

Lösningar tenta SF1688 DISKRET MATEMATIK, D3 m.fl.

20 december 2017

Tryckfel kan förekomma.

- 1a)** (1p) Graferna $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ är isomorfa omm det finns en bijektion $\phi : V_1 \rightarrow V_2$ sådan att $\{x, y\} \in E_1 \Leftrightarrow \{\phi(x), \phi(y)\} \in E_2$ för alla $x, y \in V_1$.
- b)** (1p) Det kromatiska talet, $\chi(G)$, för en graf $G = (V, E)$ är det minsta antalet färger som gör det möjligt att färga hörnen så att inga grannar har samma färg.
- c)** (1p) För en plan sammanhängande graf gäller $v - e + r = 2$, där v är antalet hörn i grafen, e antalet kanter i den och r antalet ytor den delar in planet i.

- 2a)** (1p) $(G, \circ)$ är en grupp omm 1. $(x \circ y) \circ z = x \circ (y \circ z)$ för alla $x, y, z \in G$ (associativitet), 2. Det finns $e \in G$ sådant att $e \circ x = x \circ e = x$ för alla $x \in G$ (identitetsselement) och 3. För varje $x \in G$ finns $x^{-1} \in G$ med $x \circ x^{-1} = x^{-1} \circ x = e$ (inverseelement).
(Villkoret om slutenhet behövs inte, eftersom vi förutsatt att $\circ : G \times G \rightarrow G$.)
- b)** (1p) Antalet delgrupper av ordning m är 1 om $m \mid n$, annars 0.
- c)** (1p) π och σ är konjugerade omm de har samma cykelstruktur, dvs för varje $i = 1, 2, \dots$ har π och σ samma antal cykler av längd i .

- 3a)** (1p) Stabilisatorn för $x \in X$ då G verkar på X är $G_x = \{g \in G \mid gx = x\}$.
- b)** (1p) Operationen $\cdot$ skall vara kommutativ och alla $x \in R$ utom 0 skall ha en invers $x^{-1} \in R$ (dvs $x \cdot x^{-1} = 1$). R skall förstås ha en etta.
- c)** (1p) Om $f(x) \in F[x]$ är $x - \alpha$ en delare till $f(x)$ omm $f(\alpha) = 0$ i F .

- 4a)** (1p) H 's kolonner skall alla vara olika och inte **0**-kolonnen.
- b)** (1p) Om p, q är primtal och $k \equiv_{(p-1)(q-1)} 1$ är $x^k \equiv_{p \cdot q} x$ för alla $x \in \mathbb{Z}$.
- c)** (1p) Fermattestet med bas b ($b \in \mathbb{Z}_+$, $b < N$) för att avgöra om $N \in \mathbb{Z}_+$ är ett primtal: Är $b^{N-1} \equiv 1 \pmod{N}$? Om svaret är "nej" är N inte ett primtal.

- 5)** (4p) Vi skall visa att om $G = (V, E)$ är isomorf med $\overline{G}$ är $|V| \equiv 0$ eller $1 \pmod{4}$.

Lösning:

För $x \in V$, låt $\delta(x)$ vara dess valens i G och $\bar{\delta}(x)$ den i $\overline{G}$. Då är $\delta(x) + \bar{\delta}(x) = |V| - 1$ för alla $x \in V$, så $\sum_{x \in V} (\delta(x) + \bar{\delta}(x)) = |V|(|V| - 1)$. Känt är att $\sum_{x \in V} \delta(x) = 2|E|$ och då G och $\overline{G}$ är isomorfa är $\sum_{x \in V} \delta(x) = \sum_{x \in V} \bar{\delta}(x)$, så $|V|(|V| - 1) = 4|E|$. Eftersom en av $|V|$ och $|V| - 1$ är udda är den andra delbar med 4, dvs $|V| \equiv_4 0$ eller 1. **Saken är klar.**

- 6)** (3p) Vi vet att g i gruppen G har ordning 60 och söker ordningen för g^{78} .

Lösning:

Ordningen för g^{78} är det minsta $k > 0$ med $(g^{78})^k = g^{78k} = 1$, identitetsselementet i G . Enligt en känd sats är $g^n = 1$ omm $60 \mid n$ (eftersom g 's ordning är 60). $60 \mid 78k \Leftrightarrow 10 \mid 13k$ (ty $60 = 6 \cdot 10$, $78 = 6 \cdot 13$), så det minsta $k > 0$ som uppfyller $g^{78k} = 1$ är 10 (sgd(10, 13) = 1, så $10 \mid k$). Det betyder att g^{78} har ordning 10.

Svar: g^{78} har ordning 10.

7) (3p) Vi söker den moniska största gemensamma delaren i $\mathbb{Z}_5[x]$ till $f(x) = x^4 + x^3 + 3x^2 + x + 1$ och $g(x) = x^5 + 3x^4 + 3x^3 + 3x + 4$.

Lösning:

Vi använder (förstås) Euklides algoritm.

