

Minimal polynomials

Note Title

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

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

$$C_{\beta} = \left[\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{d-1}} \right]$$

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

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

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

α : prim element

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

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

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

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

Ex: $F_8 = \{0, 1, \alpha, \alpha^2, \dots, \alpha^6\}$ $\alpha^7 = 1$
 $\alpha^3 = 1 + \alpha$

$x C_0 = \{0\}$ $(C_1) = \{d^i\}_{x+1}$

$x^3 + x + 1$ $C_\alpha = \{\alpha, \alpha^2, \alpha^4\}$ $C_{\alpha^2} = C_{\alpha^4} = C_\alpha$

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

$x^3 + x^2 + 1$ $C_0 = C_{\alpha^0} = \{0\}$ $(C_1) \leftarrow C_{\alpha^1} = \{1, 2, 4\}$

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

\mathbb{Z}_x : $F_{16} = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{14}\}$ $\alpha^{15} = 1$

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

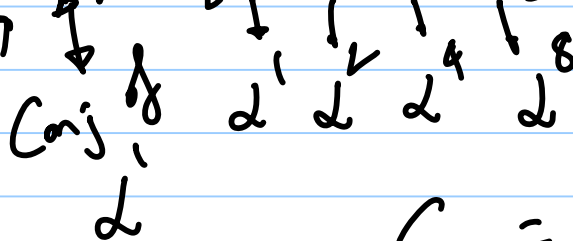
$\alpha^4 = 1 + \alpha$

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

$C_1 = \{1, 2, 4, 8\}$ $x^4 + x + 1$

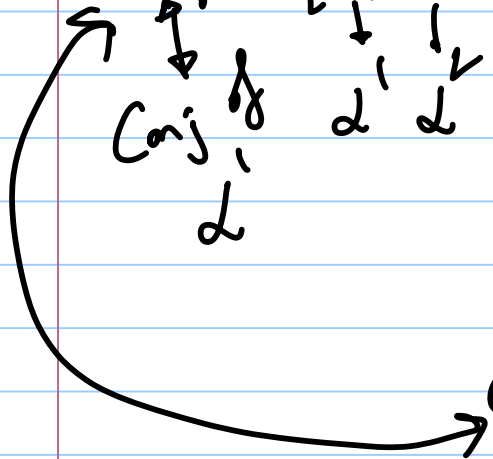
$C_3 = \{3, 6, 12, 9\}$

x by 2, mod 15



$C_5 = \{5, 10\}$ $x^4 + x + 1$

$C_7 = \{7, 11, 13, 14\}$
 $x^4 + x^3 + 1$



Cyclotomic cosets: under mult by p (prime)

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

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

d : smallest s.t. $ip^d \equiv i \pmod{p^m - 1}$

Fact: Cyclotomic cosets partition the set

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

$$\rightarrow \bigcup_i C_i = S \quad ; \quad \text{either } C_i = C_j \text{ (or) } C_i \cap C_j = \emptyset$$

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

For what i , is α^i also primitive?

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

$\rightarrow \text{ord}(\alpha)$
 \downarrow
 $\text{ord}(\alpha)$

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

Conjugates of α^i are primitive

$$\alpha^i : \text{primitive} \Rightarrow |C_i| = m$$

$$\alpha^i : \text{primitive} \Leftrightarrow \alpha^{-i} : \text{primitive}$$

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

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

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

$$\boxed{\deg(M_{\alpha^i}(x)) = 7, \text{ if } i \neq 0 \pmod{127}}$$