Matematiska Institutionen
KTH

Tentamensskrivning i Diskret Matematik för CINTE och CMETE, SF1610, onsdagen den 20 augusti 2014, kl 14.00-19.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (**OBS:** Totalsumma poäng vid denna tentamensskrivning är 36p.)

13	poäng totalt eller mer ger minst omdömet	Fx
15	poäng totalt eller mer ger minst betyget	E
18	poäng totalt eller mer ger minst betyget	D
22	poäng totalt eller mer ger minst betyget	C
28	poäng totalt eller mer ger minst betyget	B
32	poäng totalt eller mer ger minst betyget	A

Observera: Generellt gäller att för full poäng krävs korrekta och väl presenterade resonemang.

DEL I

Var och en av nedanstående uppgifter svarar mot en kontrollskrivning. Godkänt resultat på kontrollskrivning nr. i under läsåret 2013-2014 ger automatiskt full poäng på uppgift nr. i. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Den oändliga talföljden a_0, a_1, a_2, ... definieras rekursivt genom sambandet

$$a_n = 2a_{n-1} + 8a_{n-2}\,, \qquad \text{för} \qquad n = 2, 3, \ldots$$

där $a_0 = 2$ och $a_1 = 2$. Visa med ett induktionsbevis att

$$a_n = 4^n + (-2)^n$$

för $n = 0, 1, 2, 3, \ldots$.

Lösning. Vi sätter $b_n = 4^n + (-2)^n$ och skall visa att den rekursivt definierade talföljden a_n satisfierar $a_n = b_n$ för $n = 0, 1, 2, \ldots$. Vi visar att om för talet n gäller att $a_{n-1} = b_{n-1}$ och $a_{n-2} = b_{n-2}$ så gäller att $a_n = b_n$:

$$a_n = 2a_{n-1} + 8a_{n-2} = 2b_{n-1} + 8b_{n-2} = 2(4^{n-1} + (-2)^{n-1}) + 8(4^{n-2} + (-2)^{n-2}) =$$

$$= 8 \cdot 4^{n-2} - 4(-2)^{n-2} + 8(4^{n-2} + (-2)^{n-2}) = 16 \cdot 4^{n-2} + 4(-2)^{n-2} = 4^n + (-2)^n = b_n.$$

Eftersom $a_0 = 2 = b_0$ och $a_1 = 2 = b_1$ så följer nu enligt induktionsprincipen att $a_n = b_n$ för $n = 0, 1, 2, \ldots$.

2. (3p) På hur många olika sätt kan 13 röda bollar och 13 blå bollar fördelas bland fyra flickor och fyra pojkar så att varje pojke får minst en blå boll och varje flicka får minst en röd boll. (Svaret skall skrivas som produkter, summor, skillnader och kvoter mellan hela tal.)

Lösning. Efter att varje flicka fått en röd boll och varje pojke fått en blå boll återstår nio röda och nio blå bollar att fördela bland de åtta barnen. De röda bollarna betraktas som identiska objekt och kan då fördelas på

$$\binom{9+8-1}{8-1}$$

olika sätt. Lika många fördelningar finns av de blå bollarna. Multiplikationsprincipen ger nu

SVAR:

$$\binom{9+8-1}{8-1}\binom{9+8-1}{8-1} = \left(\frac{16\cdot 15\cdot 14\cdot 13\cdot 12\cdot 11\cdot 10}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7}\right)^2$$

3. Betrakta gruppen $\mathcal{S}_7$ bestående av alla permutationer av elementen i mängden $\{1, 2, \ldots, 7\}$. Låt $\varphi = (1\ 2\ 4\ 5\ 6)$ och $\psi = (1\ 3\ 6\ 7)$.

   (a) (1p) Bestäm ordningen av permutationen $\varphi\psi$

   Lösning. Ordningen av en permutation kan beräknas som minsta gemensamma multipeln av de cykellängder som uppstår när permutationen skrivs som en produkt av disjunkta cykler. Vi finner

   $$\varphi\psi = (1\ 2\ 4\ 5\ 6)(1\ 3\ 6\ 7) = (1\ 3)(2\ 4\ 5\ 6\ 7)$$

   SVAR: Ordningen av $\varphi\psi$ är 10.

