KTH Matematik
B.Ek

Lösningar tentan SF1610(/5B1118) DISKRET MATEMATIK, CL m.fl., 31 maj 2010

Tryckfel kan förekomma.

1) (3p) Finn $\text{sgd}(392, 462)$ och heltal m, n så att $392m + 462n = \text{sgd}(392, 462)$.

Lösning: Med Euklides algoritm fås:

$$\begin{cases} 462 = 1 \cdot 392 + 70, \\ 392 = 5 \cdot 70 + 42 \\ 70 = 1 \cdot 42 + 28 \\ 42 = 1 \cdot 28 + 14 \\ 28 = 2 \cdot 14 + 0, \end{cases} \quad \text{så sgd är 14 och} \quad \begin{cases} 14 = 42 - 28 = \\ 42 - (70 - 42) = -70 + 2 \cdot 42 = \\ -70 + 2(392 - 5 \cdot 70) = 2 \cdot 392 - 11 \cdot 70 = \\ 2 \cdot 392 - 11(462 - 392) = -11 \cdot 462 + 13 \cdot 392. \end{cases}$$

Svar: $\mathbf{sgd(392, 462) = 14 = 392}\boldsymbol{m}\mathbf{ + 462}\boldsymbol{n}$ för (bl.a.) $\boldsymbol{m}\mathbf{ = 13}$, $\boldsymbol{n}\mathbf{ = -11}$.

---

2) (3p) Högst 100 identiska guldmynt skall delas ut till 20 (särskiljbara) barn, så att var och en får minst ett mynt. På hur många sätt kan det ske? Det totala antalet mynt som delas ut kan vara allt från 20 till 100.

Lösning: 20 mynt går till att ge alla varsitt. Sökta antalet är alltså = antalet sätt dela ut upp till 80 bland 20 barn = antalet sätt dela ut precis 80 bland 21 barn (ett fiktivt "21:a barn" får de överblivna mynten). 20 väggar kan utses bland $80 + 20 = 100$ på $\binom{100}{20}$ sätt.
Svar: Mynten kan fördelas på $\mathbf{\frac{100!}{20!80!}}$(= 535983370403809682970) sätt.

---

3) Låt G vara gruppen $(U(\mathbb{Z}_{30}), \cdot)$, dvs de inverterbara elementen i $\mathbb{Z}_{30}$ med operationen multiplikation.
a) (1p) Ange alla element i G.
b) (2p) Är G en cyklisk grupp? Finn i så fall ett genererande element för G.

Lösning: $U(\mathbb{Z}_{30}) = \{r \in \{0, 1, 2, \ldots, 29\} \mid \text{sgd}(r, 30) = 1\} = \{1, 7, 11, 13, 17, 19, 23, 29\}$, så $|U(\mathbb{Z}_{30})| = 8$ och G är cyklisk omm något element har ordning $8 = 2^3$.
Man finner $1^2 = 29^2 = 1$, $7^2 = 23^2 = 19$, $11^2 = 19^2 = 1$, $13^2 = 17^2 = 19$, så
$o(1) = 1$, $o(11) = o(19) = o(29) = 2$, $o(7) = o(13) = o(17) = o(23) = 4$.
Svar: a) $\boldsymbol{U(\mathbb{Z}_{30}) = \{1, 7, 11, 13, 17, 19, 23, 29\}}$, b) $\boldsymbol{G}$ är inte cyklisk.

---

4) En linjär binär kod ges av kontrollmatrisen $H = \begin{bmatrix} 1&0&1&1&0&0&1 \\ 1&1&0&1&0&1&0 \\ 0&0&1&1&1&1&0 \end{bmatrix}$.
a) (1p) Vilket kodord kan med högst ett fel bli 1010101?
b) (2p) Finn x, y så att $10xy001$ är ett kodord.

Lösning: $H(1010101)^T = (110)^T = H$:s kolonn 1, så bit 1 fel, det sökta ordet är 0010101.
$H(10xy001)^T = (000)^T$ precis om $x\cdot$(kolonn 3)+$y\cdot$(kolonn 4)= $(010)^T$, vilket ger $x = y = 1$.
Svar: a) Det sökta kodordet är 0010101, b) $\boldsymbol{x = y = 1}$ ger kodordet 1011001.

