KTH Matematik
B.Ek

Lösningar tentan SF1610(/5B1118) DISKRET MATEMATIK, CL m.fl., 27 maj 2009

Tryckfel kan förekomma.

1) (3p) Finn alla heltal x, y så att $12x - 21y = 15$.

Division med 3 ger den ekvivalenta ekvationen $4x - 7y = 5$. Euklides algoritm:
$\begin{cases} 7 = 1 \cdot 4 + 3, \\ 4 = 1 \cdot 3 + 1 \end{cases}$ så $\begin{cases} 1 = 4 - 3 = \\ 4 - (7 - 4) = 4 \cdot 2 - 7 \cdot 1 \end{cases}$ och $\begin{cases} x_0 = 10 \\ y_0 = 5 \end{cases}$ är en lösning.
x, y är då en lösning omm $4(x - x_0) = 7(y - y_0)$, dvs (eftersom $\text{sgd}(7, 4) = 1$, måste $7 \mid (x - x_0)$ etc.)
$x - x_0 = 7a$, $y - y_0 = 4a$ för något $a \in \mathbb{Z}$. $b = a + 1$ ger
Svar: Alla lösningar ges av $\begin{cases} \boldsymbol{x = 3 + 7b} \\ \boldsymbol{y = 1 + 4b} \end{cases}$ **, där** $\boldsymbol{b} \in \mathbb{Z}$**.**

---

2) (3p) I en klass med 12 flickor och 15 pojkar skall man dansa (pardans, en pojke och en flicka i varje par). Lukas måste vara med och dansa, men kan inte dansa med Maja. På hur många sätt kan 12 par då bildas?
(Svaret får innehålla fakulteter, heltalspotenser och de fyra vanliga räknesätten.)

Lukas partner kan väljas på 11 sätt (vem som helst utom Maja). Därefter kan 11 flickor välja bland 14 pojkar på $(14)_{11} = 14 \cdot 13 \cdot \ldots \cdot 5 \cdot 4 = \frac{14!}{3!}$ sätt. Multiplikationsprincipen ger
Svar: Paren kan bildas på $\boldsymbol{\frac{11 \cdot 14!}{3!}}$ **(= 159826867200) sätt.**
Alternativt t.ex. $\frac{11}{15} \cdot (15)_{12} = \ldots$ (andelen av alla hopparningar där Lukas varken dansar med Maja eller står över).

---

3) (3p) $U(\mathbb{Z}_{14})$, alla inverterbara element i $\mathbb{Z}_{14}$, utgör en grupp med operation multiplikation (det behöver du inte visa). Avgör om gruppen är cyklisk.

$U(\mathbb{Z}_{14}) = \{r \in \{0, 1, 2, \ldots, 13\} \mid \text{sgd}(r, 14) = 1\} = \{1, 3, 5, 9, 11, 13\}$, så $|U(\mathbb{Z}_{14})| = 6$ och den är cyklisk omm något element har ordning=6.
Man finner $(1 = 1,\, o(1) = 1,)\ 3^2 = 9$, $3^3 = 9 \cdot 3 = 13$, så $o(3) = 6$ (ty $o(g) \mid 6$).
Svar: $\boldsymbol{U(\mathbb{Z}_{14})}$ **är cyklisk (generatorer är 3 och 5).**

---

4) (3p) Man vill skapa ett RSA-system för kryptering med de ”stora” primtalen $p = 43$ och $q = 61$. Vidare vill man ha krypteringsexponenten $e > 1000$.
Finn det minsta möjliga e-värdet.

$m = (p - 1)(q - 1) = 42 \cdot 60 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$. e fungerar som krypteringsexponent omm $\text{sgd}(e, m) = 1$, så ($7 \mid 1001$, $2 \mid 1002$, $2, 3, 5, 7 \nmid 1003$):
Svar: Det minsta möjliga $\boldsymbol{e > 1000}$ **är** $\boldsymbol{e = 1003}$**.**

---

5) (3p) En plan, 3-reguljär (dvs alla hörn har valens (grad) 3) graf består av 7 komponenter och delar in planet i 42 ytor (fasetter), inklusive den obegränsade ytan. Hur många hörn och hur många kanter har grafen?

