Matematiska Institutionen
KTH

Lösning till tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 1 juni 2011 kl 08.00-13.00.

Examinator: Olof Heden, tel. 0730547891.

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

Betygsgränser: (Totalsumma poäng är 36p.)

12	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

1. (3p) Ett RSA-krypto har parametrarna $n = 57$ och $e = 31$. Dekryptera meddelandet 3, dvs bestäm $D(3)$

   Lösning: Då $n = 57 = 3 \cdot 19$ så är $m = 2 \cdot 18 = 36$. Krav på den dekrypterande nyckeln d är att $e \cdot d \equiv_m 1$. Vi använder Euklides algoritm för att bestämma d:

   $$\begin{aligned} 36 &= 31 + 5 \\ 31 &= 6 \cdot 5 + 1 \end{aligned}$$

   varur

   $$1 = 31 - 6 \cdot 5 = 31 - 6(36 - 31) = 7 \cdot 31 - 6 \cdot 36 \, ,$$

   eller ekvivalent

   $$7 \cdot 31 = 1 + 6 \cdot 36 \, .$$

   Vi har alltså att $d = 7$ och kan nu dekryptera meddelandet 3:

   $$D(3) \equiv_{57} 3^7 \equiv_{57} 3^5 \cdot 3^2 \equiv_{57} 15 \cdot 9 \equiv_{57} 135 \equiv_{57} 21 \, .$$

   SVAR: 21.

2. Nedanstående matris är en check-(kontroll-)matris till en 1-felsrättande kod C

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

(a) (1p) Undersök om koden C kan rätta ordet 01111011, och rätta ordet i så fall.

Lösning: Vi finner att

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

så eftersom matrismultiplikationen ovan inte resulterade i någon av kontrollmatrisens kolonner kan det givna ordet inte rättas.

(b) (1p) Bestäm tre olika ord i C.

Lösning: Då

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

har vi

SVAR: till exempel orden 00000000, 00010011 och 10011000

(c) (1p) Bestäm antalet ord som koden C inte kan rätta.

Lösning: Då antalet ord i C är $2^{8-4} = 16$ och varje kodord "kan rätta" $8 + 1 = 9$ ord så kan koden totalt rätta $16 \cdot 9 = 144$ stycken ord. Eftersom det totalt finns 256 ord av längd 8 har vi att koden inte kan rätta $256 - 144$ stycken ord så

SVAR: 112.

3. Antag gruppen G har delgrupper med 2, 3, resp 5 element samt eventuellt också delgrupper med ett annat antal element.

   (a) (2p) Vilket är det minsta antal element en sådan grupp G kan ha? Ange detta antal och en grupp med delgrupper med 2, 3 och resp 5 element och med detta minimala antal element.

   Lösning: Enligt Lagranges sats så gäller att talen 2, 3 och 5 måste dela antalet element i G. Gruppen $G = (Z_{30}, +)$ har de cykliska delgrupperna $< 6 >$, $< 10 >$ och $< 15 >$ med respektive 5, 3 och 2 element.

   (b) (1p) Ange en grupp G' med samma antal element som den grupp G du angav ovan, som inte är isomorf med G, men som också har delgrupper med 2, 3 och resp 5 element.

   Lösning: Den direkta produkten $\mathcal{S}_3 \times (Z_5, +)$ där $\mathcal{S}_3$ betecknar mängden av permutationer av en mängd med tre element.

4. (3p) Betrakta gruppen $G = (Z_{18}, +)$. Bestäm den till antalet minsta mängd, som innehåller elementen 3 och 5, och som är en sidoklass till någon delgrupp till G.

   Lösning: Antag den sökta mängden är en sidoklass $a + H$ till delgruppen H. Då gäller att det finns h och h' i H sådana att

   $$3 = a + h, \quad 5 = a + h' \qquad \Longrightarrow \qquad h' - h = 2 \in H \ .$$

   Den minsta delgrupp till G som innehåller elementet 2 är den cykliska delgrupp $< 2 >$ som genereras av 2, så

   SVAR: $3 + < 2 >= \{3, 5, 7, 9, 11, 13, 15, 17, 1\}$

5. (3p) Låt F_{16} beteckna den kropp med 16 element som består av elementen i mängden $\{\ a_0 + a_1 x + a_2 x^2 + a_3 x^3 \ \mid \ a_0, a_1, a_2, a_3 \in Z_2\ \}$ och där man räknar som om $1 + x + x^2 + x^3 + x^4 = 0$. Lös ekvationen

   $$z(x + 1) + x^2 = 1 \ ,$$

   i denna kropp.

