

**Lösningar tentan TEN1 SF1631(/SF1630) DISKRET MATEMATIK, D3 m.fl.,
7 januari 2013**

Tryckfel kan förekomma.

1) (4p) Vi skall visa att en graf med 21 hörn och 58 kanter inte kan vara planär.

Lösning: Antag (för att få en motsägelse) att grafen är planär och betrakta en plan ritning av den.

Låt antalet hörn i grafen vara v , antalet kanter e , antalet ytor grafen delar in planet i r (inklusive den omgivande, obegränsade ytan) och antalet komponenter c .

Summan av antalen kanter kring ytorna är $2e$ (varje kant räknas dubbelt) och de summerade antalen är alla ≥ 3 (inga multipla kanter eller öglor), så $2e \geq 3r$, dvs $r \leq \frac{2}{3}e$.

Enligt en känd sats ger det $c+1 = v - e + r \leq v - \frac{1}{3}e = 21 - \frac{58}{3} = \frac{5}{3}$, så $c \leq \frac{2}{3}$. Men eftersom $v \neq 0$ är $c \geq 1$. Antagandet att grafen är planär ledde till motsägelse, så **saken är klar**.

(Alt.: Åberopa direkt olikheten $3v \geq e + 3(c+1)$ för planaritet, i stencilen om planära grafer.)

2) (4p) Vi söker alla lösningar $x \in \mathbb{Z}_{741}$ till ekvationen $51x = 18$.

Lösning: Problemet motsvarar den diofantiska ekvationen $51x - 741k = 18$. Euklides algoritmen ger $741 = 14 \cdot 51 + 27$, $51 = 1 \cdot 27 + 24$, $27 = 1 \cdot 24 + 3$, $24 = 8 \cdot 3$ så **sgd(741, 51) = 3** och $3 = 27 - 1 \cdot 24 = 27 - 1(51 - 1 \cdot 27) = -1 \cdot 51 + 2 \cdot 27 = -51 + 2(741 - 14 \cdot 51) = 2 \cdot 741 - 29 \cdot 51$.

Multiplikation med 6 ger $-174 \cdot 51 + 12 \cdot 741 = 18$, så $\begin{cases} x_0 = -174 \\ k_0 = -12 \end{cases}$ är en lösning till den diofantiska ekvationen.

(x, k) uppfyller då ekvationen precis om $51(x - x_0) - 741(k - k_0) = 0$, dvs (dividera med $\text{sgd}(51, 741) = 3$) $17(x - x_0) = 247(k - k_0)$, där $\text{sgd}(17, 247) = 1$. Så (entydig faktorisering) $x - x_0 = 247q$, för något $q \in \mathbb{Z}$. Varje $q \in \mathbb{Z}$ ger också en lösning ($k - k_0 = 17q$). $0 \leq x < 741$ ger tre värden $x = 73, 320, 567$. **Svar: Alla lösningar i $\mathbb{Z}_{741}$ är $x = 73, 320, 567$.**

3) De 5 första uppgifterna på en skrivning kan ge 0 eller 1 poäng och de övriga 5 kan ge 0, 1 eller 2 poäng. Vi söker (a, 1p) antalet möjliga resultat och (b, 3p) antalet av dem som innehåller alla poäng 0, 1 och 2.

Lösning: Låt X vara mängden möjliga resultat. Multiplikationsprincipen ger $|X| = 2^5 \cdot 3^5 (= 7776)$.

För b) använder vi principen om inklusion och exklusion (sällprincipen).

Låt A_i för $i = 0, 1, 2$ vara mängden resultat utan något "i".

Då är $|A_0| = |A_1| = 1^5 \cdot 2^5$ (bara 1 resp. 0 möjligt för uppgift 1-5), $|A_2| = 2^{10}$ (bara 0 och 1 möjliga för alla uppgifter), $|A_0 \cap A_1| = 0$ (inget möjligt resultat för uppgift 1-5), $|A_0 \cap A_2| = |A_1 \cap A_2| = 1^{10}$ (bara 1 resp. 0 möjligt för alla uppgifter), $|A_0 \cap A_1 \cap A_2| = 0$ (inget möjligt resultat för någon uppgift).

Med X som ovan är det sökta antalet $|X \setminus (A_0 \cup A_1 \cup A_2)| = |X| - (|A_0| + |A_1| + |A_2|) + (|A_0 \cap A_1| + |A_0 \cap A_2| + |A_1 \cap A_2|) - |A_0 \cap A_1 \cap A_2| = 2^5 \cdot 3^5 - (2 \cdot 2^5 + 2^{10}) + (0 + 1 + 1) - 0 = 3^5 \cdot 2^5 - 2^{10} - 2^6 + 2 (= 6690)$

Svar a: $3^5 \cdot 2^5 (= 7776)$, b: $3^5 \cdot 2^5 - 2^{10} - 2^6 + 2 (= 6690)$ möjliga resultat.

