

Lösningar tentan SF1662 DISKRET MATEMATIK, CL1,

21 augusti 2013

Tryckfel kan förekomma.

1) (3p) Vi söker alla heltal x, y så att $28x - 46y = 4$.**Lösning:** Division med 2 ger den ekvivalenta ekvationen $14x - 23y = 2$.

Euklides algoritim:

$$\begin{cases} 23 = 1 \cdot 14 + 9, \\ 14 = 1 \cdot 9 + 5, \\ 9 = 2 \cdot 5 - 1 \end{cases} \quad \text{så} \quad \begin{cases} 1 = -9 + 2 \cdot 5 = -9 + 2(14 - 9) = \\ = 2 \cdot 14 - 3 \cdot 9 = 2 \cdot 14 - 3(23 - 14) = \\ = -3 \cdot 23 + 5 \cdot 14 \end{cases}$$

 $14 \cdot 5 - 23 \cdot 3 = 1$ ger $14 \cdot 10 - 23 \cdot 6 = 2$ och $\begin{cases} x_0 = 10 \\ y_0 = 6 \end{cases}$ är en lösning.

 x, y är då en lösning om $14(x - x_0) = 23(y - y_0)$, dvs (eftersom $\text{sgd}(14, 23) = 1$, måste $23 \mid (x - x_0)$, så $x - x_0 = 23k$, $k \in \mathbb{Z}$, och alla $k \in \mathbb{Z}$ ger lösningar) $x - x_0 = 23k$, $y - y_0 = 14k$ för något $k \in \mathbb{Z}$.

Svar: Alla lösningar ges av $\begin{cases} x = 10 + 23k \\ y = 6 + 14k \end{cases}$, där $k \in \mathbb{Z}$.
2) (3p) Vi skall avgöra om dels 1. $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$, dels 2. $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ gäller för godtyckliga mängder A och B .
Lösning: Om $a \in A$, $a \notin B$ och $b \in B$, $b \notin A$ gäller $\{a, b\} \in \mathcal{P}(A \cup B)$ (ty $\{a, b\} \subseteq A \cup B$) och $\{a, b\} \notin \mathcal{P}(A)$, $\notin \mathcal{P}(B)$ (ty $\{a, b\} \not\subseteq A$, $\not\subseteq B$). 1. gäller alltså inte för A och B där det finns sådana a och b .

Eftersom $A \subseteq A \cup B$ gäller $C \subseteq A \Rightarrow C \subseteq A \cup B$, så $\mathcal{P}(A) \subseteq \mathcal{P}(A \cup B)$ och på samma sätt $\mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$, så $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$, dvs 2., gäller för godtyckliga A och B .

Svar: Relationen 2. gäller för godtyckliga mängder A och B . Det gör inte 1.

3) (3p) Vi söker antalet sätt 18 flickor och 22 pojkar kan paras ihop för dans, om Harry måste vara med och dansa, men inte kan dansa med Hermione.

Lösning: Harrys partner kan väljas på 17 sätt (vem som helst utom Hermione). Sedan kan de 17 återstående flickorna välja bland 21 pojkar på $(21)_{17} = \frac{21!}{4!}$ sätt. Multiplikationsprincipen ger totala antalet sätt som $17 \cdot \frac{21!}{4!}$.

Svar: Paren kan bildas på $\frac{17 \cdot 21!}{4!} (= 36\,189\,417\,371\,627\,520\,000)$ sätt.
4) G är gruppen $(U(\mathbb{Z}_{36}), \cdot)$ och H är den minsta delgruppen till G som innehåller 5. Vi skall (a, 1p) finna alla G :s element och (b, 2p) finna alla H :s element och sidoklasser.
Lösning: Eftersom $U(\mathbb{Z}_{36})$ består av alla $x \in \mathbb{Z}_{36}$ som uppfyller $\text{sgd}(x, 36) = 1$ och $36 = 2^2 \cdot 3^2$, är $G = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

 H består av alla potenser av 5 (de bildar en delgrupp och måste alla ingå i H). Man finner $5^2 = 25$, $5^3 = 5 \cdot 25 = 17$, ... och $H = \{5, 25, 17, 13, 29, 1\}$. $|G \setminus H| = 6 = |H|$, så H har bara en ytterligare (dvs utöver H själv) sidoklass, $G \setminus H = \{7, 11, 19, 23, 31, 35\}$.

Svar a: $G = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$,

b: $H = \{1, 5, 13, 17, 25, 29\}$ och dess sidoklasser är H och $\{7, 11, 19, 23, 31, 35\}$.

