Tutorial on Finite fields

Note Title

- Construction of $GF(p^m)$: polys of deg $\leq m-1$ in $Z_p[\alpha]$

$\pi(\alpha)$: deg-m irred poly from $Z_p[\alpha]$

α: primitive

mult mod $\pi(\alpha)$

α^i	vector
1	$[a_0\ a_1 \cdots a_{m-1}]$
α	
α^2	
$\vdots$	
α^i	
$\vdots$	
α^{p^m-2}	

$a_i \in Z_p$

$\pi(x)$: irred, deg-m over $\mathbb{Z}_p[x]$

is primitive if smallest 'i' for which

$$\pi(x) \mid x^i - 1 \quad \text{is} \quad i = p^m - 1$$

Ex: - $\pi(x) = x^4 + x + 1$, irred & primitive

- $\pi(x) = x^4 + x^3 + x^2 + x + 1$, irred, but not primitive

↓ divides $x^5 + 1$

- $\pi(x) = x^2 + 1 \in \mathbb{Z}_3[x]$, irred, but not primitive

$x^2 + x + 2 \in \mathbb{Z}_3[x]$, primitive

(4) - $GF(9) = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^7\}$

$ord(\alpha) = 8$

$$ord(\alpha^i) = \frac{ord(\alpha)}{gcd(i, ord(\alpha))}$$

$ord(\alpha^2) = 4$
$ord(\alpha^3) = 8$
$ord(\alpha^4) = 2$
$ord(\alpha^5) = 8$
$ord(\alpha^6) = 4$
$ord(\alpha^7) = 8$

- $GF(16)$

- $GF(32)$: $ord(\alpha) = 31$

order of every $\alpha^i = 31$, $i = 1, 2, \ldots, 30$

(7) $\alpha \in GF(16)$, primitive, $\alpha^4 = \alpha + 1$

$x + y = \alpha^{14}$

$x^3 + y^3 = \alpha$

$\therefore y = \alpha^{14} + x$

· Find x and y.

$$x^3 + (\alpha^{14} + x)^3 = \alpha$$

$$x^3 + \alpha^{12} + \alpha^{13}x + \alpha^{14}x^2 + x^3 = \alpha$$

$$\alpha^{14}x^2 + \alpha^{13}x + (\alpha + \alpha^{12}) = 0$$

– by trial & error find roots.

(8) (a) $x + y = \alpha^3$

$x^2 + y^2 = \alpha^6$ → × same as

→ 16 pairs of solutions

(b) $x + y = \alpha^3$

$x^2 + y^2 = \alpha$ ↕ inconsistency

⇓

No solutions in GF(16)

(18) Factor

$x^n + 1$ over $GF(2)$

↓

Factor into linear factors in some $GF(2^m)$

↓

α : primitive : root of $x^{2^m-1} + 1$

$\alpha^{2^m-1} = 1$

powers of α are distinct roots

Suppose $\beta \in GF(2^m)$

has order $= n$

$x^n + 1 = (x+\beta)(x+\beta^2)$

$\cdots (x+\beta^{n-1})(x+\beta^n)$

↓

$x+1$

Find m s.t. $n \mid 2^m - 1$ $\quad \alpha$: prim $\in GF(2^m)$

Claim: $\text{ord}\left(\alpha^{\frac{2^m-1}{n}}\right) = n$

Factor $x^n + 1$ into linear factors in $GF(2^m)$.

Combine linear factors of conjugates to get factors over $GF(2)$.

(a) $x^5+1 = (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^9)(x+1)$

$m=4$: $5 \mid 2^4-1=15$

$\alpha \in GF(16)$, prim

$ord(\alpha^3) = 5$

Combine $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$ to get

$x^5+1 = (x+1)(x^4+x^3+x^2+x+1)$

$x^9+1 = (x+\alpha^7)(x+\alpha^{14})(x+\alpha^{21})(x+\alpha^{28})(x+\alpha^{35})(x+\alpha^{42})(x+\alpha^{49})(x+\alpha^{56})(x+1)$

$m=6 \qquad 9 \mid 2^6-1 = 63$

$\alpha \in GF(64)$, prim.

$ord(\alpha^7) = 9$

Conjugates: $\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}\}$

$\{\alpha^{21}, \alpha^{42}\} \to x^2+x+1$

$x^9+1 = (x+1)(x^2+x+1) M_{\alpha^7}(x)$

$M_{\alpha^7}(x) = 1+x^3+x^6$