Math 335 HW 5 - Due March 5, 2004

1. Verify by hand that the CORRECTED algorithm from class for the S-box of AES matches figure 3.8 on page 106 of the text for

   (a) 10000001 → 00001100

   (b) 00000010 → 01110111

   CORRECTED ALGORITHM:

   $b_7b_6b_5b_4b_3b_2b_1b_0 \rightarrow b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0 = b(x)$ viewed as a polynomial in $\mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$. Then $b(x) \rightarrow (b(x))^{(-1)}$ in $\mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$. Call this polynomial $c(x)$. Now view $c(x)$ in $\mathbb{Z}_2[x]/(x^8+1)$ and map it to $d(x) = [(x^4+x^3+x^2+x+1)\cdot c(x)]+(x^6+x^5+x+1)$ in $\mathbb{Z}_2[x]/(x^8+1)$. Finally, $d(x) = d_7x^7+d_6x^6+d_5x^5+d_4x^4+d_3x^3+d_2x^2+d_1x+d_0 \rightarrow d_7d_6d_5d_4d_3d_2d_1d_0$.

2. Let F be the finite field $\mathbb{Z}_5[x]/(x^2+x+1)$.

   (a) Calculate $((x+3)y+4)\cdot((x+2)y+2)$ in $F[y]$.

   (b) Does y have a multiplicative inverse in $F[y]/((x+1)y^2+xy+3)$? If not, why not? If so, find it.