Polynomdivision i $\mathbb{Z}_5[x]$ ger $g(x) = (x+2)f(x) + (3x^3 + 3x^2 + 2) = (x+2)f(x) + h(x)$,

$f(x) = 2x \cdot h(x) + (3x^2 + 2x + 1) = 2x \cdot h(x) + k(x)$ och $h(x) = (x+2)k(x)$.

$k(x) = 3x^2 + 2x + 1$ är alltså en sgd till $f(x)$ och $g(x)$. För att finna den moniska sgd:n multiplicerar vi med (det inverterbara elementet) 2 och får $x^2 + 4x + 2$.

Svar: Den moniska största gemensamma delaren är $x^2 + 4x + 2$.

8) Vi söker i $\mathbb{Z}_{1547}$ ($1547 = 7 \cdot 13 \cdot 17$) potenserna (a, 1p) 55^{1153} , (b, 1p) 10^{100} och (c, 1p) 26^{224} .

Lösning:

Kinesiska restsatsen och Fermats lilla sats för vart och ett av primtalen 7, 13 och 17.

a. $1153 \equiv_6 1, \equiv_{12} 1, \equiv_{16} 1$ och Fermats lilla ($7, 13, 17 \nmid 55$) ger $55^{1153} \equiv_7 55, \equiv_{13} 55, \equiv_{17} 55$, så $55^{1153} = 55$ i $\mathbb{Z}_{1547}$. (Alt. Eulers sats, $\phi(1547) = 6 \cdot 12 \cdot 16 = 1152$.)

b. $100 \equiv_6 4, \equiv_{12} 4, \equiv_{16} 4$ och Fermats lilla ($7, 13, 17 \nmid 10$) ger $10^{100} \equiv_7 10^4, \equiv_{13} 10^4, \equiv_{17} 10^4 = 10\,000$, så $10^{100} \equiv_{1547} 10\,000 \equiv_{1547} 718$.

c. $26 \equiv_7 5, \equiv_{13} 0, \equiv_{17} 9$ och $224 \equiv_6 2, \equiv_{16} 0$ och Fermats lilla ($7, 17 \nmid 26$) ger $26^{224} \equiv_7 5^2 = 25 \equiv_7 4, \equiv_{13} 0, \equiv_{17} 9^0 = 1$.

Med $x = 26^{224}$ har vi alltså $x \equiv_{13} 0$, $x \equiv_7 4$ och $x \equiv_{17} 1$.

Den första ger $x = 13s$ för något $s \in \mathbb{Z}$. Den andra ger då $13s \equiv_7 4$, så $0 \equiv_7 s + 4$, dvs $s = 7t + 3$ och $x = 13(7t + 3) = 91t + 39$ för något $t \in \mathbb{Z}$. Den tredje ekvationen ger $91t + 39 \equiv_{17} 6t + 5 \equiv_{17} 1$. Eftersom $\text{sgd}(3, 17) = 1$ kan vi multiplicera med 3 och får $18t + 15 \equiv_{17} t - 2 \equiv_{17} 3$, så $t = 17u + 5$ för något $u \in \mathbb{Z}$ och för varje $u \in \mathbb{Z}$ fås en lösning $x = 91(17u + 5) + 39 = 1547u + 455 + 39 \equiv_{1547} 494$.

Svar: Potenserna är a: 55, b: 718, c: 494 i $\mathbb{Z}_{1547}$.

9) Gruppen G har delgrupperna H och N , varav N är en normal delgrupp. Vi skall visa att HN är en delgrupp till G .

Lösning:

Enligt en känd sats är $M \subseteq G$, $M \neq \emptyset$, en delgrupp till G om $x, y \in M \Rightarrow xy, x^{-1} \in M$. $x, y \in HN \Rightarrow x = h_1n_1, y = h_2n_2$ för några $h_i \in H, n_i \in N$, så $xy = h_1n_1h_2n_2 = h_1h_2n_3n_2$, $x^{-1} = n_1^{-1}h_1^{-1} = h_1^{-1}n_4 \in HN$ (ty $Nh_2 = h_2N$ ger att $n_1h_2 = h_2n_3$ för något $n_3 \in N$ och motsvarande $n_1^{-1}h_1^{-1} = h_1^{-1}n_4$ för något $n_4 \in N$). $HN \neq \emptyset$, ty $1 \in H, N$ ger $1 = 1 \cdot 1 \in HN$, så HN är en delgrupp. **Saken är klar.**

10) (4p) 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 en av 0 och 1, innehåller minst en cykel.

Lösning:

Låt $V' = \{v \in V \mid \delta(v) \neq 0\}$ och $G' = (V', E)$. $V' \neq \emptyset$ (annars vore alla G :s valenser 0, otillåtet.)

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 det finns $v \in V$ med $\delta(v) \neq 0$ ($V' \neq \emptyset$). Antagandet att grafen saknar cykler gav en motsägelse, så den har minst en cykel. **Saken är klar.**

11) Vi söker (a, 2p) alla möjliga cykelstrukturer för udda permutationer av ordning 12 i S_{10} och (b, 2p) det totala antalet udda permutationer av ordning 12 i S_{10} .

