Matematiska Institutionen
KTH

Lösning till tentamensskrivning i Diskret Matematik för CINTE, CL2 och Media 1, SF1610 och 5B1118, onsdagen den 17 augusti 2011, kl 14.00-19.00.

Examinator: Olof Heden

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng 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

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 en kontrollskrivning ger automatiskt full poäng på motsvarande uppgift. Att lösa en uppgift som man på detta sätt redan har till godo ger inga extra poäng.

1. (3p) Bestäm samtliga lösningar x och y till den diofantiska ekvationen $258x + 496y = 8$.

   Lösning: Vi söker först, och med hjälp av Euklides algoritm, den största gemensamma delaren till talen 258 och 496:

   $$\begin{aligned} 496 &= 2 \cdot 258 - 20 \\ 258 &= 13 \cdot 20 - 2 \\ 20 &= 10 \cdot 2 \end{aligned}$$

   så $\text{sgd}(496, 258) = 2$. Den givna ekvationen är då ekvivalent med ekvationen

   $$129x + 248y = 4 \, .$$

   Beräkningarna ovan ger, efter division med 2, att

   $$1 = 13 \cdot 10 - 129 = 13(2 \cdot 129 - 248) - 129 = 25 \cdot 129 - 13 \cdot 248 \, ,$$

   och efter multiplikation med 4:

   $$4 = 129 \cdot 100 + 248 \cdot (-52) \, .$$

   En lösning till givna ekvationen är alltså $x = 100$ och $y = -52$. Låt x' och y' beteckna en godtycklig annan lösning, dvs

   $$129x' + 248y' = 4 \, .$$

   Subtraktion ger då att

   $$129(x' - 100) + 248(y' + 52) = 0 \, ,$$

   eller ekvivalent

   $$129(x' - 100) = -248(y' + 52) \, .$$

   Eftersom 129 och 248 saknar gemensamma delare måste 248 dela $x' - 100$, dvs

   $$x' - 100 = k \cdot 248$$

för något heltal k. Detta substituerat i ekvationen ovan ger

$$129 \cdot k \cdot 248 = -248(y' + 52)$$

och division med -248 ger nu

$$-129 \cdot k = y' + 52$$

Slutsatsen blir att om x' och y' är lösningar till den givna ekvationen så finns ett heltal k sådanat att

$$\begin{aligned} x' &= 100 + k \cdot 248 \\ y' &= -52 - k \cdot 129 \end{aligned}$$

Vi ser nu "omvänt" att för varje heltal k så gäller

$$129x' + 248y' = 129(100 + k \cdot 248) + 248(-52 - k \cdot 129) = 129 \cdot 100 + 248 \cdot (-52) = 4 \, .$$

Således

SVAR: $x = 100 + k \cdot 248$ och $y = -52 - k \cdot 129$ där k kan vara vilket heltal som helst.

2. (3p) En klass med åtta flickor och åtta pojkar skall utse en grupp om fem klassrepresentanter. På hur många olika sätt kan man sätta samman en grupp av klassrepresentater i denna klass om alla flickor utom flickorna B och C vägrar vara med om pojken A utses. För full poäng krävs att svaret ges i formen av ett heltal.

   Lösning: Vi betraktar två möjliga fall:

   Fall 1: Pojken A väljs inte till klassrepresentant. Av total $8 + (8 - 1) = 15$ elever skall man då utse 5 elever. Antalet sätt detta kan ske på är

   $$\binom{15}{5} = \frac{15 \cdot 14 \cdot 13 \cdot 12 \cdot 11}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 3003 \, .$$

   Fall 2: Pojken A väljs. Det återstår då att välja 4 elever bland $2 + (8 - 1) = 9$ elever. Antalet sätt detta kan ske på är

   $$\binom{9}{4} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3 \cdot 4} = 126 \, .$$

   SVAR: $3003 + 126 = 3129$.

3. (3p) Bestäm tre olika delgrupper till gruppen $G = (Z_{24}, +)$ som samtliga innehåller elementet 6.

