Math 641, Fall 1999
R.A. Brualdi
Exercise Set 5, * exercises due Friday, November 12, 1999

***** 1. Prove that in F_{2^m} every element a has a *square root*, that is, there is an element b such that $b^2 = a$.

***** 2. Let $f(x) \in F_q[x]$ be a monic polynomial of degree k. The *reciprocal polynomial* is the polynomial $f_{-1}(x) = x^k f(x^{-1})$. Prove that if $f(x)$ is an irreducible polynomial of degree > 2 satisfying $f(x) = f_{-1}(x)$, then $f(x)$ is not a primitive polynomial.

***** 3. Let $C_1 = \langle g_1(x) \rangle$ and $C_2 = \langle g_2(x) \rangle$ be cyclic codes in $R_n = F_q[x]/\langle x^n - 1 \rangle$ with gen. polys. $g_1(x)$ and $g_2(x)$, respectively. Prove:

(a) $C_1 \subseteq C_2$ if and only if $g_2(x) | g_1(x)$;

(b) $C_1 \cap C_2$ is a cyclic code with generator polynomial

$$\text{LCM}\{g_1(x), g_2(x)\};$$

(c) $C_1 + C_2 (=_{\text{def}} \{c_1(x) + c_2(x) : c_1(x) \in C_1, c_2(x) \in C_2\})$ is a cyclic code with generator polynomial

$$\text{GCD}\{g_1(x), g_2(x)\};$$

(d) C is self-orthogonal if and only if $h'(x) | g(x)$ where $h'(x)$ is the reciprocal of the check polynomial of C.

***** 4. Let $g(x)$ be the generator polynomial of a binary cyclic code containing at least one odd weight vector. Prove that the set of codewords of even weight form a cyclic code C and determine its generator polynomial.

***** 5. Let C be a binary cyclic code. Prove that C contains a codeword of odd weight if and only if the all 1's vector is in C.