Matematiska Institutionen
KTH

Lösningar till entamensskrivning på kursen Diskret Matematik, moment B, för D2 och F, SF1631 och SF1630, den 19 augusti 2009 kl 14.00-19.00.

DEL I

1. (3p) Ett RSA-krypto har parametrarna $n = 65$ och $e = 7$. Dekryptera meddelandet 2, dvs bestäm $D(2)$.

   Lösning. Vi finner att $n = p \cdot q = 5 \cdot 13$ så $m = (p-1)(q-1) = 4 \cdot 12 = 48$. Det sökta dekrypterade meddelandet $D(2)$ ges av
   $$D(2) = 2^d \pmod{n},$$
   där $e \cdot d \equiv 1 \pmod{m}$. Med det givna värdet på $e = 7$ är det lätt att gissa värdet på d eftersom $7 \cdot 7 = 49 \equiv 1 \pmod{48}$. Vi får nu

   SVAR $D(2) = 2^7 \pmod{65} = -2 \pmod{65} = 63$.

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 01111011, och rätta ordet i så fall.

   Lösning. Vi finner att
   $$H \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix},$$
   vilket är matrisen H's sista kolonn, så ett fel uppstod i sista positionen.
   SVAR: Ordet går att rätta till ordet 01111010.

   (b) (1p) Bestäm antalet ord i C.

   Lösning. Ordlängden är 8 och kontrollmatrisen har 4 (linjärt oberoende) rader så
   SVAR: Antal ord i koden är $2^{8-4} = 16$.

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

   Lösning. Ord som går att rätta ligger på avstånd 1 från ett unikt kodord. Antal ord på avstånd 1 från ett givet kodord, vilket som helst, är $1 + 8 = 9$ eftersom ordlängden är 8. Totalt kan alltså $16 \cdot 9 = 144$ ord rättas. Eftersom det finns totalt $2^8 = 256$ ord så får vi
   SVAR: $256 - 144 = 112$ ord kan inte rättas.

3. (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

Visa att elementet a genererar gruppen och bestäm samtliga delgrupper till G.

Lösning. Elementet a genererar gruppen om a:s ording är 6, eftersom antalet element i gruppen är 6. Vidare är ordningen av a alltid en delare till 6, dvs 1, 2 eller 3. Vi testar:

$$a^2 = b \neq e, \qquad a^3 = a \circ a^2 = a \circ b = c \neq e.$$

Enda möjligheten är att a:s ordning är 6 vilket visar att a genererar gruppen.

Så gruppen är cyklisk och har då precis en delgrupp, som kommer att vara cyklisk, med d element för varje delare d till antalet element i gruppen. Vi finner följande delgrupper med 1, 6, 3 respektive 2 element

$$\{e\}, \qquad \{e, a, a^2, \dots\} = G, \qquad \{a^2, a^4, e\}, \qquad \{a^3, e\},$$

vilket alltså var vårt **SVAR.**

4. (3p) Bestäm ett irreducibelt andragradspolynom i polynomringen $Z_{11}[x]$.

Lösning. Vi kan t ex ta ett polynom av typen $p(x) = x^2 - a$ där a inte är en kvadrat i Z_{11}. Eftersom polynomet är av grad två och saknar nollställen kommer det att vara irreducibelt.

Kvadraterna i Z_{11} är

$$\mathcal{Q}_{11} = \{(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 = 5, (\pm 5)^2 = 3\}.$$

Så t ex följande

SVAR: $x^2 - 6$.

5. (3p) Går det att bestämma a och b och n så att nedanstående mängd H blir en sidoklass till en delgrupp till $(Z_n, +)$,

$$H = \{1, 6, 16, a, b\}$$

Lösning. Sidoklassen H består av fem element så motsvarande delgrupp K skall innehålla fem element och enligt Lagranges sats måste 5 dela talet n. Gruppen $(Z_n, +)$ är cyklisk och då är K också cyklisk. K innehåller elementet 0 så

$$H = 1 + K \qquad \text{där} \qquad K = \{0, 5, 15, a - 1, b - 1\}.$$

Med $a = 11$, $b = 21$ och $n = 25$ så blir H en sidoklass till delgruppen K till $(Z_n, +)$, vilket är vårt **:SVAR**

DEL II

6. Betrakta den ändliga kropp F som på sedvanligt sätt konstrueras med hjälp av det irreducibla polynomet $p(x) = x^3 + x + 1$ i polynomringen $Z_2[x]$.

