Matematiska Institutionen
KTH

Lösning till 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}.

   Lösning: Eftersom
   $$5 \cdot 13 = 65 \equiv 1 \pmod{64}$$
   så $13^{-1} = 5$ i ringen Z_{64}. Alltså
   $$13x + 18 = 13 \;\Leftrightarrow\; 13x = 13 - 18 \;\Leftrightarrow\; x = 13^{-1}(-5) \;\Leftrightarrow\; x = -25\,.$$
   Men $-25 + 64 = 39$ så

   Svar: $x = 39$.

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.

   Lösning: Vi delar in i olika fall beroende på om A är med i kommittén eller ej med i kommittén.

   Fall 1: A är med. Då skall vi välja ut ytterligare 4 elever, men bland 10 elever, de 12 utom A och B. Antal sätt detta går på är
   $$\binom{10}{4} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 4} = 210\,.$$

Fall 2: A är inte med. Då skall 5 elever väljas bland alla 11 övriga elever. Antal sätt detta går på är

$$\binom{11}{5} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 462$$

Svar: 672

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.

   Lösning:

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

   (b) (1p) Är φ en udda eller en jämn permutation.

   Lösning: Till exempel har vi

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

   så φ är en produkt av fyra transpositioner och därmed
   Svar: Permutationen är jämn.

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.

   Lösning: Enligt känd formel har vi

$$|C| = 2^{7-3} = 16\ .$$

   (b) (1p) Bestäm två ord i C.

   Lösning: Ett ord är nollordet 0000000 och eftersom summan av de tre första kolonnerna är nollkolonnen så är även ordet 1110000 ett kodord.

   (c) (1p) "Rätta" ordet 1110110.

   Lösning: Vi finner att

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

vilket är den andra kolonnen i matrisen H. Vid informationsöverföringen så uppstod alltså ett fel i andra positionen. Vi rättar och får

Svar: 1010110

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!

   Lösning: Rita till exempel först en cykel med 7 noder och 7 kanter. Återstår 5 kanter att rita ut. Från tre av noderna v_1, v_2 och v_3 rita kanter till de övriga fyra enligt följande. Från v_1 och v_2 drag tre kanter och från v_3 en kant.

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.

   Lösning: Välj först grupp åt eleverna A_1, A_2 och A_3 vilket kan ske på 3! olika sätt. Resterande nio elever skall nu delas in i tre etiketterade delgruper med 3 elever vardera. Antalet sätt detta kan ske på är

   $$\binom{9}{3,3,3}.$$

   Multiplikationsprincipen ger nu

   Svar:

   $$3! \cdot \binom{9}{3,3,3}.$$

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

   Lösning: Vi skall först bestämma vilka av gruperna med färg som skall ha 3, 4 resp 5 elever. Detta kan ske på 3! olika sätt. Sen skall eleverna A_1, A_2 och A_3 fördelas i tre olika grupper.

   Sen delar vi upp de övriga eleverna i de olika grupperna. Antalet sätt detta kan ske på är

   $$\binom{9}{2,3,4}.$$

   Multiplikationsprincipen ger nu

   Svar:

   $$3! \cdot 3! \cdot \binom{9}{2,3,4}.$$

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

Lösning: Först bestämmer vi vilken färg som gruppen med 6 elever skall ha. Detta kan ske på 3 olika sätt. Sen skall eleverna A_1, A_2 och A_3 fördelas i tre olika grupper.

Sen delar vi upp de övriga eleverna i de olika grupperna. Antalet sätt detta kan ske på är

$$\binom{9}{2,2,5}.$$

Multiplikationsprincipen ger nu

Svar:

$$3 \cdot 3! \cdot \binom{9}{2,2,5}.$$

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

Lösning: Vi skall jämföra de tre talen

$$A = 3!\binom{9}{3,3,3} = \frac{3! \cdot 9!}{3! \cdot 3! \cdot 3!}, \quad B = 3! \cdot 3! \cdot \binom{9}{2,3,4} = \frac{3! \cdot 3! \cdot 9!}{2! \cdot 3! \cdot 4!},$$

och

$$C = 3 \cdot 3! \cdot \binom{9}{2,2,5} = \frac{3 \cdot 3! \cdot 9!}{2! \cdot 2! \cdot 5!}.$$

Vi finner att

$$\frac{A}{B} = \frac{4}{18}, \quad \text{och} \quad \frac{A}{C} = \frac{4}{27/5}.$$

Ur detta ser vi, genom att jämföra täljare och nämnare i bråken ovan, att

Svar: $A < C < B$.