4) (4p) Vi söker det minsta möjliga e -värdet > 1000 för ett RSA-system för kryptering med de "stora" primtalen $p = 43$ och $q = 61$.

Lösning: $m = (p-1)(q-1) = 42 \cdot 60 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$. e fungerar som krypteringsexponent om $\text{sgd}(e, m) = 1$, så $(7 \mid 1001, 2 \mid 1002, 2, 3, 5, 7 \nmid 1003)$:

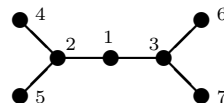
Svar: Det minsta möjliga $e > 1000$ är $e = 1003$.

5) (4p) Vi söker antalet irreducibla monadiska andragradspolynom i $\mathbb{Z}_5[x]$.

Lösning: Ett monadiskt andragradspolynom i $\mathbb{Z}_5[x]$ har formen $x^2 + ax + b$, där $a, b \in \mathbb{Z}_5$ och olika (a, b) ger olika polynom. Det totala antalet sådana polynom är alltså $5 \cdot 5 = 25$. Reducibla monadiska andragradspolynom i $\mathbb{Z}_5[x]$ kan skrivas $(x - \alpha)(x - \beta)$, med $\alpha, \beta \in \mathbb{Z}_5$. Olika $\{\alpha, \beta\}$ ger olika polynom, så antalet reducibla är $5 + \binom{5}{2} = 15$ (5 med $\alpha = \beta$ och $\binom{5}{2} = 10$ med $\alpha \neq \beta$). De irreducibla är alltså $25 - 15 = 10$ st.

Svar: Antalet irreducibla monadiska andragradspolynom i $\mathbb{Z}_5[x]$ är 10.

6) (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 (Thm 21.4 i boken) är antalet väsentligt olika färgningar = antalet banor för gruppens verkan på färgningarna $= \frac{1}{|G|} \sum_{g \in G} |F(g)|$.

Om $g \in G$ som permutation har cykelstrukturen $[1^{\alpha_1} 2^{\alpha_2} \dots]$, är $|F(g)|$, 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: På 105 olika sätt.

7) (5p) Vi söker antalet $\pi \in S_8$ som uppfyller att $\pi^6(1) \neq 2$.

Lösning: Vi beräknar först antalet $\pi \in S_8$ med $\pi^6(1) = 2$ (och drar bort dem).

$\pi^6(1) = 2$ precis om 1 ingår i en cykel av form $(1 \ 2 \dots)$, $(1 \ 2 \dots)$, $(1 \dots \dots 2)$, $(1 \dots \dots 2 \dots)$ (cykler av längd 1, 2, 3 eller 6 ger $\pi^6(1) = 1$). Antalen π med sådana cykler är resp. $(6)_2 \cdot 4! = 6!$ ("..."arna i cykeln kan väljas bland 3-8 på $(6)_2 = 6 \cdot 5$ sätt och de övrigas permutation på $4!$ sätt), $(6)_3 \cdot 3! = 6!$, $(6)_5 \cdot 1! = 6!$, $(6)_6 \cdot 0! = 6!$. Inget π kan innehålla mer än en av dessa cykler, så det totala antalet med $\pi^6(1) = 2$ är $4 \cdot 6!$.

(Alternativt: Antalet π med $\pi^6(1) = 2$ är $\frac{1}{7}$ av alla med $\pi^6(1) \neq 1$ och de med $\pi^6(1) = 1$ är de med 1 i 1, 2, 3, 6-cykler, som ovan $(7)_0 \cdot 7! + (7)_1 \cdot 6! + (7)_2 \cdot 5! + (7)_5 \cdot 2! = 4 \cdot 7!$ stycken, så de med $\pi^6(1) = 2$ är $\frac{1}{7}(8! - 4 \cdot 7!) = 4 \cdot 6!$.) Det sökta antalet är alltså $8! - 4 \cdot 6! = (8 \cdot 7 - 4)6! = 52 \cdot 720 = 37440$.

Svar: Antalet $\pi \in S_8$ med $\pi^6(1) \neq 2$ är 37440.

8) (5p) Vi skall visa att en graf $G = (V, E)$ (där $V \neq \emptyset$) med antalet hörn med valens 3 lika med antalet hörn med valens antingen 0 eller 1, innehåller minst en cykel.

Lösning: Låt $V' = \{v \in V \mid \delta(v) \neq 0\}$ och $G' = (V', E)$.

