Matematiska Institutionen
KTH

Lösningar till några övningar, inför tentan moment B, på de avsnitt som inte omfattats av lappskrivningarna, Diskret matematik för D2 och F, vt08.

1. Ett RSA-krypto har $n = 187$ och $e = 23$. Kryptera meddelandet 2 och dekryptera meddelandet 3.

   Lösning: För att ta reda på parametern m så faktoriserar vi talet $n = 187$. Vi finner att $187 = 11 \cdot 17$, och alltså att $m = (11-1)(17-1) = 160$. För dekrypteringsnyckeln d gäller alltid att $e \cdot d \equiv_m 1$. För att ta reda på d söker vi en lösning till den diofantiska ekvationen

   $$x \cdot 23 + y \cdot 160 = 1,$$

   med hjälp av Euklides algoritm:

   $$160 = 7 \cdot 23 - 1,$$

   och vi ser direkt en lösning till den diofantiska ekvationen

   $$7 \cdot 23 - 160 = 1.$$

   Räknar vi nu modulo 160 i likheten ovan finner vi att $23 \cdot 7 \equiv_{160} 1$ och alltså att $d = 7$.
   Vi krypterar nu meddelandet 2, dvs beräknar $E(2) = 2^{23} \pmod{187}$:

   $$2^{23} = 2^{16}2^4 2^2 2,$$

   och då

   $$2^2 = 4, \quad 2^4 = 16, \quad 2^8 \equiv_{187} 2^4 2^4 \equiv_{187} 16 \cdot 16 \equiv_{187} 69,$$
   $$2^{16} \equiv_{187} 69 \cdot 69 \equiv_{187} 86,$$

   ger

   $$E(2) \equiv_{187} 86 \cdot 16 \cdot 4 \cdot 2 \equiv_{187} 162.$$

   Vi dekrypterar nu meddelandet 3, dvs beräknar $D(3) = 3^7 \pmod{187}$:

   $$3^7 \equiv_{187} 3^4 3^2 3 \equiv_{187} 81 \cdot 9 \cdot 3 \equiv_{187} 243 \cdot 9 \equiv_{187} 56 \cdot 9 \equiv_{187} 504 \equiv_{187} 130.$$

   SVAR: $E(2) = 162$ och $D(3) = 130$.

   (**Anm. Svårighetsgraden i kalkylen på eventuella tentamenstal ligger i nivå med beräkningen av** $D(3)$**.**)

2. En 1-felsrättande kod C har kontrollmatrisen

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

   (a) Rätta ordet 111110.

   Lösning: Låt H beteckna den givna kontroll matrisen. Vi finner att

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

   vilket är den femte kolonnen i matrisen H och därmed felet var i position nummer 5. Vi rättar felet och det avsedda ordet var ordet 111100.

(b) Bestäm samtliga ord i C.

Lösning: C består av lösningarna till ekvationssystemet $H\bar{x}^T = \bar{0}$, där $\bar{x} = (x_1, x_2, \ldots, x_6)$, som vi löser på sedvanligt sätt t ex med hjälp av Gausselimination och i tablåform:

$$\left(\begin{array}{cccccc|c} 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

Vi låter $x_4 = s$, $x_5 = t$ och $x_6 = u$ och får

$$x_1 = s + t, \quad x_2 = s + u, \quad x_3 = s + t + u,$$

och alltså

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (s + t, s + u, s + t + u, s, t, u),$$

dvs

$$(x_1, x_2, x_3, x_4, x_5, x_6) = s(1, 1, 1, 1, 0, 0) + t(1, 0, 1, 0, 1, 0) + u(0, 1, 1, 0, 0, 1).$$

Det finns totalt åtta möjligheter att välja parametrarna s, t och u (eftersom de antingen är 0 eller 1) och vi får

SVAR:

$$C = \{000000, 111100, 101010, 011001, 010110, 100101, 110011, 001111\}.$$

(c) Hur många ord har avstånd minst två till samtliga ord i koden?

Lösning: Ord på avstånd ett från något kodord ligger i en sk 1-sfär. Antalet ord i en 1-sfär är

$$S_1(\bar{0}) = 1 + \binom{6}{1} = 7.$$

Eftersom koden C är ettfelsrättande är dessa 1-sfärer disjunkta. Då koden C innehåller precis åtta stycken ord ligger precis $8 \cdot 7 = 56$ ord på avståndet högst ett från precis ett kodord. Resterande $2^6 - 56 = 8$ ord har ett avstånd minst två till samtliga kodord.