   Lösning: Vi finner att ekvationen kan skrivas

   $$z(x + 1) = x^2 + 1 \ ,$$

   men då $(x + 1)^2 = x^2 + 1$ har vi omedelbart

   SVAR: $z = x + 1$.

DEL II

6. (3p) Låt $\mathcal{M}$ beteckna mängden av binära 2×2-matriser (a_{ij}), dvs med $a_{ij} \in Z_2$ för $i = 1, 2$ och $j = 1, 2$. Mängden $\mathcal{M}$ utgör med de vanliga matrisoperationerna en ring (om vi räknar modulo 2). Låt $U(\mathcal{M})$ beteckna mängden av multiplikativt inverterbara element i ringen $\mathcal{M}$. Denna mängd utgör en grupp. Avgör om denna grupp är en cyklisk grupp.

   Lösning: Eftersom Z_2 är en kropp så gäller att en kvadratisk matris med element i Z_2 är inverterbar om och endast om matrisens determinant är skild från noll. Efterrsom ringen $\mathcal{M}$ endast består av 16 element är det nu lätt att använda detta kriterium på inverterbarhet, eller alternativt att undersöka samtliga element i $\mathcal{M}$, för att finna de inverterbara elementen i $\mathcal{M}$: Förutom identitetsmatrisen har vi ytterligare fem inverterbara matriser

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

   En cyklisk grupp är kommutativ så då

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

   och

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

   kan gruppen inte vara cyklisk.

7. (4p) Låt H vara en delgrupp till gruppen G med gruppoperationen $\circ$. Visa att för varje element g i G så är mängden $gHg^{-1} = \{\, g \circ h \circ g^{-1} \mid h \in H \,\}$ också en delgrupp till G. Om H är en cyklisk delgrupp till G kommer då också gHg^{-1} att vara en cyklisk delgrupp till G? Motivera ditt svar.

   Lösning: (i) Mängden är sluten under operationen $\circ$ ty om $g \circ a \circ g^{-1}$ och $g \circ b \circ g^{-1}$ är två godtyckliga element i gHg^{-1} så får vi

$$(g \circ a \circ g^{-1}) \circ (g \circ b \circ g^{-1}) = g \circ a \circ b \circ g^{-1},$$

   som ju tillhör gHg^{-1} eftersom $a \circ b \in H$.

   (ii) Associativa lagen gäller generellt i G och därför i varje delmängd till G, och då speciellt i gHg^{-1}.

   (iii) Identitets elementet e finns i gHg^{-1} eftersom elementet $e = g \circ e \circ g^{-1} \in gHg^{-1}$.

   (iv) Låt $g \circ a \circ g^{-1}$ vara godtyckligt i gHg^{-1} med $a \in H$. Då gäller att $a^{-1} \in H$ och alltså $g \circ a^{-1} \circ g^{-1} \in gHg^{-1}$. Men

$$g \circ a^{-1} \circ g^{-1} \circ g \circ a \circ g^{-1} = e$$

och

$$g \circ a \circ g^{-1} \circ g \circ a^{-1} \circ g^{-1} = e$$

så varje element i gHg^{-1} har en invers i gHg^{-1}.

Nu har vi visat att gHg^{-1} är en grupp och såsom varandes en delmängd till G blir det då också en delgrupp till G.

Antag att H genereras av elementet a. Ur relationen

$$(g \circ a \circ g^{-1})^n = g \circ a^n \circ g^{-1} \ ,$$

ser vi att då genereras gHg^{-1} av elementet $g \circ a \circ g^{-1}$.

8. (4p) Låt K beteckna den ändliga kroppen med 97 element. Bestäm samtliga lösningar till ekvationen $z^7 = 1$ i K.

