Problems

Note Title

www.ee.iitm.ac.in/~andrew

Click on "Courses"

Click on "EE512"

"Additional Questions"

(1) $x \in GF(32)$

$$Tr(x) = x + x^2 + x^4 + x^8 + x^{16}$$

(a) $Tr(x)^2 = x^2 + x^4 + x^8 + x^{16} + x = Tr(x)$

$$Tr(x)\left(Tr(x)+1\right) = 0$$

$$Tr(x) = \underline{0 \text{ or } 1}$$

(b) $Tr(x+y) = Tr(x) + Tr(y)$

(c) Find x s.t. $Tr(x) = 0$

$$Tr(x^2) = Tr(x) \longrightarrow ?$$

(2) Similar to (1)

(3) $f(x) = x^2 + x + k = 0$, $k \in GF(32)$

Variable $x \in GF(32)$

(a) $\exists x$ s.t. $x^2 + x + k = 0$. You can show $\underbrace{k + k^2 + k^4 + k^8 + k^{16}}_{Tr(k)} = 0$

(b) Find i & j s.t.

$f(k^i + k^j) = 0$

$k + (k^2 + k^8) + (k^2 + k^8)^2 = 0$

$k^2 + k^8$: one root of $f(x) = 0$

(4) $\alpha \in GF(2^m)$, primitive n^{th} root of unity

n: $1 + x + x^2 + \cdots + x^{n-2} + x^{n-1} = \sum_{i=0}^{n-1} x^i$ is irreducible over $GF(2)[x]$.

(a) $M_\alpha(x)$ over $GF(2)[x]$

$$f(x) = x^n + 1 \quad : \quad f(\alpha) = 0$$

$$(x+1)\left(\sum_{i=0}^{n-1} x^i\right) :$$

(b) Smallest +ve integer j s.t. $2^j = 1 \bmod n$

$$\alpha : \{1, 2, 2^2, 2^3, \ldots, 2^{n-2}, 2^{n-1} = 1\}$$
mod n $\qquad$ mod n

(5) $GF(16) = \{f(\alpha) \in GF(2)[\alpha] : \deg f(\alpha) \leq 3\}$

$$+, \times : \pi(\alpha) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$$

(a) Find $f_i(\alpha) \in GF(16)$ with minimal poly

$$x^4 + x^3 + 1$$

$$\overline{GF(16)} = \{a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 : a_i \in \{0, 1\}\}$$

$$\beta^4 + \beta^3 + 1 = 0$$

$$\beta \in \overline{GF(16)}, \text{ primitive}$$

$$M_{\beta^3}(x) = 1 + x + x^2 + x^3 + x^4$$

Isomorphism: $\beta^3 \leftrightarrow \alpha$

$1+\beta^3=\beta^4 \longleftrightarrow 1+\alpha$: should have $1+x^3+x^4$ as minimal poly.

$m_{\beta^4}(x)=x^4+x^3+1$

Check: $1+(1+\alpha)^3+(1+\alpha^4)$

$=1+1+\alpha+\alpha^2+\alpha^3+1+\alpha^4$

$=1+\alpha+\alpha^2+\alpha^3+\alpha^4=0$

(b) x^4+x+1

Use $\underline{\underline{\alpha^5=1}}$

Try $\underline{\underline{\alpha+\alpha^2}}$

$\alpha^4+\underbrace{\alpha^8}_{=\alpha^3}+\alpha+\alpha^2+1=0$