Matematik, KTH
B.Ek

Lösningar tentan TEN1 SF1631(/SF1630) DISKRET MATEMATIK, D3 m.fl., 7 januari 2014

Tryckfel kan förekomma.

1) (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 $\overline{\delta}(x)$ den i $\overline{G}$. Då är $\delta(x) + \overline{\delta}(x) = |V| - 1$ för alla $x \in V$, så $\sum_{x \in V}(\delta(x) + \overline{\delta}(x)) = |V|(|V| - 1)$. Känt är att $\sum_{x \in V} \delta(x) = 2|E|$ och då G och $\overline{G}$ är isomorfa är $\sum_{x \in V} \delta(x) = \sum_{x \in V} \overline{\delta}(x)$, 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.

---

2) (4p) Vi söker alla heltal x, y sådana att $186x + 69y = 3$.

Lösning: Då ekvationen divideras med 3 fås den ekvivalenta $62x + 23y = 1$.
Euklides algoritm ger $62 = 2 \cdot 23 + 16$, $23 = 1 \cdot 16 + 7$, $16 = 2 \cdot 7 + 2$, $7 = 3 \cdot 2 + 1$ (så $\text{sgd}(62, 23) = 1$ och) $1 = 7 - 3 \cdot 2 = 7 - 3(16 - 2 \cdot 7) = -3 \cdot 16 + 7 \cdot 7 = -3 \cdot 16 + 7 \cdot (23 - 16) = 7 \cdot 23 - 10 \cdot 16 = 7 \cdot 23 - 10(62 - 2 \cdot 23) = -10 \cdot 62 + 27 \cdot 23$.
$\begin{cases} x_0 = -10 \\ y_0 = 27 \end{cases}$ är alltså en lösning till ekvationen. (x, y) uppfyller då ekvationen precis om $62(x - x_0) + 23(y - y_0) = 0$, dvs $62(x - x_0) = -23(y - y_0)$, så (entydig faktorisering och $\text{sgd}(62, 23) = 1$) $x - x_0 = 23k$, för något $k \in \mathbb{Z}$. Det ger $y - y_0 = -62k$. Man ser att $x = x_0 + 23k$, $y = y_0 - 62k$ också löser ekvationen för alla $k \in \mathbb{Z}$, så vi har funnit alla lösningar.
Svar: Alla lösningar ges av $\begin{cases} \boldsymbol{x = -10 + 23k}, \\ \boldsymbol{y = 27 - 62k}, \end{cases}$ **för godtyckligt** $\boldsymbol{k} \in \mathbb{Z}$**.**

---

3) Vi söker (a, 3p) antalet sätt att fördela 12 olika böcker och 6 identiska pennor bland 20 personer, då varje person kan få högst en bok, och (b, 1p) antalet sätt då dessutom minst en person får både en bok och minst en penna.

Lösning: a. Böckerna kan fördelas på $(20)_{12} = \frac{20!}{(20-12)!} = \frac{20!}{8!}$ sätt (antalet injektioner böcker $\rightarrow$ personer).
Pennorna kan fördelas på $\binom{20+6-1}{6} = \frac{25!}{6! \cdot 19!}$ sätt (6 pennor utses bland 25 pennväggar).
Multiplikationsprincipen ger svaret $\frac{20!}{8!} \cdot \frac{25!}{6! \cdot 19!} = \frac{20 \cdot 25!}{6! \cdot 8!}$.
b. Från svaret i a) dras antalet fördelningar då alla som fått en bok blir utan penna. De är som ovan $\frac{20!}{8!} \cdot \binom{8+6-1}{6} = \frac{13! \cdot 20!}{6! \cdot 7! \cdot 8!}$ (pennorna fördelas bland de 8 som inte fått någon bok). Antalet blir alltså $\frac{20!}{8!}\left(\frac{25!}{6! \cdot 19!} - \frac{13!}{6! \cdot 7!}\right) = \frac{20!}{6! \cdot 8!}\left(\frac{25!}{19!} - \frac{13!}{7!}\right)$.
Svar a: På $\frac{20 \cdot 25!}{6! \cdot 8!}(= 10\,686\,184\,167\,859\,200\,000)$ **sätt,**
b: På $\frac{20!}{6! \cdot 8!}\left(\frac{25!}{19!} - \frac{13!}{7!}\right)(= 10\,582\,641\,016\,915\,968\,000)$ **sätt.**