Om en plan graf har v hörn, e kanter, r ytor och c komponenter gäller $v - e + r - c = 1$. Eftersom $3v = \sum_{x \in V} 3 = \sum_{x \in V} \delta(x) = 2e$, fås $v - \frac{3}{2}v + 42 - 7 = 1$, så $v = 68$ och $e = \frac{3}{2} \cdot 68 = 102$.
Svar: Grafen har 68 hörn och 102 kanter.

---

6) (4p) Finn alla heltal x så att 17 är en delare till $12x^{35} + 8x^3 + 14x$, dvs

$$12x^{35} + 8x^3 + 14x \equiv 0 \pmod{17}.$$

Eftersom $12x^{35} + 8x^3 + 14x = x(12x^{34} + 8x^2 + 14)$ är en möjlighet att $17 \mid x$.
Om $17 \nmid x$ ger Fermats lilla sats (17 är ju primtal) att $x^{16} \equiv 1 \pmod{17}$, så $12x^{35} + 8x^3 + 14x \equiv 12x^3 + 8x^3 + 14x \equiv 3x^3 - 3x = 3x(x-1)(x+1) \pmod{17}$ och enda nya möjligheterna är $17 \mid x - 1$ och $17 \mid x + 1$, så
Svar: Alla lösningar ges av $\boldsymbol{x = 17n}$**,** $\boldsymbol{17n + 1}$**, och** $\boldsymbol{17n - 1}$**,** $\boldsymbol{n} \in \mathbb{Z}$**.**

7) (4p) För vilka $n \geq 3$ gäller att den fullständiga (kompletta) grafen K_n innehåller dels en hamiltoncykel och dels en sluten väg som saknar gemensamma kanter med hamiltoncykeln och går exakt en gång genom var och en av grafens övriga kanter?

K_n innehåller alltid en hamiltoncykel (eftersom det går kanter mellan alla par av hörn, kan man gå cykliskt genom alla hörn). Om man tar bort kanterna i den, återstår en graf som är sammanhängande om $n \geq 5$ (om $n = 3$ saknar den kanter) och varje hörn har valens $n - 3$. Problemet är när det finns en sluten eulerväg i den återstående grafen. Det gör det som bekant (en sats av Euler) om alla hörn har jämn valens, dvs
Svar: För udda $n \geq 5$. (Om man godtar en tom väg som sluten, går också $n = 3$ bra).

---

8) Permutationen $\pi \in S_9$ ges av att
$\pi(1)=6$, $\pi(2)=7$, $\pi(3)=1$, $\pi(4)=9$, $\pi(5)=5$, $\pi(6)=3$, $\pi(7)=2$, $\pi(8)=8$, $\pi(9)=4$.
a) (1p) Uttryck π i cykelnotation.
b) (3p) Hur många $\sigma \in S_9$ uppfyller $\sigma\pi = \pi^{-1}\sigma$ (dvs $\sigma\pi\sigma^{-1} = \pi^{-1}$)?

---

a) Eftersom $\pi(1) = 6$, $\pi(6) = 3$, $\pi(3) = 1$ etc, fås $\pi = (1\,6\,3)(2\,7)(4\,9)(5)(8)$.
b) $\sigma\pi\sigma^{-1} = (\sigma(1)\,\sigma(6)\,\sigma(3))(\sigma(2)\,\sigma(7))(\sigma(4)\,\sigma(9))(\sigma(5))(\sigma(8))$. För att den skall vara samma som $\pi^{-1} = (1\,3\,6)(2\,7)(4\,9)(5)(8)$ krävs att i-cykel svarar mot i-cykel osv. $\sigma(1)$ kan vara 1, 3 eller 6 (3 möjligheter), $\sigma(6)$, $\sigma(3)$ bestäms entydigt av $\sigma(1)$. $\sigma(2)$ kan vara 2, 7, 4 eller 9 (4 möjligheter), den bestämmer $\sigma(7)$, varefter $\sigma(4)$ har två möjliga värden, sedan är $\sigma(9)$ bestämd. $\sigma(5)$ kan vara 5 eller 8, $\sigma(8)$ då bestämd. Multiplikationsprincipen ger totalt $3 \cdot 1 \cdot 1 \cdot 4 \cdot 1 \cdot 2 \cdot 1 \cdot 2 \cdot 1 = 48$ möjliga σ.
Svar: a) $\pi = (1\,6\,3)(2\,7)(4\,9)(5)(8)$, b) Det finns 48 sådana σ.