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

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

Lösning: Vi sorterar de olika Booleska funktioner som satisfierar ekvationen i olika listor:

Fall 1: $f(1,1,1,1) = 1$ och då kan de övriga $2^4 - 1 = 15$ olika funktionsvärdena väljas godtyckligt till 0 eller 1, så denna lista kommer att innehålla 2^{15} olika funktioner.

Fall 2: $f(1,1,1,1) = 0$ men då måste $f(1,0,1,0) = f(0,1,1,1) = 1$ så det återstår nu 13 funktionsvärden att ange och därmed finns det totalt 2^{13} funktioner i denna lista.

Svar: $2^{15} + 2^{13}$ som ju är lika med $2^{12} \cdot 2 \cdot (2^2 + 1) = 10 \cdot 2^{12} = 40960$.

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 $\text{sgd}(b,c) = D$.

   Lösning: Förutsättningarna ger att D delar dels både a och b, eftersom $D = \text{sgd}(a,b)$, och likaledes D delar a och c. Således delar D både b och c och då par definition också $\text{sgd}(b,c)$, vilket skulle visas.

   Den andra frågan utgick men här kommer ett svar. Det enda som man kan säga är att

$$\text{sgd}(\frac{b}{D}, \frac{c}{D}) = 1 \ ,$$

   ty om vi hittar ett primtal p som delar både b/D och c/D skulle pD dela både b och c och D skulle inta vara lika med $\text{sgd}(b,c)$.

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.

   Lösning: Vi får en graf med fyra komponenter, med som noder elementen i de fyra sidoklasserna, och i varje komponent har vi kanter mellan alla noder, samt en loop vid varje nod.

   (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.

   Lösning: Antal komponenter är lika med antalet sidoklasser, valensen vid varje nod är lika med $|H| + 1$, eftersom varje element i H bidrar med en kant utfrån varje nod, men identiteten ger en loop som ger bidraget 2 till valensen vid noden. Grafen är planär precis då $|H| < 5$, enligt Kuratowskis sats, eftersom varje komponent kan betraktas som en komplett graf utökad med loopar vid varje nod.

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

   Lösning: Ja, det finns grupper som är lika stora och som har delgrupper so är lika stora, till exempel mängden av permutationer av mängden $\{1,2,3\}$ utgör en icke abelsk grupp $G = \mathcal{S}_3$ med 6 element med delgruppen $H = \{id., (1\ 2)\}$, eftersom grafens struktur endast beror på storleken hos gruppen

och dess delgrupp. Men grafen blir isomorf med den graf man får om man betraktar $G' = (Z_6, +)$ med delgruppen $H' = \{0, 3\}$. Eftersom G' är abelsk men G inte är abelsk så är grupperna inte isomorfa.

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.

    Lösning: Det går bra att generalisera enligt följande:

    Låt $n = pqr$ där p, q och r är olika primtal. Bilda

    $$m = (p-1)(q-1)(r-1) \, ,$$

    och välj e och d så att

    $$ed \equiv 1 \pmod{m} \, .$$

    Detta ger att

    $$ed = 1 + d(p-1)(q-1)(r-1) \, .$$

    Vi visar nu att för varje a så gäller att p delar $(a^e)^d - a$, vilket är trivialt om p delar a. Om p inte delar a får vi med hjälp av Fermats lilla sats, emedan $ed = 1 + k(p-1)$, att

    $$(a^e)^d \equiv_p a^{ed} \equiv_p a^{1+k(p-1)} \equiv_p a \cdot (a^{p-1})^k \equiv_p a \, .$$

    På samma sätt inser vi att både q och r delar $(a^e)^d - a$. Eftersom de tre valda primtalen är olika följer då att $n = pqr$ delar $(a^e)^d - a$, dvs

    $$(a^e)^d \equiv a \pmod{n} \, .$$

    Om vi krypterar a med $E(a) = a^e \pmod{n}$ och dekrypterar ett b med $D(b) = b^d \pmod{n}$ har vi ett fungerande krypto.

    Detta krypto är nog lättare att avslöja än det traditionella, eftersom de ingående primtalen är mindre, och en faktorisering av talet n, vilken skulle ge först m och sedan d, skulle då vara lättare att genomföra.