   (b) (2p) För vilka positiva heltal n, m och k är permutationen $\varphi^n\psi^m\varphi^k$ en udda permutation?

   Lösning. Eftersom φ är en produkt av ett jämnt antal 2-cykler, t ex

   $$(1\ 2\ 4\ 5\ 6) = (1\ 6)(1\ 5)(1\ 4)(1\ 2)$$

   så är φ en jämn permutation. Pss är ψ en udda permutation. Produkter av jämna permutationer är en jämn permutation, en produkt av två udda permutationer är en jämn permutation, men en produkt av en udda permutation och en jämn permutation är en udda permutation. Detta ger

   SVAR: $\varphi^n\psi^m\varphi^k$ en udda permutation precis när m är ett udda tal.

4. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 111$ och $e = 29$. Dekryptera meddelandet $b = 5$, (dvs bestäm $D(5)$).

   Lösning. Vi lyckas faktorisera $n = 111 = 3\cdot 37$ och kan då beräkna $m = (3-1)(37-1) = 72$. Vi vet att den dekrypterande nyckeln d satisfierar ekvationen $e\cdot d \equiv 1 (\text{mod } m)$. Euklides algoritm

   $$72 = 3\cdot 29 - 15, \qquad 29 = 2\cdot 15 - 1$$

   ger

   $$1 = 2\cdot 15 - 29 = 2(3\cdot 29 - 72) - 29 = 5\cdot 29 - 2\cdot 72$$

   varur vi får att $29\cdot 5 \equiv 1 (\text{mod } 72)$. Vi vet att $D(5) = 5^d (\text{mod } n)$:

   $$D(5) = 5^5 \equiv_{111} 5^3 5^2 \equiv_{111} 125\cdot 25 \equiv_{111} 14\cdot 25 \equiv_{111} 350 \equiv_{111} 17.$$

   SVAR: $D(5) = 17$.

5. (3p) Om exakt två av noderna i en graf G har udda valens (grad) så finns en stig mellan dessa två noder. Förklara varför.

   Lösning. Vi delar in grafen G i komponenter K_1, ..., K_t. I varje komponent K_i gäller att summan av valenserna av noderna i K_i är lika med två gånger antalet kanter. Antal noder med udda valens i en komonent K_i måste då vara jämnt. En komponenten K_i kan då inte ha precis en nod med udda valens. De två noderna i G med udda valens måste då tillhöra samma komponent K_i. En komponent i grafen G är en saammanhängande delgraf till G och då finns en stig mellan varje par av noder i delgrafen, speciellt finns då en stig mellan de två noderna med udda valens i K_i.

DEL II

6. (3p) På hur många olika sätt kan de sju flickorna F_1, ..., F_7 och de sju pojkarna P_1, ..., P_7 delas in i fyra grupper, grupp 1, grupp 2, grupp 3 och grupp 4, så att varje grupp kommer att innehålla minst en flicka och minst en pojke. (Svaret skall skrivas som produkter, summor, skillnader och kvoter mellan hela tal.)

   Lösning. Vi använder inklusion exklusion för att lösa problemet. Först till flickorna. Låt A_i beteckna mängden fördelningar där grupp nummer i saknar en flicka. Vi finner att $|A_1| = 3^7$ eftersom var och en av de sju flickorna då fritt kan välja grupp 2, 3 eller 4. Likaledes för $i, j, k \in \{1, 2, 3, 4\}$ med $i \neq j$, $i \neq k$ och $j \neq k$:

$$|A_i| = 3^7, \qquad |A_i \cap A_j| = 2^7, \qquad |A_i \cap A_j \cap A_k| = 1^7$$

   Inklusion exklusion ger nu att antalet sätt att fördela flickorna är

$$4^7 - 4 \cdot 3^7 + \binom{4}{2} 2^7 - \binom{4}{3} 1^7 = 4^7 - 4 \cdot 3^7 + 6 \cdot 2^7 - 4.$$

   Pojkarna kan fördelas på lika många sätt så, enligt multiplikationsprincipen,

   SVAR: $(4^7 - 4 \cdot 3^7 + 6 \cdot 2^7 - 4)^2$

7. (a) (3p) Visa att i en abelsk (kommutativ) grupp $(G, \circ)$, med identitetselementet e, så gäller att mängden

$$H = \{g \in G \mid g \circ g \circ g \circ g = e\}$$

   bildar en delgrupp till gruppen $(G, \circ)$.