   Lösning: Vi tar tre cykliska delgrupper

   $$\begin{aligned} \langle 6 \rangle &= \{6, 12, 18, 0\} \\ \langle 3 \rangle &= \{3, 6, 9, 12, 15, 18, 21, 0\} \\ \langle 2 \rangle &= \{2, 4, 6, 8, \ldots, 22, 0\} \end{aligned}$$

   men också gruppen G innehåller elementet 6 och är en delgrupp till sig själv.

4. (a) (2p) Ett RSA-krypto har parametrarna $n = 51$, $e = 3$. Dekryptera meddelandet 2, dvs bestäm $D(2)$.

   Lösning: Då $n = 51 = 3 \cdot 17$ så är $m = (3 - 1)(17 - 1) = 32$. Den dekrypterande nyckeln d ges av villkoret $e \cdot d \equiv 1 (\text{mod } m)$. Enkel huvudräkning ger att $3 \cdot 11 = 32 + 1$, så $3 \cdot 11 \equiv 1 (\text{mod } 32)$, och alltså är $d = 11$. Då gäller att $D(2) = 2^d (\text{mod } 51)$ och vi får

   $$D(2) \equiv_{51} 2^{11} \equiv_{51} 2048 \equiv_{51} 40 \cdot 51 + 8 \equiv_{51} 8 \, .$$

   SVAR: $D(2) = 8$.

(b) (1p) Ett RSA-kryto har parametern $n = 51$. Ange samtliga möjliga värden på parametern e som man kan välja till detta val av parametern n.

Lösning: Enligt läroboken är enda kravet på krypteringsnyckeln e att det skall finnas ett tal d, sådant att $e \cdot d \equiv 1 (\text{mod } m)$, där $n = p \cdot q$ produkt av två olika primtal och $m = (p-1)(q-1)$. Eftersom, med givet $n = 51$ vi har att $m = 32$, så kan vi välja de tal e till vilka det finns ett tal d med $e \cdot d \equiv 1 (\text{mod } 32)$. Enligt den allmänna teorin för räkning i ringarna Z_n som finns i läroboken kan vi då välja precis de tal e sådana att $\text{sgd}(e, 32) = 1$, vilket är de udda talen. Så vi svarar med
SVAR: De positiva udda talen.

5. (3p) I en planär sammanhängande graf med 11 noder (hörn) har noderna valenserna (graderna) 1, 1, 2, 3, 3, 3, 4, 4, 4, 5 och 6. Bestäm antal områden som uppstår vid en plan ritning av grafen, ytterområdet medräknat.

Lösning: Valenssumman är

$$1 + 1 + 2 + 3 + 3 + 3 + 4 + 4 + 4 + 5 + 6 = 36 \, ,$$

så antalet kanter är $e = 36/2 = 18$. Eulers polyederformel ger då, eftersom grafen är sammanhängande, att antalet områden r är lika med

$$r = e - v + 2 = 18 - 11 + 2 = 9 \, .$$

SVAR: Nio områden.

DEL II

6. (3p) Bestäm antalet hela tal n mellan 1 och 1000, dvs $1 \leq n \leq 1000$, som inte är delbara med något av talen 4, 6 eller 8.

Lösning: Låt A, B och C beteckna de mängder av tal mellan 1 och 1000 som är delbara med 4, 6 resp. 8. Svaret ges då av

$$1000 - |A \cup B \cup C| \, .$$

Formen för inklusion exklusion som vi kommer att använda lyder

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \, .$$

Då

$$|A| = \lfloor \frac{1000}{4} \rfloor = 250, \quad |B| = \lfloor \frac{1000}{6} \rfloor = 166, \quad |C| = \lfloor \frac{1000}{8} \rfloor = 125,$$

$$|A \cap B| = \lfloor \frac{1000}{12} \rfloor = 83, \quad |A \cap C| = \lfloor \frac{1000}{8} \rfloor = 125, \quad |B \cap C| = \lfloor \frac{1000}{24} \rfloor = 41,$$

och

$$|A \cap B \cap C| = \lfloor \frac{1000}{24} \rfloor = 41 \, ,$$

så

SVAR: $1000 - (250 + 166 + 125) + (83 + 125 + 41) - 41 = 667$.