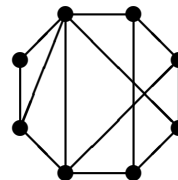
- 5) (3p) Vi skall avgöra om det finns någon enkel graf med åtta hörn med valenser
 i) 2, 3, 3, 3, 3, 4, 5, ii) 0, 1, 2, 3, 3, 5, 5, 6, iii) 1, 1, 3, 3, 5, 5, 5, 7.

Lösning:

i) Möjligt, se figuren till höger.

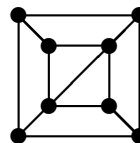
ii) Omöjligt, ty summan av valenserna i en graf är 2 gånger antalet kanter, ett jämnt tal, men summan av de givna talen är 25.

iii) Omöjligt, ty om hörnet med valens 7 och de två hörnen med valens 1 toges bort ur en sådan graf finge vi en med fem hörn och valenser 2,2,4,4,4. Det går inte, ty tre hörn med valens 4 ger att alla måste ha valens minst 3.



Svar: i) är möjlig, ii) och iii) är omöjliga.

- 6) (4p) Vi skall för grafen härintill avgöra om det finns en sluten kurva i planet som korsar varje kant precis en gång och inte går genom något hörn.



Lösning:

En sådan sluten kurva vore precis en eulerkrets i den duala grafen (dess kanter korsar ju varje kant i den givna grafen exakt en gång). En sådan finns precis om alla hörn i den duala grafen har jämn valens, dvs alla ytor i den givna har ett jämnt antal kanter, men det har ju inte de triangulära yterna "längst in".

Svar: Nej, någon sådan kurva finns inte.

- 7) Med $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$ skall vi (a, 1p) skriva α och $\alpha\beta$ på cykelform, (b, 1p) avgöra om dels α och dels $\alpha^6\beta\alpha^{-11}\beta^6$ är jämn eller udda och (c, 2p) finna ett $\pi \in S_5$ sådant att $\beta\pi, (\beta\pi)^2, \dots, (\beta\pi)^6$ alla är olika.

Lösning: Man finner $\alpha = (1\ 5)(2\ 3)(4) = (1\ 5)(2\ 3)$ (ty $\alpha(1) = 5, \alpha(5) = 1, \alpha(2) = 3$ etc.), $\alpha\beta$ betyder "först β , sedan α " och man finner $\alpha\beta = (1)(2\ 5\ 4\ 3) = (2\ 5\ 4\ 3)$ (ty $\beta(1) = 5, \alpha(5) = 1, \beta(2) = 1, \alpha(1) = 5$ etc.).

α är en jämn permutation, ty den innehåller ett jämnt antal (2 st) cykler av jämn längd, så det är α^{-1} också. $\beta = (1\ 5\ 4\ 2)(3)$ är udda (bara en cykel av jämn längd). Eftersom $\alpha^6\beta\alpha^{-11}\beta^6$ totalt innehåller ett udda antal β är den udda (α är ju jämn).

Alla $\beta\pi, (\beta\pi)^2, \dots, (\beta\pi)^6$ är olika omm ingen av $\beta\pi, (\beta\pi)^2, \dots, (\beta\pi)^5$ är identitetspermutationen ($\sigma = \tau$ omm $\sigma\tau^{-1} = id$), dvs omm $\beta\pi$:s ordning, $o(\beta\pi)$, är minst 6. En lösning (bland flera) får vi genom att välja $\beta\pi = (1\ 2)(3\ 4\ 5)$, som ju har ordning $\text{mgm}(2, 3) = 6$. Det ger $\pi = \beta^{-1}(\beta\pi) = (1\ 2\ 4\ 5)(1\ 2)(3\ 4\ 5) = (1\ 4)(3\ 5)$.

Svar a: $\alpha = (1\ 5)(2\ 3)$, $\alpha\beta = (2\ 5\ 4\ 3)$, **b:** α är jämn och $\alpha^6\beta\alpha^{-11}\beta^6$ är udda, **c:** t.ex. $\pi = (1\ 4)(3\ 5)$.

- 8) α är ett reellt tal sådant att $\alpha + \frac{1}{\alpha} \in \mathbb{Z}$. Vi skall visa att $\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$ för alla $n = 0, 1, 2, \dots$

Lösning: Vi låter $P(n)$ vara påståendet att både $\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$ och $\alpha^{n+1} + \frac{1}{\alpha^{n+1}} \in \mathbb{Z}$. Med induktion över n visar vi att $P(n)$ är sann för alla $n = 0, 1, 2, \dots$. Det räcker ju.

Bas: $P(0)$ är sann, ty $\alpha^0 + \frac{1}{\alpha^0} = 1 + \frac{1}{1} \in \mathbb{Z}$ och $\alpha^1 + \frac{1}{\alpha^1} \in \mathbb{Z}$ enligt förutsättning.

Steg: Antag att $P(k)$ är sann för ett $k = 0, 1, 2, \dots$.

