Math 641, Fall 1999
R.A. Brualdi
Exercise Set 6, * exercises due Friday, December 3, 1999

*1. A cyclic code C of length n is *degenerate* provided there exists an integer r with $r \mid n$ such that each codeword $\mathbf{c}$ has the form $\mathbf{c} = \mathbf{c}'\mathbf{c}'\cdots\mathbf{c}'$ where $\mathbf{c}'$ is an r-tuple. Prove that a cyclic code is degenerate if and only if its check polynomial $h(x)$ satisfies $h(x) \mid x^r - 1$. HINT: Show that the generator polynomial takes the form $a(x)(1 + x^r + x^{2r} + \cdots + x^{n-r})$.

*2. Let C_1 and C_2 be cyclic codes of order n with idempotent generators $e_1(x)$ and $e_2(x)$, respectively. Prove that the idempotent generator of $C_1 \cap C_2$ is $e_1(x)e_2(x)$ and that the idempotent generator for $C_1 + C_2$ is $e_1(x) - e_2(x) - e_1(x)e_2(x)$.

*3. Identify all the binary cyclic codes of order 7 giving their generator polynomials and idempotent generators.

*4. Page 111 of van Lint's book, # 2: Determine the idempotent generator of the [15,11,3] binary Hamming code.

*5. Consider the narrow sense binary BCH code of length 17 with designed distance 3. Use the van Lint Wilson bound to show that the minimum distance is at least 5. HINT: Start with $I_0 = \emptyset$ and $I_1 = \{\gamma^3\}$.