7. (3p) Visa, t ex med hjälp av ett induktionsbevis, att lösningen till rekursionsekvationen

$$a_n = -a_{n-1} + 6a_{n-2} \qquad n = 2, 3, \ldots ,$$

med begynnelsevärdena $a_0 = 7$ och $a_1 = 4$, ges av talföljden $a_n = 5 \cdot 2^n + 2(-3)^n$, $n = 0, 1, 2, \ldots$.

Lösning: Rekursionsekationen definierar en talföljd, och vår uppgift är att visa att denna talföljd överensstämmer med den i uppgiften givna. Vi använder ett induktionsbevis.

De givna talföljden överensstämmer med den av rekursionsekvationen definierade talföljden för $n = 0$ och $n = 1$ ty

$$\begin{aligned} a_0 &= 5 \cdot 2^0 + 2(-3)^0 = 7 \, , \\ a_1 &= 5 \cdot 2^1 + 2(-3)^1 = 4 \, . \end{aligned}$$

Antag nu att den explicit givna talföljden överensstämmer med den av rekursionesekvationen definierade talföljden för alla tal $n < k$, för något tal k. Då gäller att

$$a_k = -(5 \cdot 2^{k-1} + 2(-3)^{k-1}) + 6(5 \cdot 2^{k-2} + 2(-3)^{k-2})$$

vilket lätt förenklas till

$$a_k = -10 \cdot 2^{k-2} + 6(-3)^{k-2}) + 30 \cdot 2^{k-2} + 12(-3)^{k-2} = 5 \cdot 2^k + 2(-3)^k \, ,$$

dvs, då kommer den explicit givna talföljden att överensstämma med den rekursivt givna talföljden också för $n = k$.

Enligt induktionsprincipen överensstämmer nu den explicit givna talföljden med den rekursivt definierade talföljden för alla naturliga tal n.

8. (a) (1p) Bestäm en abelsk (kommutativ) icke-trivial delgrupp till gruppen $\mathcal{S}_3$ av permutationer på mängden $\{1, 2, 3\}$

Lösning: Vi kan välja en cyklisk delgrupp till $\mathcal{S}_3$, t ex den delgrupp som genereras av permutationen (1 2 3):

$$\langle (1\ 2\ 3) \rangle = \{(1\ 2\ 3), (1\ 3\ 2), \mathrm{id}\} \, .$$

Denna grupp är cyklisk, par definition, och alla cykliska grupper är abelska.

(b) (2p) Bevisa att varje icke-abelsk (icke-kommutativ) grupp G har minst två olika abelska icke-triviala delgrupper.

Lösning: Gruppen med bara ett element e är abelsk, så om gruppen G inte är abelsk måste det finnas minst ett element $g \neq e$. Detta element genererar en cyklisk delgrupp $\langle g \rangle$, som är abelsk (eftersom den är cyklisk), och då inte kan innehålla alla element i den icke abelska gruppen G. Om h är ett annat element i G så genererar h en cyklisk delgrupp $\langle h \rangle$ som är abelsk.

Vi har nu hittat två abelska delgrupper till G, nämligen $\langle g \rangle$ och $\langle h \rangle$.

(c) (2p) Är påståendet i deluppgiften ovan sant för abelska grupper. Motivera ditt svar!

Lösning: Nej, det finns många exempel på att påståendet i b)-uppgiften inte gäller för abelska grupper. Till exempel den abelska gruppen $G = (Z_p, +)$, där p är ett primtal, har inga icketriviala delgrupper. Vidare till exempel $(Z_4, +)$ har bara en icketrivial delgrupp, delgruppen $H = \{0, 2\}$, och är abelsk.

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. I kursen behandlas bl a binära felrättande koder och hur sådana kan konstrueras med hjälp av så kallade kontrollmatriser (parity-check matriser). Detta kan generaliseras till ternära felrättande koder, vars ord bildas med hjälp av symbolerna 0, 1 och 2. Tex kommer de kolonner som multiplicerade med matrisen $\mathbf{H}$ nedan

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix}$$

ger nollkolonnen, om man räknar modulo 3, att utgöra en felrättande ternär kod C.