---

4) (4p) Vi skall visa att om G är en grupp och $a, b, c \in G$ uppfyller $abc = b^{-1}$ så är $cba = b^{-1}$.

Lösning: $abc = b^{-1} \Rightarrow abcb = 1 \Rightarrow bcb = a^{-1} \Rightarrow bcba = 1 \Rightarrow cba = b^{-1}$. **Saken är klar.**

---

5) (4p) 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 $\boldsymbol{x^2 + 4x + 2}$**.**

---

6) (5p) Vi söker $|V|$ och $|E|$ för en graf $G = (V, E)$ där varje komponent innehåller högst en cykel, precis 18 av komponenterna saknar cykel och medelvärdet av hörnens valenser är $\frac{78}{41}$.

Lösning: Låt $v = |V|$, $e = |E|$. En komponent utan cykel är ett träd, så den innehåller ett hörn mer än kanter, medan en komponent med precis en cykel har en kant mer, dvs lika många hörn som kanter. Det ger att $v = e + 18$.
Medelvärdet av valenserna, $\frac{78}{41} = 2 - \frac{4}{41}$, är $\frac{1}{v}\sum_{x \in V} \delta(x) = \frac{1}{v} \cdot 2e = \frac{2(v-18)}{v} = 2 - \frac{36}{v}$, så $\frac{36}{v} = \frac{4}{41}$ och $v = \frac{36}{4} \cdot 41 = 369$ och $e = v - 18 = 351$.
Svar: Grafen har 369 hörn och 351 kanter.

---

7) $\pi \in S_8$ ges av $\pi(1)=3$, $\pi(2)=1$, $\pi(3)=8$, $\pi(4)=7$, $\pi(5)=4$, $\pi(6)=6$, $\pi(7)=5$, $\pi(8)=2$.
Vi skall (a, 1p) skriva π i cykelnotation, (b, 1p) avgöra om π är jämn eller udda, (c, 1p) finna $\tau \in S_8$ med $\pi\tau = \tau\sigma$, där $\sigma = (1\,6\,4)(2\,8\,3\,7)$ och (d, 2p) finna antalet möjliga τ i c).

Lösning: a. $\pi(1) = 3$, $\pi(3) = 8$, $\pi(8) = 2$, $\pi(2) = 1$, $\pi(4) = 7, \ldots$ ger att $\pi = (1\,3\,8\,2)(4\,7\,5)(6)$.
b. Eftersom π har ett udda antal (1) cykler av jämn längd är det en udda permutation.
c. $\pi\tau = \tau\sigma \Leftrightarrow \pi = \tau\sigma\tau^{-1}$ och $\tau\sigma\tau^{-1} = \big(\tau(1)\,\tau(6)\,\tau(4)\big)\big(\tau(2)\,\tau(8)\,\tau(3)\,\tau(7)\big)\big(\tau(5)\big)$, så vi kan ta $\tau(1)=4$, $\tau(6)=7$, $\tau(4)=5$, $\tau(2)=1$, $\ldots$, $\tau(5)=6$. Det ger $\tau = (1\,4\,5\,6\,7\,2)(3\,8)$.
d. τ skall ta varje i-cykel i σ till i-cykeln i π. Det kan göras på i sätt (om man bestämmer bilden av ett element bestäms övriga). Totalt finns alltså (multiplikationsprincipen) $3 \cdot 4 \cdot 1 = 12$ möjliga τ.
Svar a: $\boldsymbol{\pi = (1\,3\,8\,2)(4\,7\,5)}$, b: $\boldsymbol{\pi}$ är udda, c: t.ex. $\boldsymbol{\tau = (1\,4\,5\,6\,7\,2)(3\,8)}$, d: 12 st.