   Lösning. Identitetselementet tillhör H eftersom

$$e \circ e \circ e \circ e = e.$$

   Mängden H är sluten eftersom, då G är abelsk,

$$g, h \in H \quad \Rightarrow \quad g \circ g \circ g \circ g \circ h \circ h \circ h \circ h = e \circ e \quad \Rightarrow \quad (g \circ h) \circ (g \circ h) \circ (g \circ h) \circ (g \circ h) = e.$$

   Vidare gäller

$$g \circ g \circ g \circ g = e \quad \Rightarrow \quad e = g^{-1} \circ g^{-1} \circ g^{-1} \circ g^{-1} \circ g \circ g \circ g \circ g = g^{-1} \circ g^{-1} \circ g^{-1} \circ g^{-1} \circ e,$$

   så inversen i G till varje element i H tillhör H. Associativa lagen gäller generellt i H och därför speciellt i H.

   (b) (2p) Visa, t ex med hjälp av ett exempel, att detta inte alltid är sant om gruppen inte är abelsk (kommutativ).

   Lösning. Vi betraktar gruppen $G = \mathcal{S}_3$ bestående av permutationerna av elementen i mängden $\{1, 2, 3\}$. I $\mathcal{S}_3$ gäller att

$$H = \{g \in G \mid g \circ g \circ g \circ g = e\} = \{(1), (1\ 2), (1\ 3), (2\ 3)\},$$

   men $(1\ 2)(2\ 3) = (1\ 2\ 3)$ som inte tillhör H. Mängden H är alltså inte sluten med avseende på gruppoperationen i G, och kan då inte vara en delgrupp till G.

8. (3p) Du får följande information om koden C: koden C är 1-felsrättande, antal ord i koden är $|C| = 16$, koden C är linjär (dvs om orden $\bar{c}$ och $\bar{c}'$ tillhör C så gäller att också ordet $\bar{c} + \bar{c}'$ tillhör C),

$$\{1111111, 1110000, 1001001, 0100011\} \subseteq C$$

   Undersök om ordet 0111110 tillhör koden C eller om det kan rättas till ett ord i C, eller varken eller? (Bristfällig motivering ger poängavdrag).

Lösning. Eftersom koden är 1-fels-rättande är minsta avstånd mellan kodord lika med 3. Det givna ordet 0111110 ligger på avståndet 2 från ordet 1111111 i C och alltså kan inte ordet 0111110 tillhöra C. Men ligger det på avstånd 1 från något kodord, dvs skulle ordet vara möjligt att rätta?

Ordens längd är 7 och då finns precis 7 ord på avstånd 1 från varje enskilt kodord. Eftersom koden är 1-fels-rättande ligger inget ord på avstånd 1 från två olika kodord. Alltså är antal ord på avstånd 1 från kodord lika med sju gånger antalet ord i koden, dvs totalt $7 \cdot 16 = 112$. Totalt finns $2^7 = 128$ ord av längd 7, och resterande $128 - 112 = 16$ ord är orden i C. Varje ord, inklusive det givna ordet 0111110, är allså antingen ett kodord eller går arr rätta till ett kodord.

DEL III

Om du i denna del använder eller hänvisar till satser från läroboken skall dessa citeras, ej nödvändigvis ordagrant, där de används i lösningen.

9. (5p) En funktion f från mängden $\{0, 1, 2, \ldots, a\}$ till den direkta produkten

$$Z_b \times Z_c = \{(x_1, x_2) \mid x_1 \in Z_a,\ x_2 \in Z_b\}$$

av ringarna Z_b och Z_c definieras av

$$f(x) = (x(\mathrm{mod}\ b), x(\mathrm{mod}\ c)).$$

För vilka heltal $a > 1$, $b > 1$ och $c > 1$ gäller att funktionen f är injektiv, surjektiv och/eller bijektiv?