   (a) (1p) Ange antalet element i F.

   Lösning. Kroppen består av åtta element, elementen i mängden
   $$\{a_0 + a_1x + a_2x^2 \mid a_0, a_1, a_2 \in Z_2\}.$$

   (b) (1p) Visa att elementet x genererar kroppens multiplikativa grupp.

   Lösning. Multiplikativa gruppen, dvs $F \setminus \{0\}$, består av sju element. Ordningen av elementen i denna grupp är alltså en delare till talet sju, dvs ett eller sju. Alla element utom elementet 1 har alltså ordning 7 och genererar multiplikativa gruppen, vilket alltså x gör.

   (c) (2p) Bestäm n så att $x^n = x^3 + x^2$.

   Lösning. Vi finner att
   $$\begin{aligned} x^4 &= x^3 \cdot x = (x+1)x = x^2 + x \\ x^5 &= x^4 \cdot x = (x^2 + x)x = x^3 + x^2. \end{aligned}$$

   SVAR: $x^5 = x^3 + x^2$

7. Betrakta ringen R bestående av elementen
   $$R = \{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in Z_3\},$$
   och där addition och multipliktion är sedvanlig matrisaddition resp matrismultiplikation fast räkningarna sker modulo 3.

   (a) (1p) Bestäm antalet element i R.

   Lösning. Det finns tre möjliga värden på vardera a, b och c som kan väljas oberoende av varandra, så ringen består av
   SVAR: nio element.

   (b) (1p) Är ringen kommutativ.

   Lösning. Matrismultilikation är generellt inte en kommutativ operation, med lite prövning får vi
   $$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix},$$
   så ringen är inte kommutativ.

   (c) (2p) Bestäm de element i R som är inverterbara.

   Lösning. Vi ser att
   $$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$
   och inverser är alltid entydigt bestämda. Dessutom är Z_3 en kropp vilket gör att om $ad - bc \neq 0$ så finns elementet $1/(ad - bc)$ också i Z_3.
   SVAR: Precis de matriser
   $$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$
   sådana att $ac \neq 0$ dvs när både a och c är skilda från noll.

8. (3p) Visa att till varje ändlig grupp G med gruppoperationen $\circ$ och identitetselement e finns minst ett primtal p och minst ett element $a \in G \setminus \{e\}$ sådant att $a^p = a \circ a \circ \cdots \circ a = e$

   Lösning. Eftersom gruppen är ändlig finns till varje element $b \in G$ ett naturlligt tal n, elementets ordning, sådant att $b^n = e$. Talet n delas av ett primtal p och med $a = b^{n/p}$ får vi

$$a^p = (b^{n/p})^p = b^n = e.$$

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) För vilka naturliga tal n gäller att mängden $Z_n \setminus \{0\}$ under operationen multiplikation i Z_n bildar en grupp $G = (Z_n \setminus \{0\}, \cdot)$. (Motivera ditt svar).

   Lösning. Vi vet att

$$a, b \in Z_n \qquad \Longrightarrow \qquad a \cdot b \in Z_n,$$

   ty Z_n är en ring. Så den givna mängden är sluten map multiplikation om och endast om

$$a, b \in Z_n \setminus \{0\} \qquad \Longrightarrow \qquad a \cdot b \not\equiv 0 \pmod{n},$$

   eller med andra ord att talet n inte delar produkten ab.
   Om nu n inte är ett primtal utan produkten av talen a och b så gäller

$$ab \equiv 0 \pmod{n},$$

   och mängden är inte sluten map multiplikation.
   Om n är ett primtal och $ab = 0$ i Z_n gäller att n delar ab vilket leder till att n delar minst ett av talen a och b, dvs a eller b är lika med noll i Z_n.
   SVAR: Precis när n är ett primtal har vi en grupp.

   (b) (2p) Visa att när den algebraiska strukturen G ovan bildar en grupp så kommer antalet element i snittet $H \cap K$ av två delgrupper H och K till G enbart att bero på antalet element i H och K.

