MATEMATISKA INSTITUTIONEN
KTH
Examinator: Olof Heden
Telefon: 0730 547 891

Lösningar till tenta B i 5B1204 DISKRET MATEMATIK för D och 5B1203 DISKRET MATEMATIK för F3 och F1spec den 21 maj 2007.

1. (3p) Formulera och bevisa Faktorsatsen för polynomringen över en ändlig kropp.

2. (3p) Ett RSA-krypto har de offentliga nycklarna $n = 33$ och $e = 7$. Dekryptera meddelandet 5.

   Lösning: Då $n = 33 = 3 \cdot 11$ har vi att $m = 2 \cdot 10 = 20$. Dekrypteringsnyckeln d skall satisfiera $e \cdot d = 1$ i ringen Z_m. Då $e = 7$ finner vi, med hjälp av multiplikationstabellen att $d = 3$. Det dekrypterade meddelandet är ju $D(5) = 5^d \pmod{33}$. Då $5^3 = 125 \equiv_{33} 26$ har vi

   Svar: 26.

3. (3p) Gruppen $(Z_{19} \setminus \{0\}, \cdot)$ är cyklisk. Bestäm ett element α som genererar denna grupp.

   Lösning: Den givna gruppen $G = (Z_{19} \setminus \{0\}, \cdot)$ har 18 element, så vi skall bestämma ett element av ordning 18. Vi använder att för varje element $g \in G$ gäller att $\sigma(g)|18$. Vi börjar med att testa om elementet 2 har ordning 18:

   $2^2 = 4 \neq 1 \implies \sigma(2) \neq 2.$
   $2^3 = 8 \neq 1 \implies \sigma(2) \neq 3.$
   $2^6 = 7 \neq 1 \implies \sigma(2) \neq 6.$
   $2^9 = 18 \neq 1 \implies \sigma(2) \neq 9.$

   Då givetvis $\sigma(2) \neq 1$ så finns bara möjligheten att $\sigma(2) = 18$ kvar.

   Svar: Elementet 2 genrererar $(Z_{19} \setminus \{0\}, \cdot)$.

4. (3p) Undersök om polynomet $x^3 + x + 1$ är irreducibelt i polynomringen $Z_7[x]$.

   Lösning: Vore det inte irreducibelt skulle polynomet ha en faktoruppdelning

   $$x^3 + x + 1 = p(x)q(x) = (x - \alpha)q(x).$$

   Elementet α vore då ett nollställe till polynomet. Vi testar om $x^3 + x + 1$ har nollställen in Z_7:

   $$\begin{array}{lcll} 0^3 + 0 + 1 & = & 1 & \neq 0 \\ 1^3 + 1 + 1 & = & 3 & \neq 0 \\ 2^3 + 2 + 1 & = & 4 & \neq 0 \\ 3^3 + 3 + 1 & = & 3 & \neq 0 \\ 4^3 + 4 + 1 & = & 6 & \neq 0 \\ 5^3 + 5 + 1 & = & 5 & \neq 0 \\ 6^3 + 6 + 1 & = & 6 & \neq 0 \end{array}$$

   Tabellen ovan visar att polynomet $x^3 + x + 1$ saknar nollställen i Z_7 och är alltså irreducibelt i $Z_7[x]$.

5. (3p) Kroppen F med 25 element består av polynom av grad högst 1, med koefficienter i Z_5, och man räknar i F som om $x^2 + 2 = 0$. Dvs

   $$F = \{ax + b \mid a, b \in Z_5\} \quad \text{och} \quad x^2 = 3.$$

   Bestäm ett element z i denna kropp sådant att $(2x + 1)z = x$.

   Lösning: Först söker vi inversen till $2x + 1$ i kroppen F. Euklides algoritm ger

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

Varur vi direkt finner att $1 = (x^2+2) - (3x+1)(2x+1)$ eller

$$(2x+4)(2x+1) = 1 - (x^2+2).$$

Inversen till $2x+1$ är alltså $2x+4$.

Det gäller då att

$$z = (2x+1)^{-1}x = (2x+4)x = 2x^2 + 4x = 2 \cdot 3 + 2x = 4x + 1.$$

Svar: $z = 4x + 1$.

6. (3p) Visa att nedanstående, ej färdigt ifyllda tabell, aldrig kan kompletteras till en grupptabell:

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

Lösning: Ur tabellen framgår att $a \circ e = a$ vilket ger att e är det unika identitetselementet i gruppen. För elementet a gäller att $a \circ a = e$. Om det funnes en grupp med den givna multiplikationstabellen skulle gruppen bestå av fem element, varav ett av elementen, elementet a, skulle ha ordning 2. Då talet 2 inte delar talet 5 så är detta omöjligt. Det finns ingen grupp med denna egenskap.

7. (3p) Tyvärr råkade någon välja en oäkta kontrollmatris (paritycheck-matrix) för att skapa en 1-felsrättande kod, enligt nedan:

$$C = \{\bar{c} = (c_1, c_2, \ldots, c_7) \mid H\bar{c}^T = (0\,0\,0)^T\} \quad \text{där} \quad H = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Det är för sent att ändra så vissa ord i koden går inte att använda. Man måste därför utesluta ord ur C och skapa en ny 1-felsrättande kod C', dvs

$$C' \subseteq C, \quad \text{och} \quad C' \quad \text{är 1-felsrättande.}$$

Hur många ord kan C' ha maximalt, givet kontrollmatrisen H ovan. (Denna kontrollmatris skall vid felrättning användas på sedvanligt sätt.)

