Primitive Polynomials

6/19/17

1. Review $\mathbb{F}_{p^k}$ and define primitive
2. REU problem 6(a)
3. Motivation from cyclic codes & REU problem 6(b)

1. Recall $\mathbb{F}_{p^k}$ = splitting field over $\mathbb{F}_p$ of $x^{p^k} - x$
$= \{\text{roots of } x^{p^k} - x\}$
$\cong \mathbb{F}_p[x]/(f(x))$, $f(x) \in \mathbb{F}_p[x]$ any which is irreducible & degree k

and recall

Theorem: $\mathbb{F}_{p^k}^{\times} := \mathbb{F}_{p^k} - \{0\} = \{1, \pi, \pi^2, \dots, \pi^{p^k-1}\} = \langle \pi \rangle$, $\pi^{p^k-1} = 1$

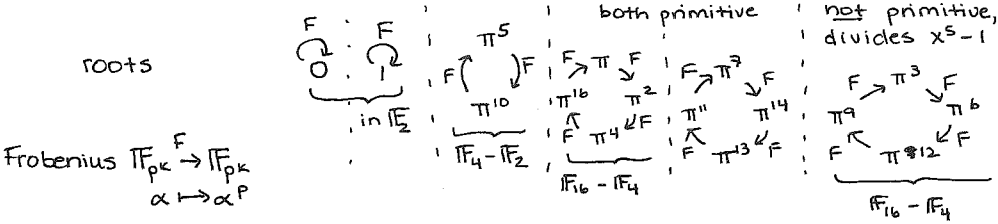
Definition: $f(x)$ irreducible in $\mathbb{F}_p[x]$ is primitive if $x \in \mathbb{F}_p[x]/f(x)$ has multiplicative order $p^k - 1$
(i.e., $\bar{x}$ can play the role of π, i.e., $\mathbb{F}_{p^k} = \langle \bar{x} \rangle$)

Equivalently, $f(x) \nmid x^d - 1$ $\forall$ proper factors d of $p^k - 1$

Ex $p = 2$, $k = 4$

$\{1, \pi, \dots, \pi^{14}\} = \mathbb{F}_{2^4} = \mathbb{F}_{16} = \{\text{roots of } x^{16} - x\} = \{\text{roots of } x(x^{15}-1)\}$ (irreducible quartics)

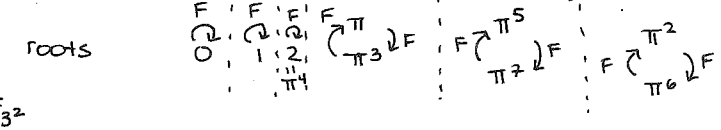
in $\mathbb{F}_2[x]$, $x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$



Ex $p = 3$, $k = 2$

$\mathbb{F}_{3^2} = \mathbb{F}_9 = \{\text{roots of } x^9 - x = x(x^8-1)\}$
$= x(x-1)(x+1)(x^2+x+2)(x^2+2x+2)(x^2+1)$
$\{0, \pi, \dots, \pi^7\}$, π^8 (the $(x-2)$ factor)

three irreducible quadratics in $\mathbb{F}_3[x]$



$\mathbb{F}_{3^2} \xrightarrow{F} \mathbb{F}_{3^2}$
$\alpha \mapsto \alpha^3$

2. **REU Problem 6(a)** Prove the following:

Conjecture: For $f(x) \in \mathbb{F}_p[x]$ irreducible with degree k, $f(x)$ is primitive $\iff$ $\frac{x^{p^k-1} - 1}{f(x)} =$
$= a_0 + a_1 x + a_2 x^2 + \cdots + a_{p^k-2} x^{p^k-2}$ with $a_i \in \{0, 1, \dots, p-1\}$
has # of descents in $(a_0, \dots, a_{p^k-2})$ is exactly $\frac{p-1}{2} p^{k-1}$
(indices i s.t. $a_i > a_{i+1}$)

Ex\\ $p=2, k=4$

$f(x)$	x^4+x+1	x^4+x^3+1	$x^4+x^3+x^2+x+1$
$\frac{x^{15}-1}{f(x)}$	$1+x^3+x^4+x^6+x^8+x^9+x^{10}+x^{11}$	$1+x+x^2+x^3+x^5+x^7+x^8+x^{11}$	$1+x+x^5+x^6+x^{10}+x^{11}$
	100110101111000 ↑ ↑ ↑ ↑ 4 descents	111101011001 00 ↑ ↑ ↑ ↑ 4 descents	110001100011000 ↑ ↑ ↑ 3 descents
			not primitive

$(a_0, \dots, a_{p^k-2})$ $\quad p^{k-1}\frac{p-1}{2} = 2^3\frac{1}{2} = 4$, primitive

Ex\\ $p=3, k=2$

$f(x)$	x^2+x+2	x^2+2x+2	x^2+1
$\frac{x^8-1}{f(x)}$	$1+x+2x^2+2x^4+2x^5+x^6$	$1+2x+2x^2+2x^4+x^5+x^6$	$2+x^2+2x^4+x^6$
$(a_0, \dots, a_{p^k-2})$	11202210 ↑ ↑↑ 3 descents	12202110 ↑ ↑ ↑ 3 descents	20102010 ↑ ↑ ↑ ↑ 4 descents
			not primitive

$3^{2-1}\cdot\frac{3-1}{2} = 3$, primitive

REU Exercise 13

(a) Show $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{k-1}x^{k-1} + x^k \in \mathbb{F}_p[x]$, which is irreducible, will be primitive $\iff$ the associated linear feedback shift register (LFSR) map

$$(\mathbb{F}_p)^k \xrightarrow{T} (\mathbb{F}_p)^k$$

$$\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{bmatrix} \longmapsto \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix} \quad \text{where } x_k = c_0x_{k-1} - c_1x_{k-2} - \cdots - c_{k-1}x_0$$

has multiplicative order p^k-1.

