Math 601 Homework #8. Due Wed., Mar. 28, 2018

Write up and hand in solutions to the following exercises. You must give complete justification for all answers. Assume all polynomials are in $\mathbf{F}[x]$.

1. Let $h(x) = 1 + x^7$. Compute $f(x) \pmod{h(x)}$ for each of the following functions.
   (a) $f(x) = 1 + x^3 + x^8$
   (b) $f(x) = x + x^5 + x^6 + x^{12}$
   (c) $f(x) = 1 + x^7 + x^8 + x^{15}$

2. Prove: For all polynomials $f(x)$, $g(x)$, and $h(x)$,
   $f(x)$ and $g(x)$ have the same remainder when divided by $h(x)$
   if and only if
   $h(x)$ divides $f(x) - g(x)$ (that is, there exists $q(x)$ such that $f(x) - g(x) = q(x)h(x)$).

3. Determine whether each of the following codes is cyclic. (The code need not be linear.)
   (a) $C = \{0000, 1100, 0011, 1111\}$
   (b) $C = \{0001, 1110, 1000, 0111, 0100, 1011, 0010, 1101\}$
   (c) $C = \{10100, 01010, 00101\}$

4. For each of the following, find all words $v \in \mathbf{F}^6$ such that
   (a) $\pi(v) = v$
   (b) $\pi^2(v) = v$
   (c) $\pi^3(v) = v$

5. Find a basis for the smallest binary linear cyclic code of length n containing v.
   (a) $n = 7$, $v = 1011100$
   (b) $n = 6$, $v = 010101$

6. For each of the following sets S, consider the smallest binary linear cyclic code C containing S. Find the generator polynomial $g(x)$ of C and write each element of S as a polynomial product $a(x)g(x)$.
   (a) $S = \{1001, 0101\}$
   (b) $S = \{010010\}$

7. Let $g(x) = 1 + x^2 + x^3$ be the generator polynomial for a binary linear cyclic code of length 7.

   (a) Encode the message polynomials $m_1(x) = 1 + x^3$ and $m_2(x) = x^2 + x^5$.

   (b) Retrieve the message polynomials from the codewords $c_1(x) = x^2 + x^4 + x^5$ and $c_2(x) = 1 + x + x^2 + x^4$.

8. Find a generator matrix for the binary linear cyclic code of length n with generator polynomial $g(x)$.

   (a) $n = 7$, $g(x) = 1 + x^2 + x^3$

   (b) $n = 9$, $g(x) = 1 + x^3 + x^6$

9. True or False? (Give proof if true; give counterexample if false.) If C_1 and C_2 are cyclic codes in $\mathbf{F}^n$ and $C_1 \cap C_2 \neq \emptyset$, then $C_1 \cap C_2$ is a cyclic code.

10. True or False? (Give proof if true; give counterexample if false.) If C_1 is a cyclic code in $\mathbf{F}^n$ and C_2 is a code in $\mathbf{F}^n$ equivalent to C_1, then C_2 is cyclic.

Extra credit:

1. Prove: Suppose C is a binary linear cyclic code of length n, and n is odd. Then C contains a codeword of odd weight if and only if the length n all ones vector $111\cdots1$ is in C.

2. Let C be a binary linear cyclic code, and let D be the set of even weight codewords in C.

   (a) Prove: D is a linear cyclic code.

   (b) Let $g(x)$ be the generator polynomial for C. Give the generator polynomial for D, in terms of $g(x)$. (And, of course, prove your answer.)