Matematiska Institutionen
KTH

Lösningar till tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 20 maj 2009 kl 08.00-13.00.

Hjälpmedel: Inga hjälpmedel är tillåtna på tentamensskrivningen.

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

DEL I

1. (3p) Ett RSA-krypto har parametrarna $n = 77$ och $e = 37$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.

   Lösning: Vi finner att $n = 77 = 7{\cdot}11$ och således är $m = 6{\cdot}10 = 60$. Söker nu dekrypteringsnyckeln d. Vet att $d \cdot e \equiv_m 1$, dvs $d \cdot 37 \equiv_{60} 1$. Euklides algoritm ger

   $$\begin{aligned} 60 &= 2 \cdot 37 - 14 \\ 37 &= 3 \cdot 14 - 5 \\ 14 &= 3 \cdot 5 - 1. \end{aligned}$$

   Deta ger att

   $$1 = 3 \cdot 5 - 14 = 3 \cdot (3 \cdot 14 - 37) - 14 = 8 \cdot 14 - 3 \cdot 37 = 8(2 \cdot 37 - 60) - 3 \cdot 37 = 13 \cdot 37 - 8 \cdot 60.$$

   Ur detta får vi att $d = 13$. Vi beräknar nu $D(3)$.

   $$D(3) = 3^d (\text{mod } n) = 3^{13} (\text{mod } 77) = 3^8 \cdot 3^4 \cdot 3 (\text{mod } 77).$$

   Men

   $$3^4 (\text{mod } 77) = 81 (\text{mod } 77) = 4, \qquad 3^8 (\text{mod } 77) = 4 \cdot 4 (\text{mod } 77) = 16 (\text{mod } 77).$$

   och alltså

   $$3^{13} \equiv_{77} 16 \cdot 4 \cdot 3 \equiv_{77} 64 \cdot 3 \equiv_{77} -13 \cdot 3 \equiv_{77} -39 \equiv_{77} 38.$$

   SVAR: 38

2. (3p) Tabellen nedan är multiplikationstabellen till en grupp G.

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

   Bestäm ett element x i G som löser ekvationen

   $$a^2bx = cd.$$

   Lösning: Tabellen ger att $cd = a$ och därmed ekvation $a^2bx = a$. Multiplikation med a^{-1} till vänster i likheten ger

   $$abx = e.$$

   I tabellen hittar vi att $ab = c$ och $cx = e$ ger ur tabellen

   SVAR: $x = c$.

3. (a) (1p) Bestäm a och b så att nedanstående matris blir en parity-check (kontroll-) matris till en 1-felsrättande kod C

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

Lösning: Ingen kolonn i en kontrollmatris är nollkolonnen alltså är $b = 1$. Kolonnerna är olika ger att $a = 1$.

(b) (1p) Undersök om koden C kan rätta ordet 011110, och rätta ordet i så fall.

Lösning: Rättningsproceduren föreskriver att vi för det mottagna ordet c beräknar

$$Hc^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

vilket är den femte kolonnen. Ett fel i femte biten och
SVAR: 011100.

(c) (1p) Bestäm två olika kodord, dvs bestäm c och c' sådana att $c \neq c'$ och $c, c' \in C$.

Lösning: Nollordet finns alltid med och vi fann ett kodord i uppgiften ovan så
SVAR: 000000, och 011100.

4. (3p) Är polynomet $x^3 + 2x + 1$ irreducibelt i polynomringen $Z_5[x]$.

Lösning: Det är ej irreducibelt om det går att faktorisera i två polynom faktorer, som har grad lägst 1. Eftersom det givna polynomets grad är tre skulle en av dessa faktorer har grad ett, vilket skulle medföra att polynomet skulle ha minst ett nollställe i Z_5. Vi testar nu detta. Låt $p(x) = x^3 + 2x + 1$. Vi får

$$p(0) = 1 \neq 0, \quad p(1) = 4 \neq 0, \quad p(2) = 3 \neq 0,$$

samt

$$p(3) = p(-2) = -1 \neq 0, \quad p(4) = p(-1) = -2 \neq 0.$$

Eftersom polynomet är av grad tre och saknar nollställen så

SVAR: Polynomet är irreducibelt.

5. Betrakta gruppen $G = (Z_{12}, +)$.

(a) (1p) Bestäm en delgrupp H till G sådan att H har fyra element.

Lösning: $< 3 >= \{0, 3, 6, 9\}$

(b) (1p) Bestäm en vänster sidoklass S till H som innehåller elementet 2.

Lösning: $S = 2 + < 3 >= \{2, 5, 8, 11\}$

(c) (1p) Förklara varför G saknar en sidoklass S till en delgrupp K med fyra element sådan att både 2 och 4 tillhör S.