---

5) (3p) Grafen $G = (V, E)$ är sammanhängande och reguljär (dvs alla hörn har samma valens (grad)) och har 147 hörn, $|V| = 147$. Avgör (med motivering) om G måste vara eulersk (dvs ha en eulerkrets).

Lösning: Om hörnens gemensamma valens kallas d fås $147d = \sum_{x \in V} \delta(x) = 2|E|$ ("handslagslemmat"), så d är ett jämnt tal. G är alltså en sammanhängande graf där alla hörn har jämn valens, så den är eulersk. **Svar: Grafen är säkert eulersk.**

---

6) (4p) Visa att $371 \mid 7n^{53} + 53n^7 - 60n$ för alla $n \in \mathbb{Z}$. $(371 = 7 \cdot 53.)$

Lösning: Enligt Fermats lilla sats är $n^7 \equiv n \pmod 7$ och $n^{53} \equiv n \pmod{53}$ (7 och 53 är ju primtal), dvs $n^7 - n = 7x$, $n^{53} - n = 53y$ för några $x, y \in \mathbb{Z}$, så $7n^{53} + 53n^7 - 60n = 7(n^{53} - n) + 53(n^7 - n) = 7 \cdot 53y + 53 \cdot 7x = 371(x + y)$. Påståendet följer, **saken är klar.**

---

7) Låt A och B vara (icke-tomma) mängder och f en funktion, $f : A \to B$. Vi säger att f har en **vänsterinvers** om det finns $g : B \to A$ så att den sammansatta funktionen $g \circ f = id_A$, där $id_A : A \to A$ är identitetsfunktionen på A, $id_A(a) = a$ för alla $a \in A$.
a) (1p) Har $s : \mathbb{N} \to \mathbb{N}$, där $s(n) = n + 1$ för $n \in \mathbb{N}$, någon vänsterinvers?
b) (3p) Finn ett enkelt nödvändigt och tillräckligt villkor för att $f : A \to B$ skall ha en vänsterinvers.

Lösning: $t : \mathbb{N} \to \mathbb{N}$, där $t(n) = \max(n - 1, 0)$ för $n \in \mathbb{N}$ uppfyller$(t \circ s)(n) = t(n + 1) = n + 1 - 1 = n$ för alla $n \in \mathbb{N}$, så $t \circ s = id_{\mathbb{N}}$.
Om $f : A \to B$ har vänsterinversen g, gäller för $c \neq d$ i A att $g(f(c)) = c \neq d = g(f(d))$, så $f(c) \neq f(d)$. f är alltså injektiv.
Om å andra sidan f är injektiv, definiera $g : B \to A$ enligt $g(b) = a$ om $b = f(a)$ för ett $a \in A$ (entydigt p.g.a. injektiviteten), $g(b) =$ något $a_0 \in A$ annars. Tydligen gäller då $(g \circ f)(a) = g(f(a)) = a$ för alla $a \in A$, så g är en vänsterinvers.
Svar: a) Ja, s har en vänsterinvers, b) f har en vänsterinvers omm f är injektiv.

---

8) (4p) Visa att en sammanhängande graf där varje hörn har valens (grad) minst 4 och alla cykler har längd minst 4, inte kan vara planär.

Lösning: Låt $G = (V, E)$ uppfylla villkoren och antag att G är planär. "Handslagslemmat" ger $2e = 2|E| = \sum_{x \in V} \delta(x) \geq 4|V| = 4v$. Om antalet ytor då G ritas plant är r fås analogt (då man summerar ytornas kantantal (≥ 4, ju) räknas varje kant 2 gånger) $2e \geq 4r$. Så $v, r \leq \frac{e}{2}$, men för en plan sammanhängande graf gäller (Euler) att $v - e + r = 2$. Det skulle ge $2 \leq \frac{e}{2} - e + \frac{e}{2} = 0$, motsägelse, så G är inte plan. **Saken är klar.**

---

9) Man har n st svarta, inte särskiljbara, kulor och $2n + 1$ st med andra, olika, färger och väljer (oordnat) ut n st av dem.
a) (2p) Visa att antalet sätt det kan ske är $\binom{2n+1}{0} + \binom{2n+1}{1} + \ldots + \binom{2n+1}{n}$.
b) (3p) Ge (med motivering) ett slutet uttryck för summan i a). Uttrycket får bara innehålla n, heltal, potenser och de fyra vanliga räknesätten.

