CMSC 442/653
Spring 2009
Instructor: Dr. Lomonaco

Homework 2
*** Corrected Version ***

- **Listening Assignment:** Listen to Rosini's Il barbiere di Siviglia (The Barber of Seville)

- **Optional Reading assignment:** Peterson & Weldon, "Error-Correcting Codes," MIT Press, (Second Edition), Chapter 6.

1U) Let

$$p(x) = x^{12} + x^9 + x^8 + x^6 + x^4 + x + 1$$

and

$$q(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1$$

a) Compute by hand $GCD\left((p(x), q(x)\right)$ over the ring $GF(2)[x]$

b) Use **Gcd mod 2** in MAPLE to check your answer. (You can access MAPLE on any xwindowing workstation at UMBC by typing "xmaple" followed by a carriage return.)

2U) Create a Log/AntiLog table for $GF\left(2^5\right)$ using the primitive (hence, irreducible) polynomial $p(x) = x^5 + x^2 + 1$.

3U) Create a Log/AntiLog table for $GF\left(3^2\right)$ using the primitive (hence, irreducible) polynomial $p(x) = x^2 + x + 2$.

4G) The polynomial $p(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $GF(2)$. Let

$$\xi = x \bmod p(x)$$

Show that ξ is not a primitive element, and therefore $p(x)$ is not a primitive polynomial. Moreover, show that

$$\alpha = 1 + \xi$$

is primitive, i.e., show that the smallest positive integer k such that $\alpha^k = 1$ is $k = 2^4 - 1$.