Minimal polynomials

Note Title

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

$$M_\beta(x) = \prod_{\gamma \in C_\beta} (x - \gamma) \in \mathbb{Z}_p[x]$$

$$C_\beta = \{\beta, \beta^p, \beta^{p^2}, \ldots, \beta^{p^{d-1}}\} \qquad \beta^{p^d} = \beta$$

$$\beta^{p^d - 1} = 1$$

$$F_{p^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}$$

α: prim element

$$\beta = \alpha^i \in F_{p^m}$$

Conjugates of β: $C_\beta = \{\alpha^i, \alpha^{ip}, \alpha^{ip^2}, \ldots, \alpha^{ip^{d-1}}\}$

$$\alpha^{ip^d} = \alpha^i$$

$$p^m - 1 \mid i(p^d - 1) \iff \alpha^{i(p^d-1)} = 1 \iff d \mid m$$

Ex: $F_8 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$ $\alpha^7 = 1$

$\alpha^3 = 1 + \alpha$

$C_0 = \{0\}$ $C_1 = \{1\}$ $x+1$

$C_\alpha = \{\alpha, \alpha^2, \alpha^4\}$ $C_{\alpha^2} = C_{\alpha^4} = C_\alpha$

x^3+x+1

$C_{\alpha^3} = \{\alpha^3, \alpha^6, \alpha^5\}$ $C_{\alpha^6} = C_{\alpha^5} = C_{\alpha^3}$

$x^3 + x^2 + 1$

$C_0 = C_{\alpha^0} = \{0\}$ $C_{\alpha^1} = C_1 = \{1, 2, 4\}$

$C_3 \to C_{\alpha^3} = \{3, 5, 6\}$

Ex: $F_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ $\alpha^{15} = 1$

$\alpha^4 = 1 + \alpha$

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

$C_0 = \{0\}$ $x + 1$

$x^4 + x + 1$

$C_1 = \{1, 2, 4, 8\}$ $C_3 = \{3, 6, 12, 9\}$

Conj α^0 α^1 α^2 α^4 α^8

α

x by 2, mod 15

$C_5 = \{5, 10\}$ $x^2 + x + 1$

$C_7 = \{7, 11, 13, 14\}$

$x^4 + x^3 + 1$

Cyclotomic cosets: under mult by p (prime) mod $p^m - 1$

$$i \in \{0, 1, 2, \ldots, p^m - 2\}$$

$$C_i = \{i, ip, ip^2, \ldots, ip^{d-1}\}$$

d: smallest s.t. $ip^d = i \mod (p^m - 1)$

Fact: Cyclotomic cosets partition the set

$$S = \{0, 1, 2, \ldots, p^m - 2\}$$

$\rightarrow \bigcup_i C_i = S$; Either $C_i = C_j$ (or) $C_i \cap C_j = \emptyset$

Facts: $\alpha \in F_{p^m}$, primitive

For what i, is α^i also primitive?

$$\text{ord}(\alpha^i) = \frac{p^m - 1}{\gcd(i, p^m - 1)}$$

$p^m - 1 \to \text{ord}(\alpha)$

$\gcd(i, p^m - 1) \to \text{ord}(\alpha)$

α^i: primitive iff $\gcd(i, p^m - 1) = 1$

$\Updownarrow$

Conjugates of α^i are primitive

α^i : primite $\Rightarrow |C_i| = m$

α^i : primite $\Leftrightarrow$ α^{-i} : primitive

Ex: F_{128} , F_{256} ?

$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8, 16, 32, 64\}$

$C_3 = \{3, 6, 12, 24, 48, 96, 65\}$

$\deg\left(M_{\alpha^i}^{(x)}\right) = 7$, if $i \neq 0 \bmod 127$