Lösning: Givna gruppen $(Z_{12}, +)$ är cyklisk, eftersom den genereras av elmentet 1, och har därför bara en delgrupp med fyra element, den ovan angivna delgruppen $< 3 >$. Sidoklasser till givna delgrupper är parvis disjunkta. Den enda möjliga sidoklasssen med fyra element som innehåller elementet 2 är den ovan angivn sidoklassen $S = 2 + < 3 >$. Den innehåller inte elementet 4.

DEL II

6. (3p) Kroppen $GF(16)$ med 16 element definieras av att kroppen består av elementen

$$GF(16) = \{a + bx + cx^2 + dx^3 \mid a, b, c, d \in Z_2\}.$$

och av att man räknar som om $x^4 + x + 1 = 0$. Lös, i den givna kroppen, ekvationen

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

Lösning: Vi finner att $(x^2 + 1)^2 = x^4 + 2x^2 + 1 = x^4 + 1 = x + 1 + 1 = x$ så ekvationen kan förenklas till

$$xz = x + 1 \qquad \Longrightarrow \qquad z = 1 + x^{-1}.$$

Söker inversen till x. Vi finner

$$x^4 + x = 1 \quad \Rightarrow \quad x(x^3 + 1) = 1 \quad \Rightarrow \quad x^{-1} = x^3 + 1.$$

SVAR: $z = 1 + (x^3 + 1) = x^3$.

7. Betrakta den direkta produkten R av ringarna Z_{10} och Z_{14}, dvs

$$R = Z_{10} \times Z_{14} = \{(a, b) \mid a \in Z_{10}, b \in Z_{14}\},$$

och där addition och multiplikation sker komponentvis.

   (a) (2p) Visa att (a, b) är inverterbar, m a p multiplikationen i R, om och endast om a är inverterbar i Z_{10} och b är inverterbar i Z_{14}.

   Lösning: Elementet $(1, 1)$ är den givna ringens identitetselement eftersom

$$(1, 1)(a, b) = (1 \cdot a, 1 \cdot b) = (a, b),$$

   för alla element (a, b) i ringen. Vidare får vi

$$(a, b)(c, d) = (1, 1) \quad \Leftrightarrow \quad (ac, bd) = (1, 1) \quad \Leftrightarrow \quad ac = 1 \quad \text{och} \quad bd = 1,$$

   vilket säger att elementet (a, b) är inverterbart om och endast om både a och b är inverterbara.

   (b) (2p) Mängden av inverterbara element i en ring R bildar en grupp, ringens så kallade multiplikativa grupp $U(R)$. Avgör om $U(R)$, för den givna ringen $R = Z_{10} \times Z_{14}$, är en cyklisk grupp.

   Lösning: Det är lätt att kontrollera vilka de inverterbara elementen är i de givna ringarna

$$U(Z_{10}) = \{1, 3, 7, 9\}, \qquad U(Z_{14}) = \{1, 3, 5, 9, 11, 13\}.$$

   Enligt deluppgift a) består då $U(R)$ av $|U(Z_{10})| \cdot |U(Z_{14})| = 4 \cdot 6 = 24$ element. Dessvärre uppfyller alla element i dessa grupper följande relationer

$$a \in U(Z_{10}) \quad \Rightarrow \quad a^4 = 1, \qquad b \in U(Z_{14}) \quad \Rightarrow \quad b^6 = 1,$$

   eftersom dessa grupper har fyra respektive sex element. Vi finner då att

$$a \in U(Z_{10}),\ b \in U(Z_{14}) \quad \Rightarrow \quad (a, b)^{12} = (a^{12}, b^{12}) = ((a^4)^3, (b^6)^2) = (1^3, 1^2) = (1, 1).$$

   Inget element har alltså en ordning större än 12 och alltså kan inte gruppen vara cyklisk eftersom element av ordning 24 saknas.

8. (4p) Går tabellen nedan att fylla i så att den blir multiplikationstabellen till en grupp

$\circ$	e	a	b	c	d
e	e				
a					b
b					
c		b			
d					

.

Lösning: Gruppen består av fem element och då kommer varje element som inte är identiteten att generera gruppen. Speciellt innebär detta att gruppen är cyklisk och därmed abelsk. (Givna indata ger att e är identiteselementet eftersom

$$ee = e \qquad \Longrightarrow \qquad e = e^{-1}e = \text{gruppens identiteselement})$$

Vidare får vi att pga av att gruppen är abelsk

$$ad = b = ca = ac \qquad \Longrightarrow \qquad a^{-1}ad = a^{-1}ac \qquad \Longrightarrow \qquad d = c.$$

I multiplikationstabeller förekommer ej samma element mer en än gång i den ”definierande” raden. Så tabellen kan inte definiera en grupp eftersom $d \neq c$.

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. (a) (1p) Låt G vara en abelsk, dvs kommutativ, grupp. Visa att om gruppen G har två olika delgrupper H_1 och H_2, som bägge har 7 element så består snittet av H_1 och H_2, dvs $H_1 \cap H_2$, endast av gruppen G:s identitetselement, med andra ord att det enda element i G som tillhör både H_1 och H_2 är G:s identitetselement. (Utan att behöva bevisa det, får man använda att $H_1 \cap H_2$ också är en delgrupp till G.)

