett uppspännande träd för H). Enligt antagandet finns ett träd $T' = (V_{T'}, E_{T'})$ med $|E_{H'}| = |E_{T'}|$, en ekvivalensrelation $\mathcal{R}'$ på $V_{T'}$ och en isomorfi $\phi': V_{H'} \rightarrow V_{T'}/\mathcal{R}'$.

Låt x :s grannar i H vara $y_1, y_2, \dots, y_k$, $k = \delta(x)$. Vi bildar $T = (V_T, E_T)$ från T' genom att för varje y_i lägga till ett hörn x_i och en kant $\{y_i, x_i\}$. T är då ett träd (sammanhängande och utan cykler) och $|E_H| = |E_{H'}| + k = |E_{T'}| + k = |E_T|$. Låt $\mathcal{R}$ vara $\mathcal{R}'$ utökad med en ny ekvivalensklass $\mathcal{V}_x = \{x_i \mid i = 1, 2, \dots, k\}$. $\mathcal{R}$ är en ekvivalensrelation på V_T och $\phi = \phi' \cup \{(x, \mathcal{V}_x)\}$ är en isomorfi mellan H och $T/\mathcal{R}$ (om $u, v \in V_{H'}$: $\{u, v\} \in E_H \Leftrightarrow \{u, v\} \in E_{H'} \Leftrightarrow \{\phi'(u), \phi'(v)\} \in E_{T'}/\mathcal{R}' \Leftrightarrow \{\phi(u), \phi(v)\} \in E_{T/\mathcal{R}}$ och $\{u, x\} \in E_H \Leftrightarrow u = y_i$, för något $i \in \{1, \dots, k\} \Leftrightarrow \{\phi(u), \mathcal{V}_x\} \in E_{T/\mathcal{R}} \Leftrightarrow \{\phi(u), \phi(x)\} \in E_{T/\mathcal{R}}$). **Enligt induktionsprincipen är saken klar.**

10) (5p) Vi söker antalet väsentligt olika sätt att färga en kubs sidoytor med lika många röda som blå sidor, då man också har k andra färger att tillgå.

Lösning:

Vi använder Burnsidess lemma och behöver $|F(g)|$ för varje (typ av) symmetrirotation g .

typ av g	g :s permutation av kubens sidor	antal g	$ F(g) $
id	$[1^6]$	1	$k^6 + 30k^4 + 90k^2 + 20$
rot $hh \pm \frac{2\pi}{3}$	$[3^2]$	8	$k^2 + 2$
rot $kk \pi$	$[2^3]$	6	$k^3 + 6k$
rot $ss \pm \frac{\pi}{2}$	$[1^2 4]$	6	$k^3 + 2k$
rot $ss \pi$	$[1^2 2^2]$	3	$k^4 + 4k^2 + 4k + 4$

("rot $xx v$ ": rotation vinkeln v kring en axel genom kubens och sidors(s), kanter(k) eller hörns(h) medelpunkter.)

$|F(g)|$: antalet g -invarianta (dvs samma färg på alla sidor i samma cykel i g :s permutation) färgningar.

$|F(id)|$: ingen röd/blå, en var $((1, 1, 4) = 30)$, två var $((2, 2, 2) = 90)$ eller tre var $((3, 3, 0) = 20)$,

på övriga rader fördelas cyklerna på liknande sätt mellan röda, blå och övriga,

termen $4k$ på sista raden: 1-cyklerna kan vara röda och en 2-cykel blå eller tvärtom ($1+1=2$).

Lemmat ger antalet färgningar: $\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{24}((k^6 + 30k^4 + 90k^2 + 20) + 8 \cdot (k^2 + 2) + 6 \cdot (k^3 + 6k) + 6 \cdot (k^3 + 2k) + 3 \cdot (k^4 + 4k^2 + 4k + 4)) = \frac{1}{24}(k^6 + 33k^4 + 12k^3 + 110k^2 + 60k + 48)$.

Svar: Det sökta antalet är $\frac{1}{24}(k^6 + 33k^4 + 12k^3 + 110k^2 + 60k + 48)$.