Då gäller $\alpha^{k+1} + \frac{1}{\alpha^{k+1}} \in \mathbb{Z}$ (ingår i $P(k)$) och $\alpha^{k+2} + \frac{1}{\alpha^{k+2}} = (\alpha + \frac{1}{\alpha})(\alpha^{k+1} + \frac{1}{\alpha^{k+1}}) - (\alpha^k + \frac{1}{\alpha^k}) \in \mathbb{Z}$ (uttrycken i alla tre parenteserna är heltal p.g.a. $P(k)$ eller $P(0)$), så $P(k+1)$ är sann.

Vi har visat $P(0)$ och $P(k) \Rightarrow P(k+1)$ för $k = 0, 1, 2, \dots$

Induktionsprincipen ger att **saken är klar**.

(Kommentar: Vi har inte riktigt använt att $\alpha \in \mathbb{R}$. Med samma resonemang visas att om $\alpha \in \mathbb{C}$ är sådant att $\alpha + \frac{1}{\alpha} \in \mathbb{Z}[i]$ så gäller $\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}[i]$ för $n = 0, 1, 2, \dots$ (och därmed för alla $n \in \mathbb{Z}$).)

9) (5p) Vi söker det största n som gör att ett RSA-system kan ha $E(x) = x^9 \pmod{n}$ och $D(y) = y^{49} \pmod{n}$.

Lösning: Med vanliga RSA-beteckningar gäller $n = pq$, där p och q är olika primtal, och $(ed) = 9 \cdot 49 \equiv 1 \pmod{m}$, där $m = (p-1)(q-1)$.

Vi har alltså $9 \cdot 49 = 441 = k(p-1)(q-1) + 1$, för något heltal k .

p och q måste alltså vara primtal med $(p-1)(q-1) \mid 440 = 2^3 \cdot 5 \cdot 11$.

Tabellen ger i storleksordning alla primtal p med $(p-1) \mid 440$.

(Man finner dem genom att söka faktorer till 440 som är primtal -1 .)

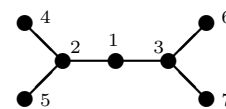
I den andra kolumnen visas motsvarande faktor till 440 och i den tredje det största pq för detta p sådant att $(p-1)(q-1) \mid 440$.

Det största möjliga värdet på $pq(=n)$ är $11 \cdot 23 = 253$.

Svar: Det största möjliga n -värdet är 253.

p	$p-1$	$\max pq$
2	1	$2 \cdot 89$
3	2	$3 \cdot 23$
5	2^2	$5 \cdot 23$
11	$2 \cdot 5$	$11 \cdot 23$
23	$2 \cdot 11$	$23 \cdot 11$
41	$2^3 \cdot 5$	$41 \cdot 2$
89	$2^3 \cdot 11$	$89 \cdot 2$

10) (5p) Vi söker antalet väsentligt olika (så att de inte blir lika hur man än vrider en del av eller hela anordningen i rummet) sätt att färga pärlorna med en röd och resten vita eller svarta.



Lösning:

Vi numrerar pärlorna som i figuren. Gruppen av "tillåtna" permutationer av pärlorna är då $G = \{(1), (45), (67), (45)(67), (23)(46)(57), (23)(47)(56), (23)(4657), (23)(4756)\}$, med $|G| = 8$.

Enligt Burnsidess lemma (se "Om gruppens verkan på mängder") är antalet väsentligt olika färgningar = antalet banor för gruppens verkan på färgningarna $= \frac{1}{|G|} \sum_{g \in G} |X_g|$.

Om $g \in G$ som permutation har cykelstrukturen $[1^{\alpha_1} 2^{\alpha_2} \dots]$, är $|X_g|$, antalet färgningar som är invarianta under g 's verkan, $= \alpha_1! \cdot 2^{\alpha_1 + \alpha_2 + \dots - 1}$ (alla pärlor i samma cykel måste ha samma färg, den röda pärlan kan vara vilken som av 1-cyklerna och övriga cykler kan var och en färgas vit eller svart). Eftersom vi har 1 element av typ $[1^7]$, 2 av typ $[1^5 2^1]$, 1 av typ $[1^3 2^2]$, 2 av typ $[1^1 2^3]$ och 2 av typ $[1^1 2^1 4^1]$ blir det sökta antalet $\frac{1}{8}(1 \cdot 7 \cdot 2^6 + 2 \cdot 5 \cdot 2^5 + 1 \cdot 3 \cdot 2^4 + 2 \cdot 1 \cdot 2^3 + 2 \cdot 1 \cdot 2^2) = 7 \cdot 2^3 + 5 \cdot 2^3 + 3 \cdot 2 + 2 + 1 = 105$.

Svar: Pärlorna kan färgas på 105 väsentligt olika sätt.