

**MATH 291T****Homework 5**

Due on Thursday 04/23/09

1. Let  $C_1$  and  $C_2$  be cyclic codes of length  $n$  over  $GF(q)$  with generator polynomials  $g_1(x)$  and  $g_2(x)$ . Prove that  $C_1 \subseteq C_2$  if and only if  $g_2(x)$  divides  $g_1(x)$ .

2. Prove that  $f^*(x)$  divides  $x^n - 1$  if  $f(x)$  divides  $x^n - 1$ .

3. Let  $n \in \mathbb{N}$  and  $f(x) \in GF(q)[x]$ . Then  $f(x)$  generates a cyclic code  $C$  of length  $n$  over  $GF(q)$ , namely

$$C = \{\mathbf{c} \in GF(q)^n : \mathbf{c}(x) \equiv f(x)q(x) \pmod{x^n - 1} \text{ for some } q(x) \in GF(x)\}$$

Example : Let  $n = 3$ ,  $q = 2$  and  $f(x) = 1 + x^2$ . Then

$$\begin{aligned} C \pmod{x^3 - 1} &= \{(1 + x^2)q(x) \pmod{x^3 - 1} : q(x) \in GF(2)[x]\} \\ &= \{(1 + x^2)(a + bx + cx^2) \pmod{x^3 - 1} : a, b, c \in GF(2)\} \\ &= \{(a + b) + (b + c)x + (c + a)x^2 \pmod{x^3 - 1} : a, b, c \in GF(2)\} \\ &= \{0, x + x^2, 1 + x^2, 1 + x\} \pmod{x^3 - 1} \end{aligned}$$

Hence  $C = \{000, 011, 101, 110\}$ . So  $C$  is indeed cyclic with generator polynomial  $1 + x$ .

Find the generator polynomial of the binary cyclic code of length 5 generated by  $1 + x + x^2 + x^3$ .

4. Let  $f(x) \in GF(q)[x]$  be a monic divisor of  $x^n - 1$  and  $C$  the cyclic code of length  $n$  over  $GF(q)$  generated by  $f(x)$  (see Ex#3). Prove that  $f(x)$  is the generator polynomial of  $C$ .