Math 476
Finite Field Conversion Table

Let $\mathbb{F} = \frac{\mathbb{Z}_2[x]}{\langle x^4+x+1 \rangle} = \left\{ ax^3 + bx^2 + cx + d : a, b, c, d \in \mathbb{Z}_2 \right\} = \left\{ x^k : 0 \leq k \leq 14 \right\}$.

The following table helps us perform computations in $\mathbb{F}$ by showing us how to convert from multiplicative form to additive for and vice versa.

Note that all of these form conversions are derived by applying the identity $x^4 + x + 1 = 0 \Rightarrow x^4 = x + 1$. For example, $x^8 = x^4 \cdot x^4 = (x + 1)(x + 1) = x^2 + 2x + 1 = x^2 + 1$.

The order of the elements is chosen in an effort to make it easier to find the element(s) we are looking for by putting the multiplicative elements first, in increasing order of exponent, followed by the corresponding additive element and then listing the additive elements grouped by maximum exponent, followed by the corresponding multiplcative element.

Multiplicative Form	Additive Form	Additive Form	Multiplicative Form
1	1	1	1
x	x	x	x
x^2	x^2	$x + 1$	x^4
x^3	x^3	x^2	x^2
x^4	$x + 1$	$x^2 + 1$	x^8
x^5	$x^2 + x$	$x^2 + x$	x^5
x^6	$x^3 + x^2$	$x^2 + x + 1$	x^{10}
x^7	$x^3 + x + 1$	x^3	x^3
x^8	$x^2 + 1$	$x^3 + 1$	x^{14}
x^9	$x^3 + x$	$x^3 + x$	x^9
x^{10}	$x^2 + x + 1$	$x^3 + x^2$	x^6
x^{11}	$x^3 + x^2 + x$	$x^3 + x + 1$	x^7
x^{12}	$x^3 + x^2 + x + 1$	$x^3 + x^2 + 1$	x^{13}
x^{13}	$x^3 + x^2 + 1$	$x^3 + x^2 + x$	x^{11}
x^{14}	$x^3 + 1$	$x^3 + x^2 + x + 1$	x^{12}