Chapter 4

10/10

21. $f(g) = g^4 + g^3 + 1 = 0$ $\quad g^4 = g^3+1$

$0 = 0$	$= 0$	$= 0$	$\rightarrow 0 = 0000$
$g^0 = g^0$	$= g^0$	$= g^0$	$\rightarrow g^0 = 0001$
$g^1 = g^1$	$= g^1$	$= g^1$	$\rightarrow g^1 = 0010$
$g^2 = g^2$	$= g^2$	$= g^2$	$\rightarrow g^2 = 0100$
$g^3 = g^3$	$= g^3$	$= g^3$	$\rightarrow g^3 = 1000$
$g^4 = g^4$	$= g^4$	$= g^3+1$	$\rightarrow g^4 = 1001$
$g^5 = g(g^4)$	$= g(g^3+1)$	$= g^3+g+1$	$\rightarrow g^5 = 1011$
$g^6 = g(g^5)$	$= g(g^3+g+1)$	$= g^3+g^2+g+1$	$\rightarrow g^6 = 1111$
$g^7 = g(g^6)$	$= g(g^3+g^2+g+1)$	$= g^2+g+1$	$\rightarrow g^7 = 0111$
$g^8 = g(g^7)$	$= g(g^2+g+1)$	$= g^3+g^2+g$	$\rightarrow g^8 = 1110$
$g^9 = g(g^8)$	$= g(g^3+g^2+g)$	$= g^2+1$	$\rightarrow g^9 = 0101$
$g^{10} = g(g^9)$	$= g(g^2+1)$	$= g^3+g$	$\rightarrow g^{10} = 1010$
$g^{11} = g(g^{10})$	$= g(g^3+g)$	$= g^3+g^2+1$	$\rightarrow g^{11} = 1101$
$g^{12} = g(g^{11})$	$= g(g^3+g^2+1)$	$= g+1$	$\rightarrow g^{12} = 0011$
$g^{13} = g(g^{12})$	$= g(g+1)$	$= g^2+g$	$\rightarrow g^{13} = 0110$
$g^{14} = g(g^{13})$	$= g(g^2+g)$	$= g^3+g^2$	$\rightarrow g^{14} = 1100$

22.

a. $g^3 + g^{12} + g^7 = g^3 + (g+1) + (g^2+g+1) = g^3+g^2 \rightarrow (1100)$

b. $g^3 - g^6 = g^3 + g^6 = g^3 + (g^3+g^2+g+1) = g^2+g+1 \rightarrow (0111)$

28.

degree(a) > 0
degree(b) > 0
$f(x) = a(x) \times b(x)$ X

Reducible polynomial can be expressed as the product of two polynomials, each with a degree greater than 0. In the case of 1-degree polynomial, it cannot be expressed as the produce of two polynomials with greater than 0. (as doing so would result in at least 2-degree polynomial) Therefore, the only two polynomials of degree 1, (x) and $(x+1)$, are irreducible polynomials.

29.

$f(x) = a(x) \times b(x)$ degree(a) = 1, degree(b) = 1

Reducible polynomial can be expressed as the product of two polynomials, each with a degree greater than 0, In the case of 2-degree polynomial, It can be factored into the product of two 1-degree polynomials, 1-degree polynomial must be either (x) or $(x+1)$. Therefore, when (x^2+x+1) is divided into two 1-degree polynomials, if it divides evenly, it's reducible, otherwise, it's irreducible. For it to divide by x, $f(0)$ must be 0, and for it to divide $(x+1)$, $f(-1)$ must be 0. However, with $f(0)=1$ and $f(-1)=1$, (x^2+x+1) is irreducible polynomial.

30.

Reducible polynomial can be expressed as the product of two polynomials, each with a degree greater than 0. In the case of 3-degree polynomial, it can be expressed as the product of a 1-degree polynomial and 2-degree polynomial. Therefore, if a 3-degree polynomial can be divided evenly either the 1-degree polynomials (x) or $(x+1)$, it's reducible, otherwise it's irreducible. For it to divide by x, $f(0)$ must be 0, and for it to divide $(x+1)$, $f(1)$ must be 0. However with $f(0)=1$ and $f(1)=1$ in (x^3+x^2+1), (x^3+x^2+1) is irreducible polynomial.

31.

a. $(11)\times(10) \Rightarrow (x+1)\times(x) \rightarrow (x^2+x) \rightarrow 110$

b. $(1010)\times(1000) \Rightarrow (x^3+x)\times(x^3) \rightarrow x^6+x^4 \rightarrow 1010000$

c. $(11100)\times(10000) \Rightarrow (x^4+x^3+x^2)\times(x^4) \rightarrow x^8+x^7+x^6 \rightarrow 111000000$

32.

The degree of $GF(2^2)$ is 2. A 2-degree polynomial has one irreducible polynomial, which is (x^2+x+1)

a.

q	r_1	r_2	r	t_1	t_2	t
x^2+x+1	x^2+x+1	1	0	0	1	1
	1	0		1	1	

The inverse of 1 is 1

b.

q	r_1	r_2	r	t_1	t_2	t
$x+1$	x^2+x+1	x	1	0	1	$x+1$
x	x	1	0	1	$x+1$	1
	1	0		$x+1$	1	

The inverse of x is $x+1$

c.

q	r_1	r_2	r	t_1	t_2	t
x	x^2+x+1	$x+1$	1	0	1	x
$x+1$	$x+1$	1	0	1	x	1
	1	0		x	1	

The inverse of $x+1$ is x

33.

q	r_1	r_2	r	t_1	t_2	t
$x+1$	x^5+x^2+1	x^4+x^3+1	x^3+x^2+x	0	1	$x+1$
x	x^4+x^3+1	x^3+x^2+x	x^2+1	1	$x+1$	x^2+x+1
$x+1$	x^3+x^2+x	x^2+1	1	$x+1$	x^2+x+1	x^3+x
x^2+1	x^2+1	1	0	x^2+x+1	x^3+x	1
	1	0		x^3+x	1	

The inverse of (x^4+x^3+1) is x^3+x

Scanned with CamScanner