암호학개론 HW#2 20191629 이주헌

Chapter 4

21. Redo Example 4.25 w/ $f(x) = x^4 + x^3 + 1$.

$0, g^0, g^1, g^2, g^3$ are trivial, and $g^4 = -g^3 - 1 = g^3 + 1$. Thus:

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

22. Redo example 4.26 w/ $f(x) = x^4 + x^3 + 1$.

The following shows the results of addition and subtraction:

a. $g^9 + g^{10} = (g^2+1) + (g^3+g) = g^3+g^2+g+1 = 1111_{(2)} = 0101_{(2)} + 1010_{(2)}$

b. $g^4 - g^3 = (g^3+1) - (g^3) = 1 = 0001_{(2)} = 1001_{(2)} - 1000_{(2)}$.

28. Prove that x and $x+1$ are irreducible polynomial of degree 1.

A polynomial $f(x)$ is reducible if polynomials with nonzero degree g, h exist that satisfies $f(x) = g(x) \cdot h(x)$. Here, degree(f) = degree(g) + degree(h). However, there exists no such polynomial that satisfies this equation. (at least one polynomial needs to be degree 0, which is not allowed by definition.)

29. Prove that (x^2+x+1) is an irreducible polynomials of degree 2.

Using the same definition as above, the given polynomial might be decomposed into two degree 1 polynomials. We can try to divide:

$$\begin{array}{r} x+1 \\ x \overline{)\, x^2+x+1} \\ \underline{x^2+x} \\ 1 \end{array} \qquad \begin{array}{r} x \\ x+1 \overline{)\, x^2+x+1} \\ \underline{x^2+x} \\ 1. \end{array}$$

There is always a remainder.
→ Cannot be factored.
→ Polynomial is irreducible. ∎

30. Prove that x^3+x^2+1 is an irreducible polynomial of degree 3.

Using the same definition, deg(3) = deg(2) + deg(1). If it could be decomposed, we should be able to factor a degree 1 polynomial out.

$$
\begin{array}{r|l}
 & x^2+1 \\
x & x^3+x+1 \\
 & x^3 \\ \hline
 & x+1 \\
 & x \\ \hline
 & 1.
\end{array}
\qquad
\begin{array}{r|l}
 & x^2+x \\
x+1 & x^3+x+1 \\
 & x^3+x^2 \\ \hline
 & x^2+x+1 \\
 & x^2+x \\ \hline
 & 1.
\end{array}
$$

There's always a remainder.

→ Polynomial is irreducible.

31. Multiply using polynomials.

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

b. $1010 \times 1000 = (x^3+x^2)(x^3) = x^6+x^4 = 1010000$

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

32. Find the multiplicative inverse in $GF(2^2)$.

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.	

⇒ Inverse 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		$x+1$	[illegible]	

⇒ inverse 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	

⇒ inverse is x.

33. Find the inverse of x^4+x^3+1 in $GF(2^5)$ with modulus (x^5+x^2+1).

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	

Inverse is x^3+x.