Finite fields

Note Title

Minimal polynomials:

$\beta \in \overline{\mathbb{F}}_p$

$\rightarrow M_\beta(x) \in \mathbb{Z}_p[x]$ s.t. $M_\beta(\beta) = 0$ + degree is minimal

Property: $M_\beta(x)$ is irreducible

Pf: Contradiction. Assume $M_\beta(x) = a(x)\,b(x)$ where $\deg a(x), \deg b(x) < \deg M_\beta(x)$

But $M_\beta(\beta) = 0 = a(\beta)\, b(\beta)$

$\Rightarrow$ $a(\beta) = 0$ (or) $b(\beta) = 0$, which is a contradiction. QED

$\rightarrow$ $f(x) \in \mathbb{Z}_p[x]$ s.t. $f(\beta) = 0$

Then, $M_\beta(x) \mid f(x)$

Corollary: Take $f(x) = x^{p^m} - x$. We know $f(\beta) = 0$.

$\Rightarrow$ $M_\beta(x) \mid (x^{p^m} - x)$

Examples: 1) $F_2 = \{0, 1\}$ $M_0(x)$ $M_1(x)$

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

2) $F_3 = \{0, 1, 2\}$ $M_0(x)$ $M_1(x)$ $M_2(x)$

$$x^3 - x = x(x-1)(x-2)$$

3) $F_5 = \{0, 1, 2, 3, 4\}$

$$x^5 - x = x(x^4 - 1) = x(x^2-1)(x^2+1)$$

$$= x(x-4)(x-1)(x-2)(x-3)$$

4) $F_4 = \{0, 1, \alpha, 1+\alpha\}$ $\alpha^2 = 1+\alpha$, $\alpha^3 = 1$

$\alpha^2 =$

$(2 = 0)$ $m_0(x)$ $m_1(x)$ $m_\alpha(x) = m_{\alpha^2}(x)$

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

$= x(x+1)(x+\alpha)(x+\alpha^2)$

5) $F_8 = \{0, 1, \alpha, \alpha^2, \dots, \alpha^6\}$ $\alpha^7 = 1$,

$\pi(\alpha) = \alpha^3 + \alpha + 1$ $\alpha^3 = \alpha + 1$

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

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

$\alpha^5 = \alpha^2 + \alpha + 1$

$\alpha^6 = \alpha^2 + 1$

$M_0(x) = x$

$m_1(x) = x+1$

$$(x+\alpha)(x+\alpha^2)(x+\alpha^4) = (x^2+\alpha^4 x+\alpha^3)(x+\alpha^4)$$

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

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

$\alpha^5 = \alpha^2+\alpha+1$

$\alpha^6 = \alpha^2+1$

$= x^3 + x + 1 =$

$M_{\alpha}(x) = M_{\alpha^2}(x) = M_{\alpha^4}(x)$

$$(x+\alpha^3)(x+\alpha^6)(x+\alpha^5) = x^3 + x^2 + 1 =$$

$$M_{\alpha^3}(x) = M_{\alpha^6}(x) = M_{\alpha^5}(x)$$

$$x^8 + x = x(x+1)(x+\alpha)\dots(x+\alpha^6)$$

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

$\left(\sum_{i} x^{i}\right)$

5) $F_{16} = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{14}\}$ $\alpha^{15} = 1$

$\alpha^4 = \alpha + 1$

$x^{16} + x = x(x+1)(x^2+x+1)$

(x^4)

$(x^2 + x)$

$(x^4 + x + 1)$

$(x^4 + x^3 + 1)$

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

A few "abstract" results

→ F: finite extension of Z_p that contains all roots of $x^{p^m} - x$.

Then, the roots of $x^{p^m} - x$ form F_{p^m} & $F_{p^m} \subseteq F$.

Pf: Roots of $x^{p^m} - x$ in $F = \{0, 1, \alpha_3, \alpha_4, \ldots, \alpha_{p^m}\}$

→ $(\alpha_i + \alpha_j)^{p^m} - (\alpha_i + \alpha_j) = 0$

→ closure for mult, inverse etc.

Property of minimal poly

Suppose $\beta \in F_{p^m}$ is primitive.

Then, $\deg M_\beta(x) = m$

Pf: Suppose $\deg \underbrace{M_\beta(x)}_{\text{irreducible over } Z_p} = d \leq m$

Construct a field F with $\pi(x) = M_\beta(x)$.

$|F| = p^d$, $F \subseteq F_{p^m}$ & it contains 'β'

$\beta^{p^d-1} = 1$. Since β: primitive,

$d \geq m$.

$\beta \in F_{p^m}$

$\pi(x) = M_\beta(x) = \pi_0 + \pi_1 x + \cdots + \pi_d x^d$

$F = \{ a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} : a_i \in \mathbb{Z}_p, \ \pi(\alpha) = 0 \}$

isomorphism

$\alpha \in F \iff \beta \in F_{p^m}$

$\alpha^L \in F \iff \beta^L \in F_{p^m}$

$|F| \geq p^m$ $\qquad$ $|\cdot| \geq p^m$

$a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \longleftrightarrow a_0 + a_1\beta + \cdots + a_{d-1}\beta^{d-1} \in F_{p^m}$