Matematiska Institutionen
KTH

Lösning till tentamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 25 maj 2010 kl 08.00-13.00.

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

Bonuspoäng: Bonuspoäng erhållna från lappskrivningar till kursen under vt09 adderas till skrivningspoängen.

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

DEL I

1. (3p) Till ett RSA-krypto väljer man primtalen $p = 3$ och $q = 23$, vilka skall användas i denna uppgift.

   (a) (1p) Vilket, eller vilka, av följande värden på parametern e kan man använda: $e = 9$, $e = 10$ och/eller $e = 11$.

   Lösning: Vi finner att $m = (p-1)(q-1) = 2 \cdot 22 = 44$, så varken 11 eller 10 skulle fungera som värden på e eftersom dessa tal inte är relativt prima med talet 44. Däremot fungerar $e = 9$ eftersom $\mathrm{sgd}(9, 44) = 1$.

   (b) (2p) Välj ett tillåtet värde på parametern e och dekryptera meddelandet 2, dvs bestäm $D(2)$.

   Lösning: Vi söker ett tal d sådant att $e \cdot d \equiv 1 \pmod{44}$. Euklides algoritm ger

   $$44 = 5 \cdot 9 - 1 \, ,$$

   så $5 \cdot 9 = 1 + 44$ och $d = 5$. Då $2^5 = 32 \pmod{69}$ så
   SVAR: 32.

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

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

(a) (1p) Undersök om koden C kan rätta ordet 01110111, och rätta ordet i så fall.

Lösning: Vi finner att

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

vilket är kontrollmatrisens näst sista kolonn, så i näst sista koordinaten uppstod ett fel, och det rätta ordet är

SVAR: 01110101.

(b) (1p) Ange antalet ord i C.

Lösning: Kontrollmatrisens fyra rader är ”ju” linjärt oberoende, och eftersom kontrollmatrisen har åtta kolonner har koden

SVAR: $2^{8-4} = 16$ ord.

(c) (1p) Bestäm antalet ord som ”kan rättas” av C.

Lösning: Koden kan rätta alla ord som ligger på avståndet ett från ett kodord, och eftersom ordlängden är åtta är det åtta ord som är på avstånd ett från ett kodord. Total kan

SVAR: $16 \cdot 8 = 128$ rättas och om kodorden själva räknas med kan ytterligare 16 ord ”rättas”, dvs totalt $128 + 16 = 144$ stycken ord. (Båda svaren ger full poäng.)

3. (3p) Betrakta gruppen $G = (Z_{20}, +)$ som innehåller elementen $\{0, 1, 2, \ldots, 19\}$ och där man räknar modulo 20. En av sidoklasserna (”coset”) till en av gruppens delgrupper innehåller elementet 2 och tre element till. Bestäm dessa tre element.

Lösning: Delgruppen ifråga innehåller lika många element som sidoklassen ifråga. Den enda delgruppen med fyra element är $H = \{0, 5, 10, 15\}$ och sidoklassen $2 + H = \{2, 7, 12, 17\}$ är den sökta, så

SVAR: elementen 7, 12 och 17.

4. Låt F vara kroppen med de 16 elementen

$$F = \{\ a_0 + a_1x + a_2x^2 + a_3x^3 \ \mid \ a_0, a_1, a_2, a_3 \in Z_2\ \} \qquad ;,$$

och där man räknar som om $x^4 + x + 1 = 0$.

(a) (2p) Bestäm det element z i F som är invers till x, dvs sådant att $x \cdot z = 1$.

Lösning: I den givna kroppen gäller att $x^4 + x = 1$ varur vi lätt ser att $x \cdot (x^3 + 1) = 1$, så

SVAR: $x^{-1} = x^3 + 1$.

(b) (1p) Bestäm ett element w i F sådant att $x \cdot w = x^2 + x + 1$.

Lösning: Vi får omedelbart, då $x^4 = x + 1$, att

$$w = x^{-1}(x^2 + x + 1) = (x^3 + 1)(x^2 + x + 1) = x^5 + x^4 + x^3 + x^2 + x + 1 =$$

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

5. (4p) Betrakta gruppen $G = (Z_{24}, +)$ som innehåller elementen $\{0, 1, 2, \ldots, 23\}$ och där man räknar modulo 24.

   (a) (2p) Bestäm en delgrupp till G som innehåller elementet 16, men inte innehåller elementet 3.

   Lösning: Eftersom 8 delar både 16 och 24 hittar vi
   SVAR: delgruppen $K = \{0, 8, 16\}$.

   (b) (2p) Visa att om en delgrupp H till G innehåller både elementet 3 och elementet 16 så måste $H = G$.

   Lösning: Eftersom H är sluten med avseende på operationen addition så måste

   $$n(16 - (3 + 3 + 3 + 3 + 3)) \pmod{24} \in H$$

   för varje naturligt tal n, dvs H innehåller elementen $n \cdot 1 \pmod{24}$, för $n = 1, 2, 3, \ldots$.

