Homework 12, due September 30

(1) Let $GF(16) = \mathbb{Z}_2[x]/(x^4 + x + 1)$. Find a generator for the multiplicative group of $GF(16)$. Write each element of $GF(16)$ as a binary number, as a polynomial, and (except for 0) as a power of a generator.

(2) If $y = abcd$ in binary in $GF(16)$ so that $y = ax^3 + bx^2 + cx + d$, find a formula for y^2 in binary. Find a formula for y^{14} in binary. If $z = efgh$, find a formula for yz. (You will probably want to use a computer algebra system. Note that in this field a coefficient such as a is either 0 or 1, and $a^2 = a$ and $2a = 0$.)

(3) In $GF(256) = \mathbb{Z}_2[x]/(x^8 + x^4 + x^3 + x + 1)$, calculate the following.

(a) $11110000 + 01011100$

(b) $00001000 \cdot 00010111$

(c) $00111010 \cdot 00010111$

(d) 00000100^3

(e) 00000010^9

(f) 00000011^{-1}