---

9) Låt G vara en grupp.
a) (2p) Visa att om ekvationen $axbxa = x^{-1}$ har (minst) en lösning $x \in G$ för alla $a, b \in G$, så finns för varje $g \in G$ ett $c \in G$ så att $g = c^3$.
b) (3p) Visa omvändningen till a), dvs att om för varje $g \in G$ finns $c \in G$ med $g = c^3$, så finns för alla $a, b \in G$ (minst) ett $x \in G$ med $axbxa = x^{-1}$.

---

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 $g = c^3$. Med $g = a^{-1}b$ ger det att det finns $c \in G$ med $a^{-1}b = c^3$. Med $d = c^{-1}a^{-1}$, dvs $c = a^{-1}d^{-1}$, fås $a^{-1}b = (a^{-1}d^{-1})^3$. Multiplikation med ada från vänster och med da från höger ger $adbda = d^{-1}$, dvs ekvationen har en lösning ($x = d$) för alla $a, b \in G$, **saken är klar**.

---

10) Vid en tentamen med 10 uppgifter kan var och en av de sex första uppgifterna ge 0, 1 eller 2 poäng, medan de återstående fyra uppgifterna kan ge 0, 1, 2 eller 3 poäng.
a) (1p) Hur många olika poängfördelningar är möjliga?
b) (4p) Hur många av dem (fördelningarna i a)) har minst en uppgift vardera bedömd med 0, 1, 2 och 3 poäng?
(Svaren får innehålla fakulteter, heltalspotenser och de fyra vanliga räknesätten.)

---

a) Enligt multiplikationsprincipen finns $3^6 \cdot 4^4$ olika poängfördelningar.
b) Låt X vara mängden av alla fördelningarna i a) och A_i vara mängden av fördelningar där ingen uppgift getts i poäng. Vi söker $|X \setminus (A_0 \cup A_1 \cup A_2 \cup A_3)|$, som enligt principen om inklusion och exklusion är $|X| - (|A_0| + |A_1| + |A_2| + |A_3|) + (|A_{01}| + |A_{02}| + |A_{12}| + |A_{03}| + |A_{13}| + |A_{23}|) - (|A_{012}| + |A_{013}| + |A_{023}| + |A_{123}|) + |A_{0123}|$ (där A_{01} betecknar $A_0 \cap A_1$ och motsvarande). Enligt a) är $|X| = 3^6 \cdot 4^4$ och på samma sätt fås $|A_0| = |A_1| = |A_2| = 2^6 \cdot 3^4$, $|A_3| = 3^{10}$, $|A_{01}| = |A_{02}| = |A_{12}| = 1^6 \cdot 2^4$, $|A_{03}| = |A_{13}| = |A_{23}| = 2^{10}$, $|A_{012}| = 0$, $|A_{013}| = |A_{023}| = |A_{123}| = 1^{10}$, $|A_{0123}| = 0$, så det sökta antalet är (med ett par extra termer för systematiken) $3^6 \cdot 4^4 - 3 \cdot 2^6 \cdot 3^4 + 3 \cdot 1^6 \cdot 2^4 - 0^6 \cdot 1^4 - 3^{10} + 3 \cdot 2^{10} - 3 \cdot 1^{10} + 0^{10}$.
Svar: a) $3^6 \cdot 4^4 (= 186624)$ olika fördelningar,
b) $3^6 \cdot 4^4 - 3 \cdot 2^6 \cdot 3^4 + 3 \cdot 2^4 - 3^{10} + 3 \cdot 2^{10} - 3 (= 115140)$ olika fördelningar.