   Lösning. Vi fann att strukturen var en grupp precis när n är ett primtal $n = p$. Då är Z_p en kropp. Multiplikativa gruppen hos en kropp är en cyklisk grupp G med $m = p - 1$ element. Alla delgrupper till G är då cykliska och till varje delare d till gruppens ordning finns precis en delgrupp med d element.
   Låt nu $d = \text{sgd}(h, k)$ där $h = |H|$ och $k = |K|$. Både H och K har vardera en delgrupp H_1 resp K_1 med d element som också då är delgrupper till G. Men G har ju bara en delgrupp med d element så $H_1 = K_1 \subseteq H \cap K$. Men $H \cap K$ är en delgrupp till både H och K och antalet element i detta snitt måste då dela största gemensamma delaren till h och k, dvs d. Så $H_1 = K_1 = H \cap K$.

   (c) (2p) Gäller det generellt för varje grupp G att antalet element i ett snitt $H \cap K$ av två delgrupper H och K till G enbart beror på antalet element i H och K. (Motivera ditt svar på lämligt sätt.)

   Lösning. Låt $G = (Z_2, +) \times (Z_2, +) \times (Z_2, +) \times (Z_2, +)$ och skriv elementen som 4-tiplar:

$$G = \{(x_1, x_2, x_3, x_4) \mid x_i \in Z_2,\ i = 1, 2, 3, 4\}.$$

Låt

$$H = \{(x_1, x_2, x_3, x_4) \in G \mid x_3 = x_4 = 0\},$$
$$K = \{(x_1, x_2, x_3, x_4) \in G \mid x_1 = x_2 = 0\},$$

och

$$L = \{(x_1, x_2, x_3, x_4) \in G \mid x_2 = x_3 = 0\}.$$

Då gäller att H, K och L är delgrupper till G med fyra element vardera samt att

$$H \cap K = \{(0,0,0,0)\}, \qquad \text{och} \qquad H \cap L = \{(0,0,0,0), (1,0,0,0)\},$$

så uppenbarligen gäller påståendet inte generellt.

10. (a) (1p) Ge en lämplig definition av vad som menas med att K är en delkropp till kroppen F.

Lösning. $K \subseteq F$, K är en kropp under samma operationer som gäller i F.

(b) (1p) Betrakta kroppen $F = \{a + b\sqrt{3} \mid a, b \in Q\}$, där Q betecknar de rationella talen. Ange en kropp $K \neq F$ som är en delkropp till F.

Lösning. $K = Q$

(c) (3p) Bestäm en kropp F som uppfyller följande krav

i. Q är innehållet i F.

ii. Ekvationerna $x^2 = 2$ och $x^2 = 3$ är lösbara i F.

och som är sådan att det inte finns någon kropp $K \subseteq F$ och $K \neq F$ som uppfyller ovanstående två krav.

Anmärkning. Det räcker med en kortfattad motivering för svaret på denna deluppgift, så inget stringent bevis krävs.

Lösning. Vi gör ett försök med mängden

$$F = \{a + b\sqrt{2} \mid a, b \in \{c + d\sqrt{3} \mid c, d \in Q\}\},$$

som innehåller Q samt talen $\sqrt{2}$ och $\sqrt{3}$. Mängden F är sluten under addition och multiplikation och F är en delmängd till kroppen av reella tal R så alla räknelagar i kroppen R kommer att gälla i F. Återstår att visa att alla element utom noll har en multiplikativ invers. Vi finner att

$$(a + b\sqrt{2})\frac{a - b\sqrt{2}}{a^2 - 2b^2} = 1.$$

Men elementet $a^2 - 2b^2 \neq 0$ och tillhör kroppen $\{c + d\sqrt{3} \mid c, d \in Q\}$ så elementet $(a^2 - 2b^2)^{-1}$ tillhör också denna kropp och $a + b\sqrt{2}$ har inversen

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Mängden F kan också beskrivas som

$$F = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in Q\},$$

och en mindre mängd än denna kommer inte att vara sluten under multiplikation och addition under de givna förutsättningarna. Vår funna kropp är den sökta.