1	2	3	4	5	TOPLAM

Adı ve Soyadı :
Numarası :
İmza :

CEVAP ANAHTARI

19.04.2019

KODLAMA TEORİSİ II ARA SINAV SORULARI

1. $\mathbb{Z}_3[x]/<x^2+x+2>\cong GF(3^2)$ **cisminin elemanlarını kök kabul eden minimal polinomları bulunuz.**

$p(x) = x^2+x+2$

$p(\beta)=0 \implies \beta^2 = 1-\beta$

$\beta^3 = 2\beta+2$

$\beta^4 = 2$

$\beta^5 = 2\beta$

$\beta^6 = \beta+2$

$\beta^7 = \beta+1$

$\beta^8 = 1$

$C_0 = \{0\}$

$C_1 = \{1,3\}$

$C_2 = \{2,6\}$

$C_4 = \{4\}$

$C_5 = \{5,7\}$

$m_0(x) = (x-\beta^0) = x+2$

$m_1(x) = m_3(x) = (x-\beta)(x-\beta^3) = x^2+x+2$

$m_2(x) = m_6(x) = x^2+1$

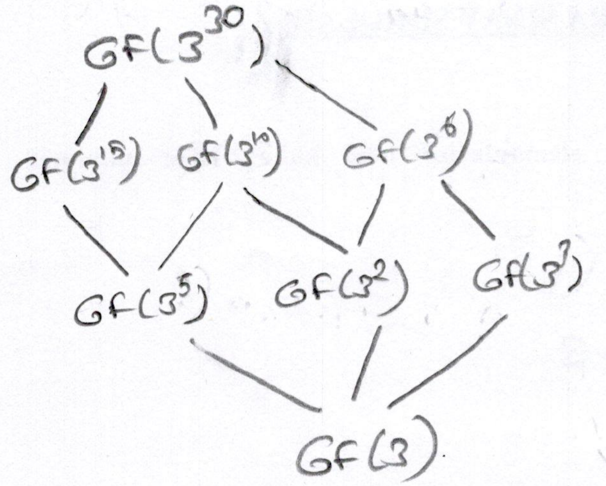
$m_4(x) = x+1$

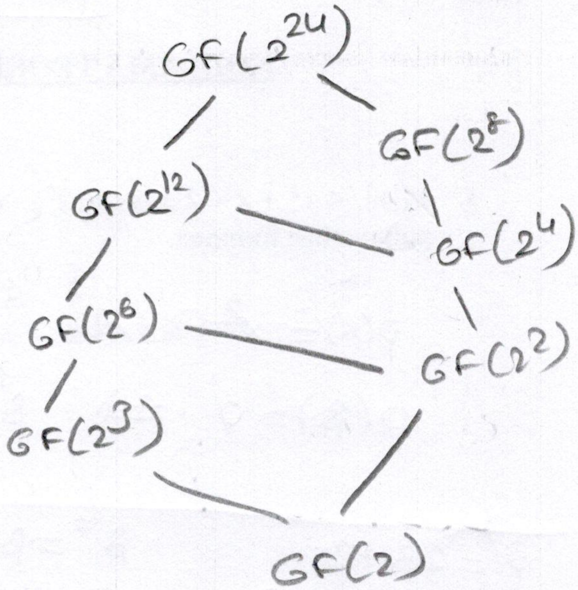
$m_5(x) = m_7(x) = x^2+2x+2$

2. *i)* $GF(3^{30})$ ve $GF(2^{24})$ **cisimlerinin alt cisimlerinin oluşturduğu kafesleri çiziniz.**

$d|30$ olmak üzere $GF(3^d)$ alt cisimler

$m|24$ olmak üzere $GF(2^m)$ alt cisimler





ii) $\mathbb{F}_2[x]/<x^2+x+1> \cong \mathbb{F}_4$ **cisminin çarpma işlemine göre çarpım tablosunu oluşturunuz.**

$p(x) = x^2+x+1$ $\qquad F_4 = \{0, 1, \beta, \beta^2 = \beta+1\}$

$p(\beta) = 0$

$\cdot$	0	1	β	β^2
0	0	0	0	0
1	0	1	β	β^2
β	0	β	β^2	1
β^2	0	β^2	1	β

$\beta^2 = \beta+1$

$\beta^3 = 1$

$\beta^4 = \beta$

3. $i)$ $x^7 - 1 \in \mathbb{Z}_2[x]$ **polinomunu çarpanlara ayırınız.**
(Primitif polinom : $x^3 + x + 1 \in \mathbb{Z}_2[x]$ **)**