(a) (2p) Ge vettiga definitioner av avstånd och felrättning, bestäm antal fel koden C ovan kan rätta, hur många ord koden har och hur många ternära ord av längd fyra som koden C inte kan rätta.

Lösning: Avståndet mellan två ord definierar vi som antalet positioner i vilka orden skiljer.

Vi visar nu att om minsta avståndet mellan ord i en kod C är $2e+1$ så kommer koden att kunna rätta e uppkomna fel: Inget ord x kan då ligga på avstånd e eller mindre från två olika ord c och c', ty om så vore fallet skulle man kunna "ta sig från" c till c' genom att först ändra i högst e koordinatpositioner för att nå x och sedan med hjälp av ytterligare högst e ändringar i koordinaterna för att sedan nå c'. Avståndet mellan c och c' skulle då vara högst $2e$.

Nu till den specifika kod C definierad med hjälp av den givna matrisen $\mathbf{H}$. Vi visar först att kodens minavstånd är 3.

Antag att c och c' är två ord i koden på avstånd 2. Då gäller att $c-c'$ är ett ord av vikt 2, dvs ett ord c'' med precis två koordinater skilda från noll. Sedvanlig matriskalkyl ger

$$\mathbf{H}c''^T = \mathbf{H}(c-c')^T = \mathbf{H}c^T - \mathbf{H}c'^T = \begin{bmatrix} 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

och då skulle nollkolonnen kunna erhållas som en summa av två kolonner i $\mathbf{H}$, varvid en eller båda kolonnerna skulle kunna vara multiplicerade med elementet 2 i Z_3.

Så vi inspekterar kolonnerna i matrisen $\mathbf{H}$ och deras multipler med 2, och finner kolonnerna

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad 2\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$$

samt för de övriga sex kolonnerna

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}; \quad \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \end{bmatrix}; \quad \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

Eftersom inga två av dessa kolonner är lika finns inget ord c'' av vikt 2 så att $\mathbf{H}c''^T = 0$.

Eftersom alla de åtta kolonnerna ovan är skilda från nollkolonnen finns inget ord c'' av vikt 1 med $\mathbf{H}c''^T = 0$ och därmed inga ord på avstånd 1 i den givna koden C.

Nu har vi visat att koden C är 1-felsrättande.

Vi visar nu att alla ord kan rättas. För den skull observerar vi först att alla kolonner utom nollkolonnen finns med i uppräkningen ovan.

Om $x = (x_1, x_2, x_3, x_4)$ är ett godtyckligt ord kommer multiplikationen $\mathbf{H}x^T$ att resultera i en av de åtta kolonnerna ovan, (eller nollkolonnen, varvid x då är ett kodord). Om t ex multiplikationen ger den sista av kolonnerna i uppräkningen ovan så kommer ordet $c = (x_1, x_2, x_3, x_4 - 2)$ att multiplicerade med $\mathbf{H}$ att ge nollkolonnen, och därmed vara ett kodord. Ordet x ligger då på avståndet 1 från ett kodord. OSV

Alla ord kan alltså rättas unikt. Totalt finns det 3^4 ord av längd 4, och kring varje kodord befinner sig precis $1 + 2 \cdot 4 = 9$ ord på avstånd noll eller ett. Då varje ord ligger på avstånd högst ett från ett kodord har vi att

$$|C| = \frac{3^4}{9} = 9\,.$$

(b) (3p) Finns det någon ternär 1-felsrättande kod med 3^{10} ord och vars ord har längden 13? Motivera ditt svar!

Lösning: Om ordlängden är 13 så kommer kring varje kodord att på avståndet högst ett befinna sig totalt

$$1 + 2 \cdot 13 = 27 = 3^3$$

stycken ord. Om C skulle bestå av 3^{10} ord skulle antalet ord koden kan rätta att vara lika med

$$|C| \cdot 3^3 = 3^{10} \cdot 3^3 = 3^{13} \ ,$$

dvs C skulle kunna rätta samtliga ord av längd 13 till ett kodord.