Lösning. Vi börjar med att avgöra injektiviteten. Vi finner att

$$f(x) = f(x') \quad \Longleftrightarrow \quad \begin{cases} x(\mathrm{mod}\ b) &= x'(\mathrm{mod}\ b), \\ x(\mathrm{mod}\ c) &= x'(\mathrm{mod}\ c) \end{cases} \quad \Longleftrightarrow \quad \begin{cases} x - x' &\equiv 0\,(\mathrm{mod}\ b), \\ x - x' &\equiv 0\,(\mathrm{mod}\ c). \end{cases}$$

Så $f(x) = f(x')$ om och endast om $M = \mathrm{mgm}(b, c)$ delar $x - x'$. Alltså, om $a < M$ så är f injektiv, men om $a \geq M$ är f inte injektiv eftersom $f(0) = f(M)$.

Nu till surjektiviteten. Vi obeserverar att $|Z_b \times Z_c| = bc$ och att $M = bc/\mathrm{sgd}(b, c)$.

Vi betraktar först fallet $\mathrm{sgd}(b, c) = 1$. Om $a \leq M - 1$ är f en injektiv funktion från mängden $\{0, 1, \ldots, a\}$ med $a + 1$ stycken element till mängden $Z_b \times Z_c$ med bc stycken element. Funktionen f är då i detta fall surjektiv om $a + 1 = M = bc$. Om $a < M - 1$ kan f inte vara surjektiv, men om $a \geq M - 1$ och $\mathrm{sgd}(b, c) = 1$ så är f också surjektiv, eftersom f avbildar delmängden $\{0, 1, 2, \ldots, bc - 1\}$ till mängden $\{0, 1, 2, \ldots, a\}$ då "surjektivt" på $Z_b \times Z_c$.

I fallet $\mathrm{sgd}(b, c) > 1$ är funktionen f aldrig surjektiv. Detta beror på att dels $f(x) = f(x + M)$ för alla heltal x, eftersom

$$f(x + M) = (x + M(\mathrm{mod}\ b), x + M(\mathrm{mod}\ c)) = (x(\mathrm{mod}\ b), x(\mathrm{mod}\ c)) = f(x), \tag{1}$$

samt att

$$|\{0, 1, \ldots, M - 1\}| < |Z_b \times Z_c|.$$

Så om $\mathrm{sgd}(b, c) > 1$ finns det $(x_1, x_2) \in Z_b \times Z_c \setminus f(\{0, 1, \ldots, M - 1\})$ sådant att

$$f(x) \neq (x_1, x_2)$$

för alla $x \in \{0, 1, \ldots, M - 1\}$, och enligt ekvation (1) finns då inget heltal x sådant att $f(x) = (x_1, x_2)$.

10. Grafen G består av två disjunkta nodmängder X och Y, och varje kant i G har sin ena ändpunkt i nodmängden X och den andra ändpunkten i nodmängden Y.

(a) (3p) Visa att om alla noder i grafen G har valensen (graden) 3 så kan kanterna i G tilldelas värdena 0 eller 1 på ett sådant sätt att vid varje nod så kommer precis en kant med värdet 0 och två kanter med värdet 1 att inträffa.

Lösning. Se nedan:

(b) (2p) Formulera och bevisa ett generellare påstående än det ovan angivna.

Lösning. Visar påståendet:

Om alla noder i grafen G har valensen (graden) k så kan kanterna i G tilldelas värdena 0 eller 1 på ett sådant sätt att vid varje nod så kommer precis $0 \leq s \leq k$ kanter med värdet 0 och $k - s$ kanter med värdet 1 att inträffa.

Låt A vara en godtycklig delmängd till X och $J(A)$ de noder i Y som är grannar med någon nod i A. Antal kanter som utgår från noder i A är lika med $k|A|$, antal kanter som utgår från noder i $J(A)$ och går till noder i A är högst $k|J(A)|$ eftersom högst k kanter från noder i $J(A)$ går mot kanter i A. Således

$$k|A| \leq k|J(A)|,$$

varur följer att Halls villkor är uppfyllt för varje delmängd A till X. Enligt Halls bröllopssats finns då en komplett matchning av kanter. Med $A = X$ får vi $J(A) = Y$ och också att $|X| = |Y|$ (eftersom $k|X| = k|J(X)| = k|Y|$). Färga kanterna i matchningen med färgen 0, och ta bort dessa kanter. I den resterade grafen har varje nod valensen $k-1$ och vi kan upprepa förfarandet ovan och rekursivt tilldela $s-1$ av de återstående kanterna med färgen 0 och $k-s$ av resterande kanter med färgen 1.