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 22 augusti 2007.

1. Se läroboken.

2. Vi bestämmer först d ur sambandet $e \cdot d \equiv 1 \pmod{m}$ där om $n = p \cdot q$ så $m = (p-1)(q-1)$. Då $143 = 11 \cdot 13$ så $m = 120$. Euklides algoritm ger

   $$\begin{array}{rcrcr} 120 & = & 103 & + & 17 \\ 103 & = & 6 \cdot 17 & + & 1 \end{array}$$

   varur vi får

   $$1 = 103 - 6 \cdot 17 = 103 - 6(120 - 103) = 7 \cdot 103 - 6 \cdot 120 \equiv_{120} 7 \cdot 103.$$

   Härav sluter vi att $d = 7$. Det gäller då att

   $$D(3) = 3^7 \pmod{143} = 3^5 3^2 \pmod{143} = 243 \cdot 9 \pmod{143} = 100 \cdot 9 \pmod{143} = 42$$

   Svar: 42.

3. Ett element a i Z_{30} är inverterbart, precis då $sgd(a, 30) = 1$. De inverterbara elementen är då

   $$G = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

   Gruppen har åtta element. Vore den cyklisk så skulle det finnas ett element av ordning 8. När vi undersöker om ett sådant finns använder vi oss av kunskapen att elementens ordningar delar antalet element i gruppen dvs i detta fall 8. Vi testar nu elementen.

   $$7^2 = 19 = -11, \quad 7^4 = (-11)^2 = 1$$

   Vi sluter att ordningen av elementet 7 är fyra, ordningen av elementet 19, liksom 11 är två och att ordningen av elementet 23, dvs -7 ochså är fyra. Elementet 29, dvs -1 är också två. Det skall nu bli mycket spännande att se vad elementet 13 har för ordning.

   $$13^2 = 19 \quad \Rightarrow \quad 13^4 = 19^2 = 1.$$

   Så inget element i gruppen har ordning åtta och gruppen kan inte vara cyklisk.

4. Vi använder Euklides algoritm:

   $$2x^5 + x^3 + 2x + 1 = (2x + 1)(x^4 + x^3 + x + 1) + x^2 + 2x.$$

   $$x^4 + x^3 + x + 1 = (x^2 + 2x + 2)(x^2 + 2x) + 1.$$

   Den sista ickeförsvinnande resten är uppenbarligen 1 och därmed

   Svar: Den största gemensamma delaren är ett.

5. Mängden är inte sluten under multiplikation ty t ex

   $$\begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 4 \end{pmatrix},$$

   så det är inte någon ring.

6. Vår lösning bygger på att vi först, med hjälp av en kontrollmatris, skapar en 1-felsrättande kod med 64 stycken ord,

   a) innehållande bland andra ordet $\bar{1} = 1111111111$,

   b) men inte ordet 0000111111.

   Koden innehåller då ett ord $\bar{c}$ på avstånd ett från detta ord, och vi skall ej ta bort ordet $\bar{c}$, men vi tar bort ordet $\bar{1}$.

   Kontrollmatrisen skall vara av formatet 10 kolonner och $10 - 6$ stycken rader, ty då kommer vi att få precis 64 stycken kodord. Lite trial and error ger kontrollmatrisen

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

   Så låt C vara den 1-felsrättande kod som denna matris ger. Koden C innehåller ordet $\bar{1}$ och ordet $\bar{c} = 1000111111$ på avstånd 1 från ordet 0000111111. Vi ser också att ordet $\bar{d} = 1011000001$ tillhör C och ligger på avstånd ett från ordet 1111000000. Vidare ligger ordet 0011111110 i C och har ett avstånd tre till ordet $\bar{1}$.

   Vår lösning av problemet är alltså att ta bort tre ord från C, ett av de borttagna orden skall vara $\bar{1}$, och de två andra skall inte vara något av orden $\bar{c}$ eller $\bar{d}$.

7. Den symmetriska gruppen S_3, bestående av alla permutationer på mängden $\{1, 2, 3\}$, innehåller precis sex element. Gruppen S_3 är inte abelsk. Gruppen $(Z_5, +)$ innehåller precis fem element. Den direkta produkten

$$(Z_5, +) \times S_3$$

   är en ickeabelsk grupp med $5 \cdot 6 = 30$ element.

8. (a) F är en delkropp till K om F med samma operationer som i K utgör en kropp och om varje element i F också är ett element i K.

   (b) Multiplikativa gruppen till en kropp med åtta element består av sju element. Om F_4 skulle vara en delkropp till en kropp med åtta element skulle dess multiplikativa grupp vara en delgrupp till multiplikativen gruppen till kroppen med åtta element. Enligt Lagranges sats, skulle då antalet element i denna multiplikativa grupp, dvs talet 3, dela talet 7. Detta är ju omöjligt.

   (c) Vi behöver ett irreducibelt polynom av grad två i polynomringen $F_4[x]$. För att underlätta sökandet skriver vi upp multiplikationstabellen för den multiplikativa gruppen i F_4:

$\cdot$	1	i	$i+1$
1	1	i	$i+1$
i	i	$i+1$	1
$i+1$	$i+1$	1	i

   Vi finner att polynomet $p(z) = z(z+1)$ antar följande värden

$$p(0) = 0, \quad p(1) = 0, \quad p(i) = 1, \quad p(i+1) = 1.$$

   Polynomet $q(z) = p(z) + i$ har då inget nollställe eftersom

$$q(0) = 0 + i, \quad q(1) = 0 + i, \quad q(i) = 1 + i, \quad q(i+1) = 1 + i.$$

   Den sökta kroppen består alltså av elementen i mängden

$$F_{16} = \{\alpha_0 + \alpha_1\tau \mid \alpha_0, \alpha_1 \in F_4\},$$

   och där man räknar som om $\tau(\tau + 1) + i = 0$, dvs som om

$$\tau^2 = \tau + i,$$

   eftersom vi använder oss av det irreducibla polynomet $q(z) = z^2 + z + i$ vid konstruktionen av kroppen F_{16}