Homework 12, due October 3

This homework is due at 5pm on Tuesday, October 3, instead of the usual 5pm on Monday, October 2. This is so you can watch general conference and not have to worry too much about homework.

(1) Let $GF(16) = \mathbb{Z}_2[x]/(x^4 + x + 1)$. The multiplicative group $GF(16)^\times$ of $GF(16)$ is the set of nonzero elements of $GF(16)$. The following turns out to be true: there is some $\alpha \in GF(16)$ such that, for any $\beta \in GF(16)^\times$, we have $\beta = \alpha^k$, for some integer k. We call such an α a *generator* of $GF(16)$.

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) 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}

(3) 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 $2a = 0$.)