Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 13 januari 2011 kl 14.00-19.00.

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 $n = 85$ och $e = 55$. Dekryptera meddelandet 2, dvs bestäm $D(2)$.

   Lösning: Eftersom $= 85 = 5 \cdot 17$ blir $m = (5-1)(17-1) = 64$, och d ges av inversen till $e = 55$ i ringen Z_m. Men $55 = -9$ i denna ringen och då $7 \cdot 9 = -1$ i denna ring har vi att $7 \cdot (-9) = 1$ och inversen till 55 är lika med $d = 7$.

   SVAR: $D(2) = 2^7 \pmod{85} = 43$.

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

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

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

Lösning: Vi får

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

vilket är kontrolmatrisens kolonn nummer 7, och ändrar vi i denna position i ordet får vi ett kodord, kodordet

SVAR: 01111001

(b) (1p) Bestäm två olika ord i C.

Lösning: Ordet vi fann i uppgift a) och nollordet som ju alltid finns med i koder definierade med hjälp av kontrollmatriser.

(c) (1p) Bestäm antalet ord i C.

Lösning: $2^{8-4} = 16$.

3. (3p) Kroppen F består av de 25 elementen $ax + b$ där a och b tillhör kroppen Z_5, och där man vid multiplikation av de 25 elementen kan ersätta x^2 med elementet 2. Bestäm ett element z i kroppen F sådant att

$$(x+1)^2 z = 3x + 2.$$

Lösning: Vi beräknar först $(x+1)^2$ och får

$$(x+1)^2 = x^2 + 2x + 1 = 2x + 3\ ,$$

sum ju råkar vara lika med $-(3x+2)$ och alltså ser vi nästan omedelbart att

SVAR: $z = -1$.

4. (3p) Låt p vara ett primtal och $\mathcal{Q}$ mängden av alla kvadrater skilda från noll i ringen Z_p. Visa, genom att verifiera de fyra axiomen för en grupp, att $\mathcal{Q}$ utgör en grupp under operationen multiplikation.

Lösning: (i)(*slutenheten*): Om $a, b \in \mathcal{Q}$ så har vi att $a = x^2$ och $b = y^2$ vilket medför att $ab = (xy)^2$ och därmed gäller att $ab \in \mathcal{Q}$

(ii) (*associativiteten:*) Antag $a, b, c \in \mathcal{Q}$. Då gäller att $a, b, c \in Z_p$ och i denna ring gäller associativitet vid multiplikation, alltså

$$a(bc) = (ab)c\ .$$

(iii) (*existens av identitet*) Då $1 = 1^2$ så har vi att $1 \in \mathcal{Q}$ och vidare för varje $a \in \mathcal{Q}$ gäller ju $a \cdot 1 = 1 \cdot a = a$ eftersom a ju även tillhör Z_p.

(iv) (*existens av invers*) Om $a \in \mathcal{Q}$ så $a = x^2$ för något $x \in Z_p$. Men eftersom p är ett primtal så har x en invers x^{-1} i Z_p, och vi finner att med $b = (x^{-1})^2$ så

$$a \cdot b = xxx^{-1}x^{-1} = 1 \, ,$$

dvs a har inversen $b = (x^{-1})^2 \in \mathcal{Q}$.

5. (3p) Betrakta gruppen $G = (Z_{18}, +)$ och bestäm en sidoklass S till någon delgrupp H till G sådan att elementen 3 och 7 tillhör S men 5 inte tillhör S.

Lösning: Uppgiften felformulerad och problemet utgick ur tentamensskrivningen.

DEL II

6. (3p) Hur många halsband med fem pärlor kan man skapa om det finns q stycken olika färger att välja bland till pärlorna.

Lösning: Vi använder Burnsides lemma och ställer för den skull upp tabellen nedan. I denna tabell betecknar $\mathrm{Aut}(H)$ gruppen av alla vridningar och vändningar av halsbandet som vrider det till sig själv, samt $|Fix(\varphi)|$ betecknar för vridningen φ, antalet färgläggningar som fixeras av φ. Tabellen blir

$\mathrm{Aut}(H)$	$\lvert Fix(\varphi)\rvert$
id.	q^5
(1 2 3 4 5)	q
(1 3 5 2 4)	q
(1 4 2 5 3)	q
(1 5 4 3 2)	q
(1)(2 5)(3 4)	q^3
(2)(1 3)(4 5)	q^3
(3)(2 4)(1 5)	q^3
(4)(3 5)(1 2)	q^3
(5)(1 4)(2 3)	q^3

Eftersom antalet element i $\mathrm{Aut}(H)$ är 10 ger Burnsides lemma

SVAR:

$$\frac{1}{10}(q^5 + 5q^3 + 4q) \, .$$

7. (4p) Bestäm samtliga delgrupper till gruppen $(Z_{29} \setminus \{0\}, \cdot)$.