(b) In fact, show that in this case, starting with any $x \in \mathbb{F}_p^k - \{\underline{0}\}$, one has $\{\underline{x}, T\underline{x}, T\underline{x}^2, \dots, T^{p^k-2}\underline{x}\}$ exhausting $\mathbb{F}_p^k - \{\underline{0}\}$.

3. Motivation from cyclic codes

In error-correcting codes, people only transmit codewords from a subset $\mathcal{C} \subsetneq \mathbb{F}_p^n$ so they can detect and correct transmission errors.

Often, $\mathcal{C} \subset \mathbb{F}_p^n$ is a $\mathbb{F}_p$-linear subspace and its perp space $\mathcal{C}^\perp := \{x \in \mathbb{F}_p^n : \underbrace{x \cdot y}_{\text{usual dot product}} = 0 \ \forall y \in \mathcal{C}\}$ is called the dual code to $\mathcal{C}$.

Ex\ the repetition code $\mathcal{C} \subset \mathbb{F}_p^n$ is $\mathcal{C} = \mathbb{F}_p \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} = \{(0,\dots,0), (1,\dots,1), \dots, (p-1,\dots,p-1)\}$

its dual is $\mathcal{C}^\perp = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}^\perp = \{x \in \mathbb{F}_p^n : \sum_{i=1}^n x_i = 0\}$, the parity check code.

Call $\mathcal{C}$ a cyclic code if its codewords are stable under cyclic shift.

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} \mapsto \begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix}$$

$\in \mathcal{C} \to \in \mathcal{C}$

If we identify $\mathbb{F}_p^n \longleftrightarrow \mathbb{F}_p[x]/(x^n-1)$

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} \longmapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

then cyclic shift = multiplication by x, and $\left\{\begin{matrix}\text{cyclic codes} \\ \mathcal{C} \text{ of length} \\ n \text{ over } \mathbb{F}_p\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{Ideals } I \text{ in} \\ \mathbb{F}_p[x]/(x^n-1)\end{matrix}\right\}$

here, $I = (g(x))$ for some $g(x) \mid (x^n-1)$ ("generator polynomial for $\mathcal{C}$")

Furthermore, $\mathcal{C}^\perp$ is also cyclic, with generator polynomial $\frac{x^n-1}{g(x)} =: g^\perp(x)$

Ex\ repetition code $\mathcal{C} = \mathbb{F}_p \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \subset \mathbb{F}_p^n$ is cyclic with $g(x) = 1 + x + x^2 + \cdots + x^{n-2}$

Its dual $\mathcal{C}^\perp$ is cyclic, $g^\perp(x) = \frac{x^n-1}{g(x)} = x - 1$

$$\updownarrow$$

$$\begin{bmatrix} 1 \\ -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Ex\ Hamming code of length $p^{k-1} - 1 = n$ over $\mathbb{F}_p$ is cyclic with generator $g(x)$ any primitive polynomial of degree k in $\mathbb{F}_p[x]$.

Dual Hamming code is its dual, with generator $\frac{x^{p^k-1}-1}{g(x)}$.

Back in May 2017, J. Propp asked:

"Are there any cyclic codes $\mathcal{C} \subset \mathbb{F}_p^n$ for which the polynomial

$$X_{\mathcal{C}}^{\text{maj}}(q) := \sum_{\underline{a} \in \mathcal{C}} q^{\text{maj}(\underline{a})}, \quad \underline{a} = (a_0, a_1, \dots, a_{n-1}) \text{ and } \text{maj}(\underline{a}) := \sum_{i=0,1,\dots,n-1 \ a_i > a_{i+1}} i$$

has $X_{\mathcal{C}}^{maj}(q)\big|_{q=\zeta_n^d}$ counting codewords fixed by c^d where c = cyclic shift.

What about with $X_{\mathcal{C}}^{inv}(q) := \sum_{\underline{a}\in\mathcal{C}} q^{inv(\underline{a})}$?" (where $inv(\underline{a}) = \#\{0\le i\le j\le n-1 : a_j > a_{j+1}\}$)

[Context: MacMahon showed

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{\substack{\text{words } \underline{a} \text{ with} \\ k \text{ 0's and } n-k \text{ 1's}}} q^{maj(\underline{a})} = \sum_{\substack{\text{same} \\ \text{words}}} q^{inv(\underline{a})},$$

so this fits with problem 2!]

Jim checked cyclic codes $\mathcal{C} \subset \mathbb{F}_2^7$ and many had this property.

Conjecture: Dual Hamming codes have the above property for $X_{\mathcal{C}}^{maj}(q)$ when $p=2,3$.

implies ⇑ REU problem 6(a)

proposition: Dual Hamming codes over $\mathbb{F}_p$ have Jim's property for $X_{\mathcal{C}}^{maj}(q)$ if and only if $\frac{x^{p^k-1}-1}{f(x)}$ ($f(x)$ primitive) has coefficient sequence with #descents relatively prime to p^k-1.

REU Problem 6(b) Prove the following:

Conjecture: Dual Hamming codes also have Jim's property for $X_{\mathcal{C}}^{inv}(q)$ when $p=2$.