Indian Institute of Technology Bombay
Department of Electrical Engineering

Handout 12 EE 706 Communication Networks
Solutions to Quiz 5 February 11, 2010

Please READ THE QUESTIONS CAREFULLY before answering.

1. A polynomial of degree k is said to be primitive if the smallest value of m for which it divides $X^m + 1$ is $2^k - 1$.

   (a) Show that $X^3 + X + 1$ is a primitive polynomial. [3 points]

   Ans.

   $X^3 + X + 1$ is a polynomial of degree 3. For it to be a primitive polynomial, the smallest value of m for which it divides $X^m + 1$ is $2^3 - 1 = 7$. So it should divide $X^7 + 1$ but not $X^6 + 1$, $X^5 + 1$, $X^4 + 1$, $X^3 + 1$, $X^2 + 1$, $X + 1$ and 1. [You should do the divisions to check this is the case].

   (b) Show that $X^3 + 1$ is not a primitive polynomial. [3 points]

   Ans.

   $X^3 + 1$ is a polynomial of degree 3. For it to be a primitive polynomial, the smallest value of m for which it divides $X^m + 1$ is $2^3 - 1 = 7$. So it should divide $X^7 + 1$ but not $X^6 + 1$, $X^5 + 1$, $X^4 + 1$, $X^3 + 1$, $X^2 + 1$, $X + 1$ and 1. But it divides itself. Hence it is not a primitive polynomial.

2. Does $X + 1$ divide $X^{2^n} + X^{2^n - 1} + X^{2^n - 2} + \cdots + X + 1$ where n is a non-negative integer? [4 points]

   Ans.

   If n is a non-negative integer, $n \geq 0$, i.e. $n \in \{0, 1, 2, 3, \ldots\}$. Let $g_n(X) = X^{2^n} + X^{2^n - 1} + X^{2^n - 2} + \cdots + X + 1$. Then for $n = 0$, $g_0(X) = X^{2^0} + 1 = X + 1$. Thus for $n = 0$, $X + 1$ divides $g_n(X)$.

   If $n > 0$, 2^n is an even number and $g_n(X)$ has $2^n + 1$ terms which is an odd number. Then $g_n(1) = 1$ because the sum of an odd number of 1's is 1. But if $X + 1$ divides $g_n(X)$, then

   $$g_n(X) = (X + 1)a(X)$$

   where $a(X)$ is the quotient polynomial obtained by dividing $g_n(X)$ by $X + 1$. Now if we substitute $X = 1$ on both sides we get $g_n(1) = 0$ which is a contradiction for $n > 0$.