   Lösning: Då $H_1 \cap H_2$ är en delgrupp till både H_1 och H_2 så gäller enligt Lagranges sats att $|H_1 \cap H_2|$ delar $|H_1| = 7$ och $|H_2| = 7$, varur, eftersom 7 är ett primtal

   $$|H_1 \cap H_2| \in \{1, 7\}.$$

   Eftersom $H_1 \neq H_2$ får vi att

   $$|H_1 \cap H_2| < 7.$$

   Detta bevisar påståendet.

   (b) (1p) Låt G, H_1 och H_2 vara som ovan. Antag $h_1, h_1' \in H_1$ och $h_2, h_2' \in H_2$. Visa att om $h_1 + h_2 = h_1' + h_2'$ så är $h_1 = h_1'$ och $h_2 = h_2'$.

   Lösning:

   $$h_1 + h_2 = h_1' + h_2' \qquad \Longrightarrow \qquad h_1 - h_1' = h_2' - h_2.$$

   Men $h_1 - h_1' \in H_1$ och $h_2' - h_2 \in H_2$ och alltså enligt föregående deluppgift

   $$h_1 - h_1' = h_2' - h_2 \in H_1 \cap H_2 \qquad \Longrightarrow \qquad h_1 - h_1' = h_2' - h_2 = 0,$$

   och påståendet bevisat.

(c) (1p) Låt G, H_1 och H_2 vara som ovan. Visa att G har minst 49 element.

Lösning: Gruppen G innehåller bland annat elementen

$$h_1 + h_2, \qquad \text{där} \qquad h_1 \in H_1, \quad h_2 \in H_2.$$

Enligt föregående deluppgift är alla dessa element olika, så simpel kombinatorik ger totalt 49 olika element, minst i G.

(d) (1p) Vilka av påståendena ovan är sanna i det fall förutsättningarna ändras och kravet G abelsk inte finns med.

Lösning: Deluppgifte a) använder inte att gruppen är abelsk. Om vi formulerar b) som $h_1 \circ h_2 = h_1' \circ h_2'$ får vi villkoret

$$h_1'^{-1} \circ h_1 = h_2' \circ h_2^{-1} = e,$$

där e betecknar gruppens identitetselement. Så även påståendet i b) är sant och därmed c), eftersom det resultatet bygger på att uppgift b) var korrekt.

(e) (2p) Formulera en allmän sats som har ovanstående resultat som ett specialfall. (Du behöver inte ge ett bevis för satsen, men poäng på denna deluppgift sätts efter kvalite'n på den sats du formulerar.)

Lösning: Minimikrav för full poäng är

Sats. *Om H_1 och H_2 delgrupper till gruppen G sådana att*

$$sgd(|H_1|, |H_2|) = 1,$$

så gäller att

$$|G| \geq |H_1| \cdot |H_2|.$$

10. (4p) Betrakta en ändlig kropp F. Låt $p(x)$ vara ett irreducibelt tredjegradspolynom i polynomringen $F[x]$. Låt K vara kroppen

$$K = \{a + bx + cx^2 \mid a, b, c \in F\},$$

där man räknar som om $p(x) = 0$. Om polynomet $q(z)$ har grad två och är irreducibelt i polynomringen $F[z]$ under vilka förutsättningar kommer då $q(z)$ också att vara irreducibelt i polynomringen $K[z]$.

Lösning: Om $q(z)$ ej vore irreducibelt i $K[z]$ skulle det, eftersom $q(z)$ har grad 2, finns ett element $\alpha \in K$ sådanat att $q(\alpha) = 0$. Vi skulle då kunna bilda kroppen L, eftersom $q(z)$ är irreducibelt i $F[z]$, enligt

$$L = \{a + b\alpha \mid a, b \in F\},$$

och där räkningar sker som om $q(\alpha) = 0$. Dessa räkningar är i överensstämmelse med kalkylerna i K, eftersom $q(\alpha) = 0$ i K. Vidare, eftersom $\alpha \in K$ så är L en delmängd till K. Vi finner att L skulle bilda en delkropp till K. Speciellt måste den multiplikativa gruppen i L vara en delgrupp till den multiplikativa gruppen i K och vi skulle ha att

$$(|L| - 1) \ \mid \ (|K| - 1).$$

Antag att $|F| = q = p^k$ för något primtal p. Eftersom $|K| = q^3$ och $|L| = q^2$ skulle nedanstående kvot då vara ett heltal

$$\frac{q^3 - 1}{q^2 - 1} = \frac{(q-1)(q^2+q+1)}{(q-1)(q+1)} = q + \frac{1}{q+1}.$$

Eftersom detta inte är ett heltal är allt fel och speciellt antagandet att $q(z)$ ej är irreducibelt i $K[z]$.

SVAR: $q(z)$ kommer att alltid vara irreducibelt i $K[z]$.