Lösning: Valet beskrivs fullständigt av vilka $k(= 0, 1, \ldots, n)$ icke-svarta kulor som väljs (resten är svarta). k st kan (oordnat) väljas bland $2n + 1$ st (särskiljbara) på $\binom{2n+1}{k}$ sätt. Olika k ger disjunkta mängder val, så med additionsprincipen fås: **Saken i a) är klar.**
Eftersom $\binom{2n+1}{k} = \binom{2n+1}{2n+1-k}$ är den givna summan
$= \frac{1}{2}\left(\binom{2n+1}{0} + \binom{2n+1}{1} + \ldots + \binom{2n+1}{n} + \binom{2n+1}{n+1} + \cdots + \binom{2n+1}{2n} + \binom{2n+1}{2n+1}\right) = \frac{1}{2}(1 + 1)^{2n+1} = \frac{1}{2} \cdot 2^{2n+1} = 2^{2n}$ (binomialsatsen gav tredje '=' från slutet).
Svar b): Antalet sätt att välja dem är 2^{2n}.

---

10) Låt $X = \{1, 2, 3, \ldots, n\}$ och A vara en delmängd till X, $A \subseteq X$.
Låt $H \subseteq S_n$ bestå av de permutationer av X som tar alla element i A till element i A, $H = \{\pi \in S_n \mid \pi(a) \in A \text{ för alla } a \in A\}$.
a) (2p) Visa att H är en delgrupp till S_n.
b) (1p) Om $|A| = m$, vad är $|H|$, H:s ordning (uttryckt i m och n)?
c) (2p) Beskriv H:s vänstersidoklasser $\tau H = \{\tau\pi \mid \pi \in H\}$ och högersidoklasser $H\tau$ (för $\tau \in S_n$).

Lösning: Eftersom S_n är ändlig räcker det i a) att visa att $H \neq \varnothing$ och $\pi, \tau \in H \Rightarrow \pi\tau \in H$. $id \in H$, så $H \neq \varnothing$ och $\pi, \tau \in H$, $a \in A$ ger $\tau(a) \in A$, så $(\pi\tau)(a) = \pi(\tau(a)) \in A$ och $\pi\tau \in H$. **Saken i a) är klar.** Element i H permuterar A och $X \setminus A$ var för sig godtyckligt. Multiplikationsprincipen ger att $|H| = m!\,(n - m)!$.
Om $A' \subseteq X$ och $|A'| = |A| = m$ finns $\tau \in S_n$ med $\tau(A)(= \{\tau(a) \mid a \in A\}) = A'$ och för $\pi \in H$, $a \in A$ fås $\pi(a) \in A$, så $\tau\pi(a) \in A'$. Om $\sigma \in S_n$ är sådan att $\sigma(a) \in A'$ för alla $a \in A$ fås $\tau^{-1}\sigma(a) \in A$, så $\tau^{-1}\sigma \in H$ och $\sigma \in \tau H$. **Varje vänstersidoklass till H beskrivs entydigt av ett $A' \subseteq X$ med $|A'| = m$: $\tau H = \{\sigma \in S_n \mid a \in A \Rightarrow \sigma(a) \in A'\}$, $\tau(A) = A'$.** "P.s.s." fås att **Varje högersidoklass till H beskrivs entydigt av ett $A'' \subseteq X$ med $|A''| = m$: $H\tau = \{\sigma \in S_n \mid b \in A'' \Rightarrow \sigma(b) \in A\}$, $\tau^{-1}(A) = A''$.**
Svar: b) $|H| = m!\,(n - m)!$, c) Sidoklasserna τH och $H\tau$ som ovan.