Lösning:

a. Eftersom ordningen för en permutation är mgm till cykellängderna, måste en av dem vara en multipel av 4, men inte 8, så en 4-cykel måste ingå (≤ 10 ju). P.s.s. måste en cykellängd vara en multipel av 3, men inte 9. 6 går inte, eftersom [46]-permutationer är jämna, så (minst) en cykel måste ha längd 3. Det totala antalet cykler av jämn längd skall vara udda för udda permutation, så enda möjligheterna är $[3^2 4]$ och $[1^3 34]$.

b. Antalet av typ $[3^2 4]$ är $\frac{10!}{2 \cdot 3^2 \cdot 4} = \frac{10!}{72}$ (10! sätt placera in 1–10 i cyklerna, samma permutation om man kastar om 3-cyklerna, i sätt skriva samma i -cykel). P.s.s fås antalet av typ $[1^3 34]$ till $\frac{10!}{3! \cdot 3 \cdot 4} = \frac{10!}{72}$.

Det sökta antalet är summan av dem (additionsprincipen!), $\frac{10!}{36} = 10 \cdot 2 \cdot 7! = 20 \cdot 5040 = 100800$.

Svar a: Möjliga cykelstrukturer är $[3^2 4]$ och $[1^3 34]$, b: Det finns 100 800 st.

12) Vi söker (a, 1p) $|R|$ och (b, 4p) alla lösningar till ekvationen $t^2 + 3t + 3 = 0$ i ringen $R = \mathbb{Z}_{11}[x]/(x^2 + 1)$. Vi kallar restklassen som innehåller x för α .

Lösning:

a. Varje restklass i R innehåller precis ett polynom av grad ≤ 1 (och alla sådana ligger förstås i sin restklass), så elementen i R kan skrivas $a + b\alpha$, där olika $a, b \in \mathbb{Z}_{11}$ ger olika element. Det ger att $|R| = 11^2 = 121$.

b. $t^2 + 3t + 3 = t^2 + 14t + 5 + 9 = (t + 7)^2 + 9$, så ekvationen kan skrivas $(t + 7)^2 + 9 = 0$. $t + 7$ måste alltså vara ett element i R med kvadraten $-9 = 2$. Kvadraterna av elementen i $\mathbb{Z}_{11} = \{0, 1, 2, 3, \dots, 10\}$ är 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1, alla skilda från 2, men eftersom $x^2 = (x^2 + 1) - 1$ är $\alpha^2 = -1$ och $(3\alpha)^2 = (8\alpha)^2 = 9(-1) = -9 = 2$, så $t + 7 = 3\alpha$, 8α ger lösningar till ekvationen: $t = -7 + 3\alpha$, $-7 + 8\alpha = 4 \pm 3\alpha$.

Det finns inget element i $\mathbb{Z}_{11}$ med kvadrat $-1 = 10$, så $x^2 + 1$ är irreducibelt (andragradspolynom utan nollställe) och R alltså en kropp. Det följer (från faktorsatsen) att ett andragradspolynom kan ha högst två nollställen i R , så vi har funnit alla lösningar.

Svar a: $|R| = 121$, b: Alla lösningar är $t = 4 \pm 3\alpha$.

13) (5p) Vi söker antalet väsentligt olika sätt att färga en kubs kanter med hälften av kanterna röda eller blå och hälften gula eller gröna.

Lösning:

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

typ av g	g :s permutation av kubens kanter	antal g	$ F(g) $
id	$[1^{12}]$	1	$\binom{12}{6} \cdot 2^{12}$
rot $hh \pm \frac{2\pi}{3}$	$[3^4]$	8	$\binom{4}{2} \cdot 2^4$
rot $kk \pi$	$[1^2 2^5]$	6	$(\binom{5}{2} + \binom{5}{3}) \cdot 2^7$
rot $ss \pm \frac{\pi}{2}$	$[4^3]$	6	0
rot $ss \pi$	$[2^6]$	3	$\binom{6}{3} \cdot 2^6$

("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 kanter i samma cykel i g :s permutation) färgningar.

$|F(id)|$: vilka 6 kanter röd/blå?, varje kant kan sedan ha en av två färger,

på övriga rader fördelas cyklerna på motsvarande sätt.

Lemmat ger antalet färgningar: $\frac{1}{|G|} \sum_{g \in G} |F(g)| = \frac{1}{24} (\binom{12}{6} \cdot 2^{12} + 8 \cdot \binom{4}{2} \cdot 2^4 + 6 \cdot (\binom{5}{2} + \binom{5}{3}) \cdot 2^7 + 6 \cdot 0 + 3 \cdot \binom{6}{3} \cdot 2^6) = \frac{1}{24} (\frac{12!}{6!^2} \cdot 2^{12} + 8 \cdot 6 \cdot 2^4 + 6 \cdot 20 \cdot 2^7 + 3 \cdot 20 \cdot 2^6) = 308 \cdot 2^9 + 2^5 + 5 \cdot 2^7 + 5 \cdot 2^5 = 77 \cdot 2^{11} + 13 \cdot 2^6 = 158\,528$.

Svar: Det sökta antalet är $77 \cdot 2^{11} + 13 \cdot 2^6 = 158\,528$.