Vi konstruerar nu en matris $\mathbf{H}$ som ger en kod C, som med vårt allmänna recept (multiplicerar ordet x med $\mathbf{H}$ och se vilken kolonn vi får) för felrättning har egenskapen att varje ord unikt kan rättas till ett kodord.

Matrisen $\mathbf{H}$ skall ha 13 olika kolonner (eftersom ordlängden är 13) som tillsammans med sina multiplar med 2 ger samtliga 26 icke nollkolonner av höjd 3. Lite trial and error ger matrisen

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}$$

som löser problemet, eftersom dessa kolonner och deras multipler med 2 ger 26 olika kolonner.

Som i första deluppgiften ser man då också, och med samma motivering, att kodens minavstånd är 3.

10. (a) (1p) Visa att om alla noder (hörn) i en bipartit graf har valensen (graden) 2 så kan kanterna färgläggas i färgerna 0 och 1 på ett sådant sätt att vid varje nod inträffar precis en kant av vardera färgen.

Lösning: Låt grafen ha nodmängderna X och Y och där det finns inga kanter mellan noder i X och inga kanter mellan noder i Y.

Om alla noder har valens 2 så kommer grafen att bestå av enbart cykler. Varannan nod i cyklerna ligger i X och varannan i Y, så sådana cykler måste ha ett jämnt antal noder och därmed också ett jämnt antal kanter. Då kan varannan kant i respektive cykel färgas med färgen 1 och varannan kant med färgen 0. Vid varje nod kommer då att finnas precis en 0-färgad kant och en 1-färgad kant.

(b) (2p) Visa att motsvarande påstående gäller om alla noder i en bipartit graf har valensen $k = 3$ och färgerna är 0, 1 och 2.

Lösning: Se nedan.

(c) (2p) Gäller ett motsvarande påstående generellt om alla noder i en bipartit graf har valensen $k > 3$.

Lösning: Vi kommer att använda ett induktivt resonemang, och basfallet ges av deluppgift a), men vi behöver förbereda oss lite. Vi kommer att använda Halls bröllopssats.

För varje delmängd A till X låter vi $\mathrm{J}(A)$ beteckna mängden

$$\mathrm{J}(A) = \{y \in Y \mid \text{finns kant från } y \text{ till någon nod } x \in A\} \ .$$

Vårt mål är att visa att Halls villkor, dvs $|A| \leq |\mathrm{J}(A)|$ för alla delmängder A till X, är uppfyllt.

Låt $E(A)$ beteckna de kanter som inträffar i nod i delmängden A till X. Eftersom alla noder i mängden A har valensen k så gäller

$$|E(A)| = k \cdot |A| \ .$$

Å andra sidan har varje nod i mängden $\mathrm{J}(A)$ också valensen k och därmed högst k stycken kanter till noder i A så då gäller att

$$k \cdot |\mathrm{J}(A)| \geq |E(A)| \ .$$

Tillsammans ger de bägge ekvationerna ovan att Halls villkor är uppfyllt. Det finns då en samling S_k av kanter som bildar en komplett matchning i den bipartita grafen. Ta nu bort kanterna i S_k. Då återstår en bipartit graf i vilken alla noder har valens $k-1$. Fortsätt nu som ovan med denna graf.
Vi hittar alltså k stycken kompletta matchningar S_i, $i = 1, 2, \ldots, k$ sådana att

$$S_i \cap S_j = \emptyset \quad \text{för} \quad i \neq j \qquad \text{och} \qquad E = \cup_{i=1}^{k} S_i,$$

där E betecknar mängden av kanter i den bipartita grafen. Dett ger att om vi färgar kanterna i kantmängden S_i med färgen i så får varje kant sin bestämda färg. Dessutom, eftersom färgen på en kant bestäms av vilken matchning kanten tillhör, finner vi att vid en och samma nod kan inte inträffa två kanter med samma färg.