SVAR: 8.

3. Konstruera en kropp med 49 element, dvs ange på lämpligt sätt de 49 elementen och beskriv hur dessa element adderas och multipliceras.

Lösning: Vi konstruerar kroppen med hjälp av ett irreducibelt polynom av grad 2 i polynomringen $Z_7[x]$, så låt oss först hitta ett sådant.

Vi undersöker först vilka element i Z_7 som är jämna kvadrater och finner att

$$Q_7 = \{(\pm 1)^2, (\pm 2)^2, (\pm 3)^2\} = \{1, 4, 2\}.$$

Det finns alltså inget element x i Z_7 sådant att $x^2 = 6$ och därmed skulle polynomet $p(x) = x^2 - 6$ sakna nollställen. Men om $p(x)$ ej skulle vara irreducibelt så skulle det, eftersom dess grad är två, ha faktorer av grad ett och därmed nollställen. Alltså är polynomet $x^2 - 6$ irreducibelt.

Nu kan vi beskriva en kropp med 49 element:

$$F_{49} = \{a + bx \mid a, b \in Z_7\},$$

där addition och multiplikation sker modulo 7 och där man ersätter x^2 med 6, dvs med -1.

4. Låt $\bar{c}_1 = 11100000$, $\bar{c}_2 = 00111000$ och $\bar{c}_3 = 11000111$ vara binära ord av längd 8.

   (a) Bestäm en linjär kod C med så få ord som möjligt och sådan att $\bar{c}_1, \bar{c}_2, \bar{c}_3 \in C$.

   Lösning: För en linjär kod C gäller att $\bar{c}, \bar{c}' \in C \Rightarrow \bar{c}+\bar{c}' \in C$. Alltså måste alla möjliga sätt att summera ihop de givna tre orden tillhöra C, eller mer precist C är det linjära höljet av de tre orden

   $$C =< 11100000, 00111000, 11000111 >,$$

   eller ekvivalent

   $$C = \{\lambda_1(1,1,1,0,0,0,0,0) + \lambda_2(0,0,1,1,1,0,0,0) + \lambda_3(1,1,0,0,0,1,1,1)\}$$

   där $\lambda_1, \lambda_2, \lambda_3 \in Z_2$.

   (b) Bestäm en kontrollmatris till den kod C du fann.

   Lösning: Låt $\bar{s} = (s_1, s_2, \ldots, s_7)$ vara en rad i den sökta kontrollmatrisen H. Eftersom $H\bar{c}_i = \bar{0}$, för $i = 1, 2, 3$, så ser vi ur definitionen av matrismultiplikation att

   $$\begin{cases} s_1 + s_2 + s_3 + 0s_4 + 0s_5 + 0s_6 + 0s_7 + 0s_8 = 0 \\ 0s_1 + 0s_2 + s_3 + s_4 + s_5 + 0s_6 + 0s_7 + 0s_8 = 0 \\ s_1 + s_2 + 0s_3 + 0s_4 + 0s_5 + s_6 + s_7 + s_8 = 0 \end{cases}$$

   Vi löser nu detta system pss som vi löste systemet i uppgift 2.

   $$\left(\begin{array}{cccccccc|c} 1&1&1&0&0&0&0&0&0\\ 0&0&1&1&1&0&0&0&0\\ 1&1&0&0&0&1&1&1&0 \end{array}\right) \sim \left(\begin{array}{cccccccc|c} 1&1&0&0&0&1&1&1&0\\ 1&1&1&0&0&0&0&0&0\\ 0&0&1&1&1&0&0&0&0 \end{array}\right) \sim$$

   $$\left(\begin{array}{cccccccc|c} 1&1&0&0&0&1&1&1&0\\ 0&0&1&0&0&1&1&1&0\\ 0&0&1&1&1&0&0&0&0 \end{array}\right) \sim \left(\begin{array}{cccccccc|c} 1&1&0&0&0&1&1&1&0\\ 0&0&1&0&0&1&1&1&0\\ 0&0&0&1&1&1&1&1&0 \end{array}\right).$$