Lösning:

Felet med matrisen är att kolonn nummer ett och kolonn nummer fyra överensstämmer. Då kommer t ex C att innehålla ordet $\bar{f} = 1001000$.

Låt $\bar{e}_i$ beteckna ett ord med en etta i position i och med nollor för övrigt. Betrakta C och två ord $\bar{c}$ and $\bar{c}'$ i C som ligger på ett avstånd ett två från varandra. Då gäller att

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = H\bar{c}^T + H\bar{c}'^T = H(\bar{c} + \bar{c}')^T = H(\bar{e}_i + \bar{e}_j)^T = H\bar{e}_i^T + H\bar{e}_j^T = \text{kolonn } i \text{ plus kolonn } j.$$

Slutsatsen är att om $\bar{c}$ och $\bar{c}'$ ligger på avstånd två från varandra så gäller att

$$\bar{c}' = \bar{c} + \bar{f}.$$

Koden C är en linjär kod som spänns upp av fyra vektorer $\bar{g}_1$, $\bar{g}_2$, $\bar{g}_3$ och $\bar{g}_4$, dvs löser vi systemet $H\bar{c}^T = \bar{0}$, får vi lösningarna

$$\bar{c} = x_1\bar{g}_1 + x_2\bar{g}_2 + x_3\bar{g}_3 + x_4\bar{g}_4, \quad \text{där} \quad x_i \in Z_2, \quad i = 1, 2, 3, 4,$$

där vi har möjlighet att låta $\bar{g}_1 = \bar{f}$. Så samtliga element i C kan skrivas

$$\bar{c} = x_1\bar{f} + x_2\bar{g}_2 + x_3\bar{g}_3 + x_4\bar{g}_4, \quad \text{där} \quad x_i \in Z_2, \quad i = 1, 2, 3, 4.$$

Enligt vårt första resonemang, om orden $\bar{c}$ och $\bar{c}'$ i C har ett inbördes avstånd av två så gäller, med

$$\bar{c} = x_1\bar{f} + x_2\bar{g}_2 + x_3\bar{g}_3 + x_4\bar{g}_4, \quad \text{där} \quad x_i \in Z_2, \quad i = 1, 2, 3, 4,$$

och

$$\bar{c}' = x_1'\bar{f} + x_2'\bar{g}_2 + x_3'\bar{g}_3 + x_4'\bar{g}_4, \quad \text{där} \quad x_i \in Z_2, \quad i = 1, 2, 3, 4,$$

att $x_1 \neq x_1'$ men $x_i = x_i'$ för $i = 2, 3, 4$.

Det finns 8 olika val av kombinationerna (x_2, x_3, x_4). Varje val av minst nio ord i koden C kommer ge att ett en kombination (x_2, x_3, x_4) kommer att förekomma två gånger och ge två ord i koden som ligger på ett avstånd två från varandra. Sluitsatsen är att fler än åtta ord kan vi aldrig ha. Låter vi däremot

$$C' = 0\bar{f} + x_2\bar{g}_2 + x_3\bar{g}_3 + x_4\bar{g}_4, \quad \text{där} \quad x_i \in Z_2, \quad i = 1, 2, 3, 4,$$

får vi en kod med åtta ord och med ett minimiavstånd av tre.

Svar: 8.

8. (3p) Låt H och K vara två delgrupper till en grupp G. Räcker nedanstående information för att bestämma antalet element i $H \cap K$.

   1) Gruppen G är cyklisk.

   2) Antalet element i H är n.

   3) Antalet element i K är m.

Lösning: Vi visar att informationen räcker. Vi använder satsen som säger att *om G är en cyklisk grupp så är varje delgrupp till G en cyklisk grupp och till varje delare d till antalet element i G finns precis en delgrupp till G med d stycken element (om G cyklisk alltså).*

Låt nu

$$D = sgd(|H|, |K|).$$

Då gäller att D delar $|H|$ och $|K|$, men även $|G|$ eftersom, enligt Lagranges sats, $|H|$ delar $|G|$. Enligt satsen är även H och K cykliska grupper. Det finns alltså, återigen enligt satsen, delgrupper L, L_H och L_K till G, H och K respektive som samtliga har precis D stycken element.

Grupperna L_H och L_K är delgrupper även till G, och eftersom G bara har en delgrupp med D element så måste

$$L_H = L = L_K.$$

Då L delgrupp till både H och K så måste L vara en delgrupp till $H \cap K$, och därmed

$$D = |L| \leq |H \cap K|.$$

$H \cap K$ är en delgrupp till både H och K, så antalet element i $H \cap K$ delar både $|H|$ och $|K|$. Eftersom då $|H \cap K|$ delar både $|H|$ och $|K|$ så gäller att $|H \cap K|$ delar talet D. Således

$$|H \cap K| \leq D.$$

Enda möjligheten är att $|H \cap K| = |L| = D = sgd(n, m)$.