   Lösning: Eftersom 29 är ett primtal så är ringen en kropp, och då är dess multiplikativa grupp cyklisk. Vi undersöker nu om elementet 2 genererar den gruppen som består av 28 element. Enligt en följdsats till Lagranges sats så delar ordningen av elementet 2 talet 28. Vi undersöker därför om någon av potenserna 2^2, 2^4, 2^7 och 2^{14} blir lika med 1 i ringen Z_{29}. Vi finner

   $$2^2 = 4 \neq 1\,, \quad 2^4 = 16 \neq 1\,, \quad 2^7 = 12 \neq 1\,, \quad 2^{14} = 12^2 = -1 \neq 1\,.$$

   Enda möjligheten är att elemetet 2 har ordining 28, och således genererar kroppens multiplikativa grupp.

   Enligt känd sats har en cyklisk grupp med n element precis en delgrup med d element för varje delare d till n, och inga andra grupper. Eftersom

   $$(Z_{29} \setminus \{0\}, \cdot) = \{2, 2^2, 2^3, 2^4, \ldots, 2^{28} = 1\}\,,$$

   ser vi delgrupperna med 1, 2, 4, 7 och 14 element:

   $$H_1 = \{1\}\,, \quad H_2 =< 2^{14} >= \{2^{14}, 1\} = \{-1, 1\},$$

   $$H_4 =< 2^7 >= \{2^7, 2^{14}, 2^{21}, 1\} = \{12, -1, -12, 1\}\,,$$

   $$H_7 =< 2^4 >= \{2^4, 2^8, 2^{12}, \ldots, 1\}\,, \quad H_{14} =< 2^2 >\,,$$

   samt hela gruppen.

8. (4p) Undersök om polynomet

   $$x^6 + 3x^5 + 6x^4 + 7x^3 + 6x^4 + 3x + 1$$

   är irreducibelt i polynomringen $Z_2[x]$.

   Lösning: Uppenbarligen saknar polynomet nollställen i ringen Z_2, så vi undersöker eventuella faktorer av grad två, och som då måste vara irreducibla, ty annars skulle det funnits ett nollställe till polynomet. Division med det enda sådana irreducibla polynomet $x^2 + x + 1$ ger

   $$x^6 + 3x^5 + 6x^4 + 7x^3 + 6x^4 + 3x + 1 =$$

   $$(x^2 + x + 1)(x^4 + 2x^3 + 3x^2 + 2x + 1)\,,$$

   så polynomet är inte irreducibelt.

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. Mängden av permutationer på mängden $\{1, 2, 3, 4\}$ bildar en grupp med 24 element, och som brukar betecknas $\mathcal{S}_4$.

   (a) (1p) Bestäm en delgrupp H_1 med 8 element till gruppen $\mathcal{S}_4$.

   Lösning: Ett element med ordning 3 kan aldrig tillhöra en grupp med 8 element, så elementen i H_1 är antingen 4-cykler, eller 2-cykler, eller produkter av 2-cykler. Efter lite exprimenterande med delgruppen

   $$\mathcal{K}_4 = \{e = \text{id.}, a = (1\ 2)(3\ 4), b = (1\ 3)(2\ 4), c = (1\ 4)(2\ 3)\}$$

   där alla element har ordning 2, samt

   $$ab = c\ , \qquad ac = b\ , \qquad bc = a\ ,$$

   finner vi med $\varphi = (1\ 2\ 3\ 4)$ att

   $$\varphi a = (1\ 3) = c\varphi, \qquad c = (2\ 4) = a\varphi$$

   samt givetvis, då $\varphi^2 = b$, att $\varphi b = b\varphi = \varphi^3$.
   Ur räkningarna ovan framgår att mängden

   $$H_1 = \mathcal{K}_4 \cup \mathcal{K}_4\varphi\ ,$$

   dvs mängden

   $$H_1 = \{\text{id.}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\,3), (2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}$$

   är sluten under multiplikation, och såsom delmängd till en ändlig grupp, därmed en grupp.

   (b) (2p) Det finns ytterligare två delgrupper H_2 och H_3 till $\mathcal{S}_4$ och som har 8 element. Bestäm H_2 och H_3.

   Lösning: Elementen 1, 2, 3 och 4 är ”jämlika” så byter vi t ex ut 2 mot 3, och 3 mot 2, i räkningarna ovan får vi också en grupp:

   $$H_2 = \{\text{id.}, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\,2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

   liksom om vi byter ut 3 mot 4 och 4 mot 3

   $$H_3 = \{\text{id.}, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4), (1\,4), (2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2)\}$$

   (c) (2p) Undersök om några av grupperna H_1, H_2 och H_3 är isomorfa med varandra.

Lösning: Utbytena ovan av symbolerna 1, 2, 3 och 4 beskriver precis isomorfierna mellan grupperna, vilket beskrivs mer precist i vad som följer.