   Vi sätter nu $s_2 = t$, $s_5 = s$, $s_6 = u$, $s_7 = v$ och $s_8 = y$. Vi får då

   $$s_1 = t + u + v + y, \quad s_3 = u + v + y, \quad s_4 = s + u + v + y,$$

   och

   $$(s_1, s_2, \ldots, s_8) = (t + u + v + y, t, u + v + y, s + u + v + y, s + u + v + y, u, v, y).$$

   Nu blir det linjär algebra. Lösningsrummet har dimension fem och spänns t ex upp av de vektorer man får om man väljer precis en av paramtrarna t, s, u, v och y till 1 och resten 0. Om vi skriver upp dessa vektorer i en matris får vi kodens kontrollmatris, eftersom matrisens rang blir fem och dess nollrum då är C som har dimension 3.

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

   (c) Bestäm en annan kontrollmatris till koden C.

Lösning: Addition av rader till andra rader i en matris ändrar inte matrisens nollrum, så tar vi t ex och adderar rad ett till rad två i matrisen H ovan får vi en annan kontrollmatris till C:

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

5. Använd det irreducibla polynomet $p(x) = x^4 + x + 1$ i $Z_2[x]$ för att konstruera en kropp F_{16} med 16 element. Bestäm samtliga generatorer till den multiplikativa gruppen i F_{16}.

Lösning: Söker först en generator till den multiplikativa gruppen. Denna grupp har 15 element så om inte ordningen av ett element z är 15 så är dess ordning 5 eller 3 (eller 1 om det rör sig om ettan). Elementet x har inte ordning 3 ty $x^3 = x^3 + 0x^2 + 0x + 0 \neq 1$. Då $x^4 = x+1$ så får vi att $x^5 = x(x+1) = x^2+x = 0x^3+x^2+x+0 \neq 1$ och alltså har elementet x ej heller ordning 5. Alltså är x en generator till den multiplikativa gruppen eftersom den enda möjliga ordningen av x uppenbarligen är 15.

Det gäller allmänt i en cyklisk grupp G med generator γ, $G =< \gamma >$, med n element att

$$\gamma^k \quad \text{genererar } G \quad \Longleftrightarrow \quad sgd(k, n) = 1.$$

I vårt specifika fall får vi generatorerna

$$\{\gamma, \gamma^2, \gamma^4, \gamma^7, \gamma^8, \gamma^{11}, \gamma^{13}, \gamma^{14}\},$$

eller i klartext

$$\gamma = x, \quad \gamma^2 = x^2, \quad \gamma^4 = x^4 = x + 1, \quad \gamma^8 = (x+1)^2 = x^2 + 1$$

samt

$\gamma^7 = \gamma^4\gamma^3 = x^4x^3 = (x+1)x^3 = x^4 + x^3 = x + 1 + x^3$
$\gamma^{11} = \gamma^8\gamma^3 = (x^2+1)x^3 = x^5 + x^3 = xx^4 + x^3 = x(x+1) + x^3 = x^3 + x^2 + x$
$\gamma^{13} = \gamma^2\gamma^{11} = x^2(x^3 + x^2 + x) = xx^4 + x^4 + x^3 = x(x+1) + (x+1) + x^3 = x^3 + x^2 + 1$
$\gamma^{14} = \gamma\gamma^{13} = x(x^3 + x^2 + 1) = x^4 + x^3 + x = x^3 + 1.$

(Alternativt hade det nog varit snabbare att först bestämma de element som inte är generatorer, dvs förutom elementet 1, de sex elementen

$$\gamma^3, \quad \gamma^5, \quad \gamma^6, \quad \gamma^9, \quad \gamma^{10}, \quad \gamma^{12}$$

dvs

$\gamma^3 = x^3$
$\gamma^5 = \gamma\gamma^4 = x(x+1) = x^2 + x$
$\gamma^6 = \gamma\gamma^5 = x(x^2+x) = x^3 + x^2$
$\gamma^9 = \gamma\gamma^6 = x^3(x^3+x^2) = x^4(x^2+x) = (x+1)(x^2+x) = x^3 + x$
$\gamma 10 = (x^2+x)^2 = x^4 + x^2 = x^2 + x + 1$
$\gamma^{12} = x^2(x^2+x+1) = x^4 + x^3 + x^2 = x^3 + x^2 + x + 1.$

De andra elementen än de ovan angivna är de sökta elementen.)