G' saknar hörn med valens 0 och antalet hörn med valens 3 är $\geq$ antalet hörn med valens 1. Det betyder att $\sum_{v \in V'} \delta(v) \geq 2|V'|$, men den summan är ("handslagslemmat") $= 2|E|$, så $|E| \geq |V'|$. Om det inte funnes några cykler, vore varje komponent ett träd och skulle innehålla ett hörn mer än kanter. Det skulle innebära att $|V'| = |E| + c$ (c antalet komponenter), men $c > 0$, ty $V \neq \emptyset$ ger att det finns $v \in V$ med $\delta(v) \neq 0$, så $V' \neq \emptyset$. Antagandet att grafen saknar cykler ledde till motsägelse, så den har minst en cykel. **Saken är klar.**

9) Vi söker (a, 1p) 3 olika x med $0 \leq x < 437$ och (b, 5p) alla heltal x som uppfyller $x^3 - 7x^2 + 12x \equiv 0 \pmod{437}$ [$437 = 19 \cdot 23$].

Lösning: Eftersom $x^3 - 7x^2 + 12x = x(x-3)(x-4)$ är $x = 0, 3, 4$ tre olika lösningar.
 $x^3 - 7x^2 + 12x \equiv 0 \pmod{437} \Leftrightarrow 19 \cdot 23 = 437 \mid x^3 - 7x^2 + 12x = x(x-3)(x-4) \Leftrightarrow$
 $\Leftrightarrow [19 \mid x(x-3)(x-4) \text{ och } 23 \mid x(x-3)(x-4)]$ (eftersom 19 och 23 är primtal).
 x uppfyller alltså den givna kongruensen om $x \equiv_{19} i$, $x \equiv_{23} j$, där $i, j \in \{0, 3, 4\}$.
Det handlar alltså om den kinesiska restsatsen. $23 = 1 \cdot 19 + 4$, $19 = 4 \cdot 4 + 3$, $4 = 1 \cdot 3 + 1$,
så $1 = 4 - 3 = 4 - (19 - 4 \cdot 4) = -19 + 5 \cdot 4 = -19 + 5(23 - 19) = 5 \cdot 23 - 6 \cdot 19 = 115 - 114$
och således $115 \equiv_{19} 1$, $\equiv_{23} 0$ och $-114 \equiv_{19} 0$, $\equiv_{23} 1$.
Modulo $19 \cdot 23 = 437$ ges alltså alla lösningar av $115 \cdot i - 114 \cdot j$. Man finner $115 \cdot 0 - 114 \cdot 0 = 0$,
 $115 \cdot 3 - 114 \cdot 0 = 345$, $115 \cdot 4 - 114 \cdot 0 = 460 \equiv_{437} 23$, $115 \cdot 0 - 114 \cdot 3 = -342 \equiv_{437} 95$,
 $115 \cdot 3 - 114 \cdot 3 = 3$, $115 \cdot 4 - 114 \cdot 3 = 118$, $115 \cdot 0 - 114 \cdot 4 = -456 \equiv_{437} 418$, $115 \cdot 3 - 114 \cdot 4 = -111 \equiv_{437} 326$,
 $115 \cdot 4 - 114 \cdot 4 = 4$. Lösningarna är alltså precis alla $x \equiv_{437}$ någon av dem.

Svar a: T.ex. $x = 0, 3, 4$,

b: $x = k + 437n$, där $k \in \{0, 3, 4, 23, 95, 118, 326, 345, 418\}$ och $n \in \mathbb{Z}$.

10) G är en grupp och vi skall visa (a, 3p) att om $axbxa = x^{-1}$ har en lösning $x \in G$ för alla $a, b \in G$, så finns för varje $g \in G$ ett $c \in G$ så att $g = c^3$ och (b, 3p) att om för varje $g \in G$ finns $c \in G$ med $g = c^3$, så finns för alla $a, b \in G$ ett $x \in G$ med $axbxa = x^{-1}$.

Lösning: a) Antag att ekvationen $axbxa = x^{-1}$ har en lösning $x \in G$ för alla $a, b \in G$. Låt d vara en lösning med $b = g$, $a = 1$, dvs $1dgd1 = d^{-1}$. Då (multiplicera med d^{-1} från båda sidor) är $g = (d^{-1})^3$ och (g var godtyckligt, $c = d^{-1}$) **saken är klar**.

b) Antag att för varje $g \in G$ finns $c \in G$ med $g = c^3$. $axbxa = x^{-1} \Leftrightarrow axbxa x = 1 \Leftrightarrow$
 $bxaxax = 1 \Leftrightarrow b(xa)^3 = a \Leftrightarrow a^{-1}b = ((xa)^{-1})^3$. Enligt förutsättningen är $a^{-1}b = c^3$ för något $c \in G$. $x = c^{-1}a^{-1}$ löser då ekvationen (med de godtyckliga a, b). **Saken är klar**.
