Homework Questions regarding Galois Field Calculations

Consider the Galois field $GF(2^3)$ using the construction $\mathbb{Z}_2[x]/\langle 1+x+x^3\rangle$. Let $\beta = [x]$, under which one can produce the following table. (As discussed in class, this can function as a "log table" for our purposes in that representing non-zero elements as a power of the element β (which is a primitive element) makes multiplication much easier. Addition however it more efficient using the representation in terms of polynomials or words. The practice problems below should help gain a proficiency with this.

(Please note, part of the beauty and utility of Galois fields is that they possess BOTH a nice vector space structure (i.e. addition and scalr multiplication) and a nice multiplicative structure.)

word	entry in $\mathbb{Z}_2[x]/\langle 1+x+x^3\rangle$
000	$[0]=0$
100	$[1]=1$
010	$[x]=\beta$
001	$[x^2]=\beta^2$
110	$[1+x]=\beta^3$
011	$[x+x^2]=\beta^4$
111	$[1+x+x^2]=\beta^5$
101	$[1+x^2]=\beta^6$

GF1. Calculate the following (working within $F = \mathbb{Z}_2[x]/\langle 1+x+x^3\rangle$), using the table above as appropriate to facilitate your calculations. (Represent your answers both as the equivalence class of a polynomial (e.g. $[1+x]$) and in corresponding word form (e.g. (110)).)

(a) $[1+x^2]+[x+x^2]$
(b) $[1+x^2]-[x+x^2]$
(c) $(111)+(110)$
(d) $[1+x^2][x+x^2]$
(e) $(111)(110)$
(f) β^4
(g) $[1+x^2]^3$
(h) $[1+x]^4+[x]$
(i) $((110)+(011))^{-1}$
(j) $f([x+x^2])$ where $f(y)=1+y+y^3$
(k) The roots of $g(y)=1+y^2+y^3$ in F (i.e. find all α in F such that $g(\alpha)=0$.)
(l) Let α_1, α_2, α_3 be the answers to part (k). Show that $(y-\alpha_1)(y-\alpha_2)(y-\alpha_3)=g(y)$, by explicitly multiplying this factorization out.

Table 5.1 provides a similar table for the Galois field $GF(2^4)$ represented as $\mathbb{Z}_2[x]/\langle 1+x+x^4\rangle$. (Note: One feature of using $[p(x)]$ to represent the equivalence class of $p(x)$ modulo $1+x+x^4$, is that it facilitates the expression of modular equivalence. For instance, when using $\mathbb{Z}_2[x]/\langle 1+x+x^4\rangle$, saying $[x^4]=[1+x]$ is equivalent to the statement $x^4 \equiv (1+x) (\text{mod } 1+x+x^4)$. The modular equivalence notation (mod $f(x)$) is rather helpful when we need to speak of "modding" with respect

to several different polynomials $f(x)$. But in $\mathbb{Z}_2[x]/\langle h(x)\rangle$ (were there a single polynomial $h(x)$ that we are regularly doing modular equivlence with respect to) then $[p(x)]$ offers a more concise notation. However, $[p(x)]$ requires interpretation within the context of a specific $\mathbb{Z}_2[x]/\langle h(x)\rangle$.

GF2. Calculate the following, (working within $F = \mathbb{Z}_2[x]/\langle 1 + x + x^4\rangle$) using Table 5.1 as appropriate to facilitate. (Let $\beta = [x]$.) (Represent your answers both as the equivalence class of a polynomial and in corresponding word form.)

(a) $[1 + x^3][1 + x^2]$
(b) $[1 + x]^3$
(c) $[1 + x]^{-1}$
(d) $(1010)^2 + 1$
(e) $0[1 + x^2 + x^3]$ (Yes, that's a zero, it's not a typo.)
(f) $\beta^4 + \beta$
(g) $[1 + x + x^3]^3$
(h) Find the roots of $g(y) = y^3 + 1$ in F. (So one can say that you are finding the cube roots of 1 in F.)
(i) Let α_1, α_2, α_3 be the answers to part (h). Show that $(y - \alpha_1)(y - \alpha_2)(y - \alpha_3) = g(y)$, by explicitly multiplying this factorization out.