Ad-Soyad:

Numara:

29.03.2019

KODLAMA TEORİSİ II QUIZ SORULARI

1) F sonlu bir cisim ve K, F cisminin sonlu bir genişlemesi olsun. $[K:F] = d$ olmak üzere $|K| = |F|^d$ olduğunu gösteriniz. (20p)

2) $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) \in \mathbb{F}_2[x]$ olmak üzere 5 uzunluklu devirli kodları bulunuz. (40p)

3) a) $GF(7)$ cisminin primitif elemanlarını varsa bulunuz. (20p)

b) $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ primitif polinom olmak üzere $\mathbb{F}_8$ cisminin elemanlarını bulunuz. (20p)

CEVAPLAR

BAŞARILAR

1) $[K:F] = d$ $\quad d \begin{pmatrix} K \\ | \\ F \end{pmatrix}$

$\{\alpha_1, \alpha_2, \dots, \alpha_d\}$ taban elemanları olsun. $\forall k \in K$ için $a_i \in F$, $i = 1, 2, \dots, d$ olmak üzere

$$k = a_1\alpha_1 + a_2\alpha_2 + \dots + a_d\alpha_d$$

şeklinde tek türlü yazılır. $\forall i$ için a_i lerin sayısı $|F|$ kadar olduğundan $|K| = |F|^d$ dir.

2) • $g(x) = \langle \overline{x^5 - 1} \rangle$

$C = \{(\bar{0}, \bar{0}, \bar{0}, \bar{0}, \bar{0})\}$

- $g(x) = \langle \bar{1} \rangle$

  $C = \mathbb{F}_2^5$

- $g(x) = \langle \overline{x+1} \rangle$

  $k = 5 - 1 = 4$

$$G = \begin{bmatrix} \bar{1} & \bar{1} & \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \bar{1} & \bar{1} \end{bmatrix}_{4\times 5}$$

$$C = \{ (\bar{0},\bar{0},\bar{0},\bar{0},\bar{0}), (\bar{1},\bar{1},\bar{0},\bar{0},\bar{0}), \dots, (\bar{1},\bar{0},\bar{0},\bar{0},\bar{1}) \}$$

- $g(x) = \langle \overline{x^4+x^3+x^2+x+1} \rangle$

  $k = 5 - 4 = 1$ $\qquad G = [\bar{1}\ \bar{1}\ \bar{1}\ \bar{1}\ \bar{1}]$

$$C = \{ (\bar{0},\bar{0},\bar{0},\bar{0},\bar{0}), (\bar{1},\bar{1},\bar{1},\bar{1},\bar{1}) \}$$

3) a) $\langle \beta \rangle = \mathbb{Z}_7^*$

$a^6 \equiv 1 \pmod 7$ $\qquad (6, i) = 1$

$3^1 \longrightarrow 3$ $\qquad 3^4 \longrightarrow 4$

$3^2 \longrightarrow 2$ $\qquad 3^5 \longrightarrow \bar{5}$

$3^3 \longrightarrow 6$ $\qquad 3^6 \longrightarrow 1$

$\therefore \mathbb{Z}_7^* = \langle \bar{3} \rangle = \langle \bar{5} \rangle$

b) $|\mathbb{F}_8^*| = 7$ $\qquad \mathbb{F}_8^* = \langle \beta \rangle$

$\mathbb{F}_8 = \{ 0, 1, \beta, \beta^2, \dots, \beta^6 \}$

$\beta^3 + \beta + 1 = 0 \implies \beta^3 = \beta + 1$

k	β^k	$a_0 + a_1\beta + a_2\beta^2$
0	1	1 0 0
1	β	0 1 0
2	β^2	0 0 1
3	$\beta+1$	1 1 0
4	$\beta+\beta^2$	0 1 1
5	$\beta^2+\beta+1$	1 1 1
6	β^2+1	1 0 1

$$F_8 = \{0, 1, \beta, \beta^2, \beta+1, \beta+\beta^2, \beta^2+\beta+1, \beta^2+1\}$$