$ii)$ **Uzunluğu** $n = 7$, **boyutu** $k = 4$ **olan** $\mathbb{Z}_2$ **üzerinde tanımlı devirli kodların üreteç polinomlarını ve üreteç matrislerini bulunuz.**

i) $2^s \equiv 1 \pmod 7 \Rightarrow s = 3$

$$K = \mathbb{Z}_2[x] / \langle x^3+x+1 \rangle$$
$$|$$
$$\mathbb{Z}_2$$

$p(x) = x^3+x+1$

$p(\beta) = 0$

$$\left.\begin{array}{l} C_0 = \{0\} \\ C_1 = \{1,2,4\} \quad , \quad w = \beta \\ C_3 = \{3,6,12=5\} \end{array}\right\} \Longrightarrow x^7 - 1 = M_0(x)\, M_1(x)\, M_3(x)$$

$M_0(x) = x+1$

$M_1(x) = (x-\beta)(x-\beta^2)(x-\beta^4) = x^3+x+1$

$M_3(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+x^2+1$

$\Rightarrow x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$

ii) $n-k = \text{der}(g(x))$

$C_1 = \langle x^3+x+1 \rangle$, $G_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

$C_2 = \langle x^3+x^2+1 \rangle$, $G_2 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$

4. F_2 **cismi üzerinde tanımlı** $n = 15,\ d = 5$ **olan** ***BCH*** **kodunu oluşturunuz.**

$2^s \geq 16 \Rightarrow s = 4$

$F_2[x] / \langle x^4+x+1 \rangle$

$|$

F_2

$p(x) = x^4+x+1$

$p(\beta) = 0$

$C_0 = \{0\}$

$C_1 = \{1, 2, 4, 8\}$

$C_3 = \{3, 6, 9, 12\}$

$$M_1(x) = M_2(x) = M_4(x) = M_8(x) = (x-\beta)(x-\beta^2)(x-\beta^4)(x-\beta^8)$$
$$= x^4+x+1$$

$$M_3(x) = M_6(x) = M_9(x) = M_{12}(x) = (x-\beta^3)(x-\beta^6)(x-\beta^9)(x-\beta^{12})$$
$$= x^4+x^3+x^2+x+1$$

BCH kodunun üreteç polinomu ;

$$g(x) = [M_1(x), M_2(x), M_3(x), M_4(x)]$$
$$= [x^4+x+1,\ x^4+x^3+x^2+x+1]$$
$$= x^8+x^7+x^6+x^4+1$$

$$\therefore\ C = \langle x^8+x^7+x^6+x^4+1 \rangle$$

5. $i)$ K**, sonlu bir cisim,** $|K| = p^n$ **ve** F, K **cisminin bir alt cismi olsun. Bu durumda** $d|n$ **olmak üzere** $|F| = p^d$ **dir. Gösteriniz.**
$ii)$ $x^6 + x^5 + x^3$ $\mathbb{F}_2[x]/\langle x^7 - 1\rangle$ **bir idempotent eleman mıdır? Gösteriniz.**

i) K, $f_{p^n}(x) = x^{p^n} - x$ polinomunun parçalanma cismi olsun.

$$d|n \Rightarrow p^d - 1 \mid p^n - 1 \Rightarrow x^{p^d - 1} - 1 \mid x^{p^n - 1} - 1$$
$$\Rightarrow x^{p^d} - x \mid x^{p^n} - x$$
$$\Rightarrow f_{p^d}(x) \mid f_{p^n}(x)$$

K, $f_{p^d}(x)$ polinomunun parçalanma cismini içerir. Yani K, p^d elemanlı bir alt cisim içerir.

$\therefore$ $|F| = p^d$

ii) $(x^6+x^5+x^3)(x^6+x^5+x^3) = x^6 + x^8 + x^9 + x^8 + x^{10} + x^{11} + x^9 + x^{11} + x^{12}$
$= x^6 + x^{10} + x^{12}$
$= x^6 + x^3 + x^5$
$= x^6 + x^5 + x^3$

$\therefore$ $x^6 + x^5 + x^3$ bir idempotent elemandır.

Başarılar

Süre: 90 dakika