DEL II

6. (3p) Mängden av element i ringen Z_{24} som är inverterbara med avseende på multiplikation bildar en grupp. Undersök om denna grupp är cyklisk.

   Lösning: Ett element a i Z_{24} är inverterbart om och endast om $\mathrm{sgd}(a, 24) = 1$. Vi finner alltså att de inverterbara elementen är

   $$G = \{\ 1, 5, 7, 11, 13, 17, 19, 23\ \}\ .$$

   Gruppen G är cyklisk om något elementen i gruppen har en ordning som är lika med antalet element i G dvs åtta. Vi undersöker nu detta och utnyttjar vetskapen om att ordningen av ett element alltid är en delare till antalet element i gruppen. Vi betecknar ordningen av ett element $g \in G$ med $\sigma(g)$. Vi testar

   $$5^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   $$7^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   $$11^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   $$13^2 = (-11)^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   $$17^2 = (-7)^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   $$19^2 = (-5)^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   $$23^2 = (-1)^2 = 1 \quad \Longrightarrow \quad \sigma(g) \neq 8\ .$$

   Så
   SVAR: Nej gruppen är inte cyklisk.

7. (3p) Är polynomet $x^4 + x - 1$ irreducibelt i polynomringen $Z_5[x]$?

   Lösning: Om polynomet $p(x) = x^4 + x - 1$ skulle han en faktorisering med en förstagradsfaktor skulle poynomet ha ett nollställe i Z_5, vilket lätt kontrollers att så ej är fallet (**alternativt:** I Z_5 gäller enligt Fermats lilla sats att $a^4 = 1$ för $a \neq 1$ vilket ger för dessa element a att $p(a) = a \neq 0$).

Vi undersöker nu om $p(x)$ kan faktoriseras i polynom av grad två:

$$x^4 + x - 1 = (x^2 + Ax + B)(x^2 + Cx + D) \ .$$

Vi utvecklar högerledet ovan och om likhet skall gälla får vi $(-1 = 4)$

$$\begin{cases} BD &= 4 \\ BC + AD &= 1 \\ B + D + AC &= 0 \\ A + C &= 0 \end{cases}$$

den första ekvationen ger två fall $(B, D) = (1, 4)$, $(3, 3)$ resp $(B, D) = (2, 2)$ att undersöka. Det tredje fallet ger, insatt i systemet ovan bland annat ekvationerna

$$\begin{cases} 2(C + A) &= 1 \\ A + C &= 0 \end{cases}$$

vilket är två ekvationer som strider mot varandra. Det första fallet ger insatt i systemets bägge sista ekvationer systemet

$$\begin{cases} AC &= 0 \\ A + C &= 0 \end{cases}$$

Så antingen $A = 0$ eller $C = 0$, enligt den första av de bägge ekvationerna, med detta medför, i bägge fallen, enligt den andra ekvationen, att då blir både $A = 0$ och $C = 0$, men detta strider mot ekvation nummer två i det ursprungliga systemet.

Det andra fallet behandlas likadant.

Så

SVAR: Det givna polynomet är irreducibelt.

8. (4p) Undersök om det finns någon grupp G med delgrupper H och K sådana att $H \not\subseteq K$, $K \not\subseteq H$ men $H \cup K$ är en delgrupp till G.

   Lösning: Nej någon sådan grupp finns inte, ty enligt förutsättningarna finns

   $$h \in H \setminus K \ , \qquad k \in K \setminus H \ ,$$

   och om nu $H \cup K$ vore en grupp skulle, eftersom både h och k tillhör $H \cup K$,

   $$g = hk \in H \cup K \ .$$

   Antag $g \in H$ (fallet $g \in K$ behandlas analogt). Då gäller

   $$k = h^{-1}g \in H \ ,$$

   eftersom både g och h tillhör H. Detta strider mot hur k var definierat.

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. Det sägs ju att alla lika stora ändliga kroppar är isomorfa, och det handlar det om nu.

   (a) (1p) Ge en lämplig definition av vad som menas med att två kroppar K och F är isomorfa.

(b) (2p) Låt K vara den kropp med åtta element som definieras med hjälp av polynomet $p(x) = x^3 + x^2 + 1$, som ju är irreducibelt i $Z_2[x]$ och F den kropp med åtta element som definieras med hjälp av polynomet $q(x) = x^3 + x + 1$ som är irreducibelt i $Z_2[x]$. Beskriv en isomorfi mellan K och F.

Ett svar som saknar motivering ger noll poäng.

(c) (2p) Bestäm antalet olika isomorfier mellan K och F.