   Lösning: Mängden $K \setminus \{0\}$ med operationen multiplikation i kroppen K utgör en grupp G (eftersom K är en kropp) med 96 stycken element. Om ett element z i G satisfierar $z^7 = 1$ så har z en ordning som är lika med 7 eller en delare till talet 7. Möjliga ordningar hos z är alltså 1 eller 7. Ordningen av ett gruppelement delar alltid antalet element i gruppen. Eftersom talet 7 inte delar talet 96 så har inget element i G ordning 7. Enda kvarvarande möjligheten är att z har ordning 1 (dvs $z = z^1 = 1$) så **SVAR:** $z = 1$.

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. (4p) Beskriv på ett "lämpligt sätt" en 2-felsrättande linjär kod med 64 element.

   Lösning: Vi beskriver koden med hjälp av en kontrollmatris **H**. Eftersom koden skall ha 64 ord skall skillnaden mellan antalet kolonner och antalet rader vara lika med 6. Kravet att koden är 2-felsrättande ger att kodens minimiavstånd skall vara $2 \cdot 2 + 1 = 5$. Eftersom koden är linjär så är detta ekvivalent med att kodens minimalvikt är fem. Ingen summa av en, två, tre eller fyra kolonner får då bli lika med nollkolonnen. Det finns många sätt att skriva upp en sådan matris. Lite "trial and error" ger t ex efter inspektion att följande matris duger:

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

10. (6p) Antag den ändliga abelska gruppen G har de k delgrupperna H_1, H_2, ..., H_k, där $k > 1$, sådana att $H_i \cap H_j = \{0\}$ för $i \neq j$, och med

$$G = H_1 \cup H_2 \cup \ldots \cup H_k \ .$$

Visa att det finns ett primtal p sådant att alla element i G utom nollelementet har ordning p. Bestäm också en sådan så kallad grupppartition till en grupp G med 25 element (och med $k > 1$).

Lösning: Låt gruppoperationen i G vara $+$. Låt a vara ett godtyckligt element i G skilt från identitetselementet 0 i G, och låt p vara ett primtal som delar a:s ordning n. Sätt $b = \frac{n}{p}a$. Då gäller att $b \neq 0$ och $pb = 0$ och alltså har b ordning p, eftersom p är ett primtal.

Antag $b \in H_j$ och betrakta ett godtyckligt element $c \in H_k$ med $j \neq k$ och låt $d = b + c$. Eftersom både H_j och H_k med $H_i \cap H_k = \{0\}$ är grupper så gäller att d varken kan tillhöra H_j eller H_k, utan d tillhör en tredje delgrupp H_l i partitionen av G.

Nu får vi

$$pd = p(b + c) = pb + pc = 0 + pc \ ,$$

men $pd \in H_l$ och $pc \in H_k$ och eftersom dessa bägge element är lika och $H_k \cap H_l = \{0\}$ så måste $pc = pd = 0$, dvs c måste ha ordning p. Elementet c var godtyckligt valt utanför H_j och alltså har alla element utanför H_j ordning p.

Upprepas resonemanget, med ett godtyckligt $b' \in H_j$ och bildandet av $d' = c + b' \in H_{l'}$ finner vi att även b' kommer att ha ordning p.

Nu till det sökta explicita exemplet. Låt $G = (Z_5, +) \times (Z_5, +)$. Vi bildar nu sex stycken cykliska delgrupper som upfyller de specifierade kraven:

$$\begin{array}{rcl}
< (1,0) > & = & \{(0,0),(1,0),(2,0),(3,0),(4,0)\}, \\
< (0,1) > & = & \{(0,0),(0,1),(0,2),(0,3),(0,4)\}, \\
< (1,1) > & = & \{(0,0),(1,1),(2,2),(3,3),(4,4)\}, \\
< (2,1) > & = & \{(0,0),(2,1),(4,2),(1,3),(3,4)\}, \\
< (3,1) > & = & \{(0,0),(3,1),(1,2),(4,3),(2,4)\}, \\
< (4,1) > & = & \{(0,0),(4,1),(3,2),(2,3),(1,4)\}.
\end{array}$$

.