Vi skriver nu permutationerna på tablåform och isomorfin mellan gruppen H_1 och H_2 med θ och har då

$$\theta : H_1 \to H_2 \ ,$$

där

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \gamma(1) & \gamma(2) & \gamma(3) & \gamma(4) \end{pmatrix} \quad \mapsto$$

$$\theta(\gamma) = \begin{pmatrix} \psi(1) & \psi(2) & \psi(3) & \psi(4) \\ \psi(\gamma(1)) & \psi(\gamma(2)) & \psi(\gamma(3)) & \psi(\gamma(4)) \end{pmatrix}$$

där $\psi = (2\ 3)$.

På precis samma sätt får vi isomorfin mellan H_1 och H_3. Eftersom H_2 och H_3 båda är isomorfa med H_1 så är även H_2 och H_3 isomorfa som grupper.

10. (5p) En felrättande kod C över ett alfabete med fyra symboler, och där orden har längd 5 kan konstrueras enligt följande recept:

    Betrakta kroppen GF(16) med 16 element och vars multiplikativa grupp genereras av elementet ϑ. Låt K_0 vara delmängden

    $$K_0 = \{0, 1, \vartheta^5, \vartheta^{10}\} \ ,$$

    till GF(16), samt låt $K_i = \vartheta^i K_0$ för $i = 1, 2, 3, 4$. Vi definerar nu C som mängden av alla de 5-tiplar $(c_0, c_1, c_2, c_3, c_4)$ som är sådana att

    $$c_0 + c_1 + c_2 + c_3 + c_4 = 0 \ ,$$

    där $c_i \in K_i$, för $i = 0, 1, 2, 3, 4$.

    Diskutera vilka egenskaper koden C har och om denna konstruktion går att generalisera.

    Lösning: Koden kommer att vara en 1-felsrättande kod med egenskapen att varje möjligt ord i $K_0 \times K_1 \times K_2 \times K_3 \times K_4$ är på avståndet 1 från något kodord. Vi bevisar nu detta.

    Tag ett godtyckligt ord $(x_0, \ldots, x_4)$ i den direkta produkten ovan. Vi bildar nu summan

    $$s = x_0 + x_1 + \ldots + x_4 \ ,$$

    och elementet s kommer att tillhöra $GF(16)$ eftersom s är en summa av element i denna kropp. Det är lätt, t ex genom inspektion, att övertyga

sig om att varje element, skilt från noll, i denna kropp tillhör precis en av mängderna K_i, för $i = 1, 2, 3, 4, 5$. Om nu t ex $s = y_1 \in K_1$ så får vi att

$$x_0 + (x_1 - y_1) + x_2 + x_3 + x_4 = s - s = 0 \ ,$$

vilket ger att ordet

$$(x_0, x_1, x_2, x_3, x_4) - (0, y_1, 0, 0, 0) \in C \ .$$

Varje ord ligger således på avstånd ett från något kodord.

Om minimiavståndet i koden är 3 så är koden 1-felsrättande. Antag nu att orden $\bar{x} = (x_1, x_2, x_3, x_4, x_5)$ och $\bar{x}' = (x_1', x_2', x_3', x_4')$ har avstånd två och att t ex $x_2 \neq x_2'$ och $x_4 \neq x_4'$. Då gäller

$$0 = 0 - 0 = (x_0 + x_1 + \ldots + x_4) - (x_0' + x_1' + \ldots + x_4') =$$

$$= x_2 - x_2' + x_4 - x_4' \ ,$$

dvs

$$x_2 - x_2' = x_4' - x_4 \ .$$

Men $x_2 - x_2' \in K_2$ och $x_4 - x_4' \in K_4$ och då dessa additiva grupper endast har nollelementet gemensamt så måste $x_2 - x_2' = 0$ och $x_4 - x_4' = 0$, och därmed har vi att $\bar{x} = \bar{x}'$. På ett liknande sätt inses att två ord i C aldrig kan ha avståndet 1 från varandra.

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

Och givetvis går konstruktionen att generalisera. Låt F' vara en delkropp till kroppen F. Multiplikativa gruppen $G' = (F' \setminus \{0\}, \cdot\ )$ i F' är då en delgrupp till multiplikativa gruppen $G = (F \setminus \{0\}, \cdot\ )$ i F. Sidoklasserna till G' i G dvs mängderna $G_i = \alpha_i G'$, för $i = 1, 2, \ldots, n = |G|/|G'|$, är disjunkta och täcker över hela G. Dessutom är mängderna $G_i' \cup \{0\}$ additiva grupper, ty t ex

$$\alpha g' + \alpha h' = \alpha(g' + h') \in \alpha G' \ ,$$

eftersom $G' \cup \{0\} = F'$ är en kropp.

Så bildar vi koden C som mängden av de ord $(c_1, c_2, \ldots, c_n)$ i den direkta produkten $G_1 \times G_2 \times \ldots \times G_n$ som är sådana att

$$c_1 + c_2 + \ldots + c_n = 0 \ ,$$

får vi, med en motivering som ord för ord är som den ovan givna motiveringen, en så kallad perfekt 1-felsrättande kod.