---

8) Vi söker i $\mathbb{Z}_{1547}$ ($1547 = 7 \cdot 13 \cdot 17$) potenserna (a, 1p) 55^{1153}, (b, 2p) 12^{50} och (c, 2p) 26^{224}.

Lösning: a. Eftersom $\phi(1547) = \phi(7 \cdot 13 \cdot 17) = 6 \cdot 12 \cdot 16 = 1152$ och $\text{sgd}(55, 1547) = 1$ ger Eulers sats att $55^{1152} = 1$ och därmed $55^{1153} = 55$ i $\mathbb{Z}_{1547}$.
b. $\text{sgd}(12, 7) = \text{sgd}(12, 13) = \text{sgd}(12, 17) = 1$, så enligt Fermats lilla sats (7, 13 och 17 är ju primtal) är $12^{48} = (12^6)^8 \equiv_7 1^8 = 1$, $12^{48} = (12^{12})^4 \equiv_{13} 1^4 = 1$, $12^{48} = (12^{16})^3 \equiv_{17} 1^3 = 1$, så $12^{48} - 1$ är delbart med 7, 13 och 17, så med 1547 och $12^{50} \equiv_{1547} 1 \cdot 12^2 = 144$.
c. Som i b) fås $26^{224} \equiv_7 5^{37 \cdot 6 + 2} = (5^6)^{37} \cdot 5^2 \equiv_7 1^{37} \cdot 25 \equiv_7 4$ (ty $7 \nmid 5$), $26^{224} \equiv_{13} 0^{224} = 0$ (ty $13 \mid 26$) och $26^{224} \equiv_{17} 26^{14 \cdot 16} = (26^{16})^{14} \equiv_{17} 1^{14} = 1$ (ty $17 \nmid 26$).
Med $x = 26^{224}$ har vi alltså $x \equiv_{13} 0$, $x \equiv_7 4$ och $x \equiv_{17} 1$. Kinesiska restsatsen!
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 $x = 91(17u + 5) + 39 = 1547u + 455 + 39 \equiv_{1547} 494$.
Svar: Potenserna är a: 55, b: 144, c: 494 i $\boldsymbol{\mathbb{Z}_{1547}}$.

---

9) (6p) En kub skall få en enfärgad kula i varje hörn. Vi söker antalet väsentligt olika sätt det kan ske om de röda och de blå kulorna tillsammans skall vara fyra stycken och övriga fyra kulors färger väljs bland k andra färger.

Lösning: Vi använder Burnsides lemma (Thm 21.4 i Biggs). Symmetrigruppen G har 24 element ($|Gx||G_x| = 8 \cdot 3 = 24$ om x är ett av kubens hörn):
identitets"rotationen" id,
8 rotationer $\frac{2\pi}{3}$ kring axlar genom motsatta hörn rot_{hh},
6 rotationer π kring axlar genom mittpunkter av motsatta kanter rot_{kk},
3 rotationer π kring axlar genom mittpunkter av motsatta sidor $\mathrm{rot}_{ss\pi}$ och
6 rotationer $\frac{\pi}{2}$ kring axlar genom mittpunkter av motsatta sidor $\mathrm{rot}_{ss\frac{\pi}{2}}$.
$|F(g)|$, antalet konfigurationer som inte ändras av g för de olika $g \in G$ blir:

g	antal g	$\lvert F(g)\rvert$
id	1	$\binom{8}{4} \cdot 2^4 \cdot k^4$ (vilka r/b? varje av dem r eller b? övriga vilka av k?)
rot_{hh}	8	$2 \cdot 2 \cdot 2^2 \cdot k^2$ (ett hörn, en 3-bana r/b, r eller b? två möjliga k-färger)
rot_{kk}	6	$\binom{4}{2} \cdot 2^2 \cdot k^2$ (fyra par, vilka två r/b? r eller b? övriga vilka av k?)
$\mathrm{rot}_{ss\pi}$	3	$\binom{4}{2} \cdot 2^2 \cdot k^2$ (som rot_{kk})
$\mathrm{rot}_{ss\frac{\pi}{2}}$	6	$2 \cdot 2 \cdot k$ (samma färger fyra och fyra, vilka r/b? etc.)