Lösning: Vi löser de tre deluppgifterna i ett svep:

Med en *isomorfi* menar vi en bijektiv avbildning φ från K till F sådan att för alla kroppselement a och b gäller

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \text{och} \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \ .$$

Vi utgår nu från att det finns minst en isomorfi φ_1 mellan kropparna och bestämmer först hur många olika isomorfier φ_i, $i = 1, 2, 3 \ldots$ det finns. Vi ser att avbildningen ψ_i definierad genom

$$\psi_i = \varphi_i^{-1}\varphi_1 \ ,$$

är en isomorfi som avbildar K på sig själv, en så kallad automorfi. Och antalet sökta isomorfier blir således lika med antalet automorfier av K.

Vi hittar nu tre automorfier av kroppen K på sig själv:

$$\psi_1(x) = x \ , \qquad \psi_2(x) = x^2 \ , \qquad \psi_3(x) = x^4 \ ,$$

som ju är automorfier eftersom, t ex,

$$\psi_2(x+y) = (x+y)^2 = x^2 + y^2 = \psi_2(x) + \psi_2(y)$$

och

$$\psi_2(xy) = (xy)^2 = x^2y^2 = \psi_2(x)\psi_2(y) \ .$$

Finns det fler automorfier? Eftersom för elementet x i K gäller att $x^3 + x^2 + 1 = 0$ så måste också

$$0 = \psi_i(x^3 + x^2 + 1) = \psi_i(x)^3 + \psi_i(x)^2 + 1 \ .$$

Slutsatsen är att $z = \psi_i(x)$ måste vara ett nollställe till polynomet $z^3 + z^2 + 1$. Och det finns högst tre nollställen till detta polynom, (grad 3). Vidare, om $\psi_i(x) = w$, så $\psi_i(x^k) = w^k$ (eftersom ψ_i förusättes vara en isomorfi), så automorfin är entydigt bestämt av värdet $\psi_i(x)$ då varje element i K är en potens av x.

Eftersom vi funnit tre automorfier och visat att antalet automorfier är högst tre, finns det precis tre automorfier, och därmed precis tre isomorfier från K till F, eftersom, som utsagt var, det finns minst en isomorfi.

Nu till deluppgift b):

Nu vet vi att det finns tre isomorfier φ_1, φ_2 och φ_3 från K till F, och att dessa är bestämda av sitt värde y_i i punkten x, dvs av att $y_i = \varphi_i(x)$ för $i = 1, 2, 3$.

Då $x^3 + x^2 + 1 = 0$ i K måste, pga egenskaperna hos en isomorfi,

$$0 = \varphi_i(x^3 + x^2 + 1) = y_i^3 + y_i^2 + 1 \ .$$

Men i F gäller att $x^3 + x + 1 = 0$, vilket medför att

$$0 = (x^3 + x + 1)^2 = x^6 + x^2 + 1 = (x^2)^3 + x^2 + 1$$

$$0 = (x^3 + x + 1)^4 = x^{12} + x^4 + 1 = (x^4)^3 + x^4 + 1$$

Ett element i F kan inte både satisfiera ekvationen $z^3 + z^2 + 1 = 0$ och ekvationen $z^3 + z + 1 = 0$ så vår slutsats blir att

$$\varphi_i(x) \in \{\ y_1, y_2, y_3\ \} \subseteq F \setminus \{\ 0, 1, x, x^2, x^4\}$$

och ”uteslutningsmetoden” ger nu de tre isomorfierna.

$$\varphi_1(x) = x^3\ , \qquad \varphi_2(x) = x^5\ , \qquad \varphi(x) = x^6\ .$$

Anmärkning: Man kunde givetvis genom prövning visat att dessa tre funktioner är isomorfier och inga andra funktioner, dvs att t ex mängden

$$M = \{\ a_0 + a_1(x+1) + a_2(x+1)^2\ \mid\ a_0, a_1, a_2 \in Z_2\ \} \subseteq F\ ,$$

blir en kropp om man räknar som om $(x+1)^3 + (x+1)^2 + 1 = 0$.

10. (5p) Låt $\varphi(n)$ beteckna antalet tal m, med $1 \leq m \leq n$, som är relativt prima med n. Visa att för alla positiva hela tal n, och alla primtal p, gäller att n är en delare till $\varphi(p^n - 1)$.

Lösning: Betrakta mängden av inverterbara element i ringen Z_{p^n-1}, som utgör en grupp G med $\varphi(p^n - 1)$ stycken element. Elementet p tillhör denna grupp eftersom p är ett primtal som inte delar $p^n - 1$, och därför är relativt primt till $p^n - 1$. Eftersom det gäller att

$$p^n = 1\ ,$$

och

$$p^k < p^n\ , \qquad \text{för} \qquad k = 1, 2, \ldots, n-1\ ,$$

så har elementet p ordning n i G. Eftersom allmänt gäller att ett elementens ordning delar antalet element i gruppen ifråga, så kan vi sluta att n delar $\varphi(p^n - 1)$.