Task 5: Show that the set of integers, Z_2^n using modular arithmetic, is not a field.

For modular aritmetic there has to be a finite number of items in the set.

In this case; $Z \rightarrow$ set of integers

$n \rightarrow$ set of real numbers.

Cannot result to finite modular arithmetic and hence Z_2^n is not a field.

Task 6: Perform polynomial arithmetic in $GF(2^3)$ modulo $(x^3 + x^2 + 1)$

Taking α as a primitive element

$\alpha^3 + \alpha^2 + 1 = 0 \rightarrow (-1) \text{ --- (a)}$

$\alpha^3 = -(\alpha^2 + 1) \text{ ------- (b)}$

$\alpha^4 = \alpha^3 \cdot \alpha = -(\alpha^2 + 1)\alpha = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$

$\alpha^5 = \alpha^4 \cdot \alpha = -(\alpha^2 + \alpha + 1)\alpha = \alpha^3 + \alpha^2 + \alpha$

$= \alpha^2 + 1 + \alpha^2 + \alpha$

$= \alpha + 1$

$\alpha^6 = \alpha^5 \cdot \alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha$

$\alpha^7 = \alpha^6 \cdot \alpha = (\alpha^2 + \alpha)\alpha = \alpha^3 + \alpha^2 = \alpha^2 + 1 + \alpha^2$

$= 1$

Power representation	Polynomial representation	3-tuple representation $1\ \alpha\ \alpha^2$
0	0	000
1	1	100
α	α	010
α^2	α^2	001
α^3	α^2+1	101
α^4	$\alpha^2+\alpha+1$	111
α^5	$\alpha+1$	110
α^6	$\alpha^2+\alpha$	011
α^7	1	100