Matematiska Institutionen
KTH

Tentamensskrivning i Diskret Matematik, SF1610 och 5B1118, torsdagen den 21 oktober 2010, kl 14.00-19.00.

Examinator: Olof Heden.

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng är 36p.)

12	poäng totalt eller mer ger minst omdömet	Fx
15	poäng totalt, varav minst 12 poäng på del I, eller mer ger minst betyget	E
18	poäng totalt, varav minst 12 poäng på del I, eller mer ger minst betyget	D
22	poäng totalt, varav minst 12 poäng på del I, eller mer ger minst betyget	C
28	poäng totalt, varav minst 12 poäng på del I, eller mer ger minst betyget	B
32	poäng totalt, varav minst 12 poäng på del I, eller mer ger minst betyget	A

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

DEL I

OBS: Godkänt resultat på kontrollskrivning nr i, för $i = 1, 2, \ldots, 5$, ger automatiskt full poäng på uppgift nr i. Att lösa en uppgift som man på detta sätt redan har tillgodo ger inga extra poäng.

1. (3p) Lös ekvationen $13x + 18 = 13$ i ringen Z_{64}.

2. (3p) Man skall i en klass med 12 elever utse en kommitté bestående av 5 elever, men om eleven A väljs till kommittén så kan inte eleven B vara med i kommittén. Hur många olika kommittéer kan utses. Svaret skall ges i formen av ett heltal.

3. (3p) Låt φ beteckna den permutation på mängden $\{1, 2, 3, 4, 5, 6, 7\}$ som kan beskrivas med produkten
$$\varphi = (1\ 2\ 3\ 4\ 5)(1\ 7\ 6\ 5)(1\ 3\ 5\ 7)\ .$$
   (a) (2p) Skriv φ som en produkt av disjunkta cykler.
   (b) (1p) Är φ en udda eller en jämn permutation.

4. (3p) Den 1-felsrättande koden C har kontrollmatrisen
$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$
   (a) (1p) Bestäm antalet ord i C.
   (b) (1p) Bestäm två ord i C.
   (c) (1p) "Rätta" ordet 1110110.

5. (3p) Rita en graf med 7 noder och 12 kanter som har en Hamiltoncykel men saknar en Eulerkrets. Glöm ej att motivera ditt svar!

DEL II

6. En klass med de 12 eleverna A_1, A_2, ..., A_{12} skall dels in i tre grupper, den röda, den blå och den gula gruppen, och på ett sådant sätt att A_1, A_2 och A_3 kommer i olika grupper. På hur många sätt kan detta ske om

   (a) (1p) De tre grupperna är lika stora.

   (b) (1p) En av grupperna består av 3 elever, en annan grupp av 4 elever, och en grupp består av 5 elever.

   (c) (1p) Två av grupperna består av 3 elever vardera och en tredje grupp betstår av 6 elever.

   (d) (1p) Ordna de tre svaren ovan i storleksordning.

   Anm: Svaren till uppgift a), b) och c) får innehålla alla beteckningar, typ binomialkoefficienter och fakulteter, som presenterats under kursen.

7. (3p) Bestäm antalet Booleska funktioner $f(x, y, z, w)$ i de tre variablerna x, y, z och w som satisfierar likheten

$$f(1,0,1,0)f(0,1,1,1) + f(1,1,1,1) = 1 \ .$$

8. (4p) Antag att a, b och c är olika heltal sådana att $\text{sgd}(a,b) = \text{sgd}(a,c) = D$. Bevisa att D delar $\text{sgd}(b,c)$ och beskriv, med en motivering, under vilka förutsättningar som $\text{sgd}(b,c) = D$.

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. En grupp $\mathcal{G}$ med en delgrupp $\mathcal{H}$ definierar tillsammans en graf $G(V, E)$ vars noder V är elementen i $\mathcal{G}$, och det finns en kant mellan noderna $g, g' \in \mathcal{G}$ precis då $g' = hg$ för något element h i $\mathcal{H}$.

   (a) (1p) Rita en sådan graf G när $\mathcal{G}$ är en cyklisk grupp med 20 element och $\mathcal{H}$ en delgrupp till $\mathcal{G}$ med 5 element.

   (b) (2p) Vad kan sägas generellt om den graf som en grupp $\mathcal{G}$ tillsammans med en delgrupp $\mathcal{H}$ på detta sätt definierar, t ex vad avser antal komponenter, valensen hos grafens noder respektive under vilka förutsättningar grafen är planär.

   (c) (2p) Kan icke isomorfa grupper ha isomorfa grafer? Motivera ditt svar!

10. (5p) I ett RSA-krypto räknar man ju modulo ett tal n som är en produkt av två olika primtal. Under vilka förutsättningar är det möjligt att generalisera RSA-kryptot så att n blir en produkt av tre primtal, men så att för övrigt fungerar kryptot som det traditionella RSA-kryptot.

    Diskutera en möjlig generalisering utifrån ett matematiskt perspektiv. Diskutera också om ett sådant krypto skulle vara lättare eller svårare att avslöja än det traditionella RSA-kryptot.