Så antalet olika utsmyckningar = antalet banor under G:s verkan på färgningarna =
$= \frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{24}(70\cdot 2^4\cdot k^4+(8\cdot 16+(6+3)\cdot 6\cdot 2^2)k^2+6\cdot 2\cdot 2\cdot k) = \frac{1}{3}(140k^4+43k^2+3k)$.
(Man finner t.ex. 62, 806, 3912 då $k=1, 2, 3$.)

Svar: Det finns $\frac{1}{3}(140k^4 + 43k^2 + 3k)$ olika sådana utsmyckningar.

---

10) Vi skall (a, 1p) visa att polynomet $f(x) = x^3 + x + 1$ är irreducibelt i $\mathbb{Z}_2[x]$, (b, 1p) finna α^3, $\alpha^4, \ldots$ i $F = \mathbb{Z}_2[x]/(f(x))$, uttryckta i 1, α och α^2, då α är ekvivalensklassen som innehåller x, och (c, 4p) faktorisera polynomet $g(t) = t^3 + t + 1 \in F[t]$ i irreducibla faktorer.

Lösning: a. Om $f(x)$ vore en produkt av två icke-konstanta polynom vore det ena av grad 1, dvs $f(x)$ skulle ha ett nollställe. Men $f(0) = f(1) = 1$, så $f(x)$ är irreducibelt.
b. α uppfyller $f(\alpha) = 0$ (ty $f(x) \equiv_{(f(x))} 0$ i $\mathbb{Z}_2[x]$), så $\alpha^3 = \alpha + 1$. Det ger
$\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha \cdot \alpha^3 = \alpha^2 + \alpha$, $\alpha^5 = \alpha \cdot \alpha^4 = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2 = \alpha^2 + \alpha + 1$,
$\alpha^6 = \alpha \cdot \alpha^5 = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$, $\alpha^7 = \alpha \cdot \alpha^6 = \alpha^3 + \alpha = \alpha + 1 + \alpha = 1$.
Alla α:s heltalspotenser fås alltså av
$\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2, \alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$
och $\alpha^i = \alpha^j$ om $i \equiv_7 j$ (ty $\alpha^7 = 1$).
c. $g(\alpha) = 0$ i F enligt definitionen av α, så $\big((t - \alpha) =\big)(t + \alpha) \mid g(t)$.
Polynomdivision i F ger $g(t) = (t + \alpha)(t^2 + \alpha t + \alpha^6) = (t + \alpha)h(t)$. För att faktorisera $h(t)$ söker vi nollställen och finner $h(\alpha) = \alpha^6$, men $h(\alpha^2) = \alpha^4 + \alpha^3 + \alpha^6 = \alpha^3(\alpha^3 + \alpha + 1) = 0$, så $(t + \alpha^2) \mid h(t)$. Division ger $h(t) = (t + \alpha^2)(t + \alpha^4)$, så $g(t) = (t + \alpha)(t + \alpha^2)(t + \alpha^4)$.
Faktorerna är alla av grad 1, så irreducibla.

Svar a: Visat ovan, b: $\alpha^i = \alpha^j$ om $i \equiv j \pmod 7$ och
$\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2, \alpha^3 = \alpha+1$, $\alpha^4 = \alpha^2+\alpha$, $\alpha^5 = \alpha^2+\alpha+1$, $\alpha^6 = \alpha^2+1$,
c: $g(t) = (t + \alpha)(t + \alpha^2)(t + \alpha^4)$.