6. Bestäm med hjälp av sfärpackningsvillkoret en övre gräns för antalet ord i en e-felsrättande kod C bestående av binära ord av längd 10 för $e = 1$, $e = 2$ och $e = 3$. Bestäm också det maximala antalet ord linjära koder med dessa parametrar kan ha.

Lösning: Först fallet $e = 1$. Varje 1-sfär innehåller $S_1(\bar{0})| = 1 + \binom{10}{1} = 11$ ord så packingsvillkoret ger

$$|C| \leq \frac{2^{10}}{11} = \frac{1024}{11} = 93.09.. \quad ,$$

så högst 93 ord. En 1-felsrättande kod C som är linjär och av längd 10 har en kontrollmatris H bestående av 10 olika kolonner skilda från nollkolonnen. Detta ger att antalet rader är minst fyra, eftersom det finns högst sju olika kolonner till en matris med tre rader. Antal ord i koden C är $2^{10-rang(H)}$. Så flest antal ord i C får vi när H har fyra rader och H:s rang är fyra. Vi ger ett exempel som visar ett en sådan matris H verkligen finns:

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

Antalet ord i den linjära koden C är $2^{10-4} = 2^6 = 64$.

Nu till fallet $e = 2$. I detta fall ger packningsvillkoret att

$$|C| \leq \frac{2^{10}}{1 + \binom{10}{1} + \binom{10}{2}} = \frac{1024}{1 + 10 + 45} = 18.285714286... \quad ,$$

så $|C| \leq 18$.

Att avgöra storkleken på en maximal linjär kod med angivna parametrar är ett i det generella fallet svårt problem. I de specifika fallen går det med lite trial and error.

Kodens minimiavstånd måste vara fem, så minvikten av ord skilda från nollordet, som ju alltid ingår i en linjär kod, är fem. Summan av varje möjligt par av ord i koden tillhör koden och antalet ord är en tvåpotens.

Om ordet 11111111111 tillhör den sökta koden så måste de övriga orden ha precis vikt 5. Vi finner med ett sådant ord 1111100000 t ex såkommer koden även att innehålla summan av dessa ord, dvs ordet 0000011111. Koden hkan nu inte innehålla fler ord av vikt fem, ty t ex om ordet 1100011100 tillhörde koden skulle ordet 0000011111+1100011100=1100000011 tillhöra koden. Slutsatsen är att om 1111111111 tillhör koden så finns max fyra ord i koden.

Näst fall, med ett ord med vikt nio i koden hanteras på ett liknande sätt, liksom övriga fall.

Efter mycket möda och stort besvär finner man att man kan maximalt ha fyra ord i en linjär 2-fels rättande kod av längd 10.

Nu till fallet $e = 3$. I detta fall ger packningsvillkoret att

$$|C| \leq \frac{2^{10}}{1 + \binom{10}{1} + \binom{10}{2} + \binom{10}{3}} = \frac{1024}{1 + 10 + 45 + 120} = 5.818181818... \quad ,$$

så $|C| \leq 5$.

Antalet element i en linjär kod är alltid en potens av talet två, dvs 1, 2, 4, eller 8 osv. Minavståndet i en 3-felsrättande kod är ju $2 \cdot 3 + 1$ dvs 7. Nollordet 00000000000 finns alltid med i den linjära koden och alla andra ord måste ha vikten minst sju. Men adderar man två ord av vikt minst sju, t ex som nedan:

$$1111111000 + 0001111111 = 1110000111,$$

så ser man att deras summa har vikten högst sex. I en linjär kod C gäller att summan av två godtyckligt valda ord i C alltid tillhör C. Alltså kan en 3-felsrättande linjär kod av längd 10 innehålla högst ett ord skild från nollordet.

SVAR: En linjär 3-felsrättande kod av längd 10 innehåller högst två ord.

7. Bestäm antalet rötter till ekvationen $z^4 = 1$ i kroppen F_{128} med 128 element.

   Lösning: Multiplikativa gruppen till en kropp med 128 element är en cyklisk grupp med 127 element. Om $z^4 = 1$ så vet vi att ordningen av elementet z delar talet 4. Men ingen delare d till talet 4 delar talet 127 förutom $d = 1$. Så den enda lösningen är det element i den multiplikativa gruppen till F_{128} som har ordning 1 dvs elementet 1.

   SVAR: Endast en lösning.

