MATH 601 Final Exam
December 17, 2002

Answer all the questions, justify your answers and show your work.

1. Find a parity check matrix for the code with generator matrix

\[
\begin{bmatrix}
1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0
\end{bmatrix}
\]

2. Construct an SDA for the code with parity check matrix

\[
\begin{bmatrix}
0 & 1 & 1 \\
1 & 1 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}
\]

(Assume CMLD - every syndrome should have a corresponding error pattern.)

3. Write out a generator matrix and a parity check matrix for the extension of the (15, 11, 3) Hamming code $H_4$.

4. Assume that $x^{10} + 1 = (1 + x)^2(1 + x + x^2 + x^3 + x^4)^2$ is a factorization into irreducible polynomials.
   a) For which values of $k$ does there exist a (10, $k$) linear cyclic code?
   b) Construct both the generating and parity check matrices for a (10, 4) linear cyclic code.

5. List the complete cyclic table for the Galois irrational associated with the mod 2 polynomial $x^4 + x + 1$.

6. Using the attached cyclic table, find the minimal polynomials of $\delta^8$, $1 + \delta^2$, and $\delta^{10}$.
7. Prove two of the following three propositions:
   A. The minimal generating polynomial of a linear cyclic \((n, k)\) code is a divisor of \(x^n + 1\).
   B. 
   \[
   \begin{vmatrix}
   1 & 1 & 1 & \ldots & 1 \\
   x_1 & x_2 & x_3 & \ldots & x_n \\
x_1^2 & x_2^2 & x_3^2 & \ldots & x_n^2 \\
   \vdots & \vdots & \vdots & \ddots & \vdots \\
x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1}
   \end{vmatrix}
   = \prod_{n \geq j > i \geq 1} (x_j - x_i)
   \]
   C. If \(\alpha \in GF(2^\nu)\) then \(\alpha^{2^\nu - 1} = 1\).

8. Break the RSA code with public key \(n = 119, e = 5\).

9. In decoding the received vector \(w = 11 \ 00 \ 00 \ 00 \ 10 \ 00 \ \ldots\) the following partial information was obtained. Compute the array that corresponds to \(t = 5\).