8. Kroppen F_9 konstrueras på sedvanligt sätt och med hjälp av det irreducibla polynomet $p(x) = x^2 + 1$.

   (a) Lös ekvationen $z^2 = 2$.

   Lösning: Multiplikativa gruppen i kroppen är cyklisk och vi börjar med att söka en generator till den. Elementen i F_9 äro

   $$F_9\{0, 1, 2, x, 2x, x + 1, x + 2, 2x + 1, 2x + 2\},$$

   och man räknar som om $x^2 = -1$.
   Elementet x kan inte vara en generator ty $x^4 = 2^2 = 1$ så ordningen av x är 4 (Obs vet redan att ordningen av x inte är två eftersom $x^2 = 2$.)
   Provar nu om elementet $x + 1$ har ordning 8, och därmed en generator till den multipliktiva gruppen.

   $$(x + 1)^2 = x^2 + 2x + 1 = -1 + 2x + 1 = 2x \neq 1, \quad (x + 1)^4 = (2x)^2 = x^2 = 2 \neq 1.$$

   Således har elementet $x + 1$ varken ordning 1, 2 eller 4. Enda möjligheten är att elementets ordning är 8 och därmed en generator till den multiplikativa gruppen.
   Beteckna $x + 1$ med γ.
   Söker nu z sådant att $z^2 = 2$. Ansätt $z = \gamma^k$. Från räkningarna ovan vet vi att $2 = \gamma^4$ och att $\gamma^s = \gamma^t \Leftrightarrow s \equiv_8 t$. Vi får nu att

   $$z^2 = 2 \Leftrightarrow \gamma^{2k} = \gamma^{4+n8} \Leftrightarrow 2k = 4 + 8n \Leftrightarrow k = 2 + 4n.$$

   Alltså

   $$z = \gamma^{2+4n} = \gamma^2 \cdot (\gamma^4)^n = 2x \cdot (-1)^n.$$

   SVAR: $z = \pm 2x$.

   (b) Lös ekvationen $z^2 = x + 1$.

   Lösning: Som ovan söker vi $z = \gamma^k$ sådant at $\gamma^{2k} = \gamma^{1+8n}$. Detta ger att

   $$2k = 1 + 8n$$

   för några tal k och n vilket ju är en orimlighet. Alltså finns inga lösningar i detta fall

   (c) Lös ekvationen $z^2 = x$.

   Lösning: Från ovan finner vi att $\gamma^2 = 2x = -x$ och då $-1 = \gamma^4$ så får vi att $x = -1(-x) = \gamma^6$. Återigen ger ansatsen $z = \gamma^k$ en lösning till ekvationen via likheten $\gamma^{2k} = \gamma^{6+8n}$, eller $2k = 6 + 8n$ eller $k = 3 + 4n$. Men

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

   Alltså
   SVAR: $z = \pm(2x + 1)$

9. Går det att använda den sk pq-formeln när man löser andragradsekvationer i ändliga kroppar eller är generellt metoden med kvadratkomplettering, dvs

$$x^2 + px + q = 0 \quad \Longleftrightarrow \quad (x + \frac{p}{2})^2 - \frac{p^2}{4} + q = 0$$

att föredra?

Lösning: Metoderna är i princip desamma och man hamnar i att bestämma alla lösningar till en ekvation av typen $z^2 = a$, där $a = \frac{p^2}{4} - q$. Dock när kroppens karakteristik är två, dvs kroppar med ett antal element som är en potens av två, så fungerar varken pq-formeln eller metoden med kvadratkomplettering eftersom vi aldrig kan dela med två i sådana kroppar.

10. Herr A vill efter att ha löst uppgifterna ovan nu tillslut konstruera en kropp med 81 element och på snabbast möjliga sätt. Hjälp honom.

Lösning: Från uppgift 8) vet vi att polynomet $p(z) = z^2 - (x + 1)$ saknar nollställen i den i denna uppgift definierade kroppen F_9 med nio element. Polynomet $p(z)$ kan alltså inte faktoriseras i icke-triviala faktorer i polynomringen $F_9[z]$ och är därför irreducibelt. Vi bildar nu

$$F_{81} = \{\alpha + \beta z \mid \alpha, \beta \in F_9\},$$

och där vi räknar som om $z^2 = x + 1$. Detta blir en kropp med 81 element.