Glenn Chia 1003118

50.042 Foundations of Cybersecurity Lab 5

1. Create a table for addition and multiplication for GF(2^4), using (x^4 + x^3+ 1) as the modulus.

For this test case we will use

- g4 = x^3+x^2+1
- g5 = x^2+x

Row	Powers	Operation	New Result	Reduction	After reduction (XOR)
1	x^0 . g_4		x^3+x^2+1	N	
2	x^1 . g_4	x . x^3+x^2+1	x^4+x^3+x	Y	x + 1
3	x^2 . g_4	x . x+1	x^2+x	N	

We then take the `After reduction` results associated with row 2, 3

Result = (x^2 + x) + (x+1) = x^2+1

Addition table

	x^0	x^1	x^2	x^3
x^2 + x	0	1	1	0
x+1	1	1	0	0
Result	1	0	1	0

Result is x^2+1

2. Second example with a different GF(2^n)

For this part we will use the test case to illustrate

- p1 = x^5+x^2+x
- p4 = $x^7+x^4+x^3+x^2+x$
- modp = $x^8+x^7+x^5+x^4+1$

Row	Powers	Operation	New Result	Reduction	After reduction (XOR)
1	$x^0 . P_4$		$x^7+x^4+x^3+x^2+x$	N	
2	$x^1 . P_4$	$x . x^7+x^4+x^3+x^2+x$	$x^8+x^5+x^4+x^3+x^2$	Y	$x^7+x^3+x^2+1$
3	$x^2 . P_4$	$x . x^7+x^3+x^2+1$	$x^8+x^4+x^3+x$	Y	$x^7+x^5+x^3+x+1$
4	$x^3 . P_4$	$x . x^7+x^5+x^3+x+1$	$x^8+x^6+x^4+x^2+x$	Y	$x^7+x^6+x^5+x^2+x+1$
5	$x^4 . P_4$	$x . x^7+x^6+x^5+x^2+x+1$	$x^8+x^7+x^6+x^3+x^2+x$	Y	$x^6+x^5+x^4+x^3+x^2+x+1$
6	$x^5 . P_4$	$x . x^6+x^5+x^4+x^3+x^2+x+1$	$x^7+x^6+x^5+x^4+x^3+x^2+x$	N	

We then take the `After reduction` results associated with row 2, 3, 6

Result = $(x^7+x^3+x^2+1) + (x^7+x^5+x^3+x+1) + (x^7+x^6+x^5+x^4+x^3+x^2+x) = x^7+x^6+x^4+x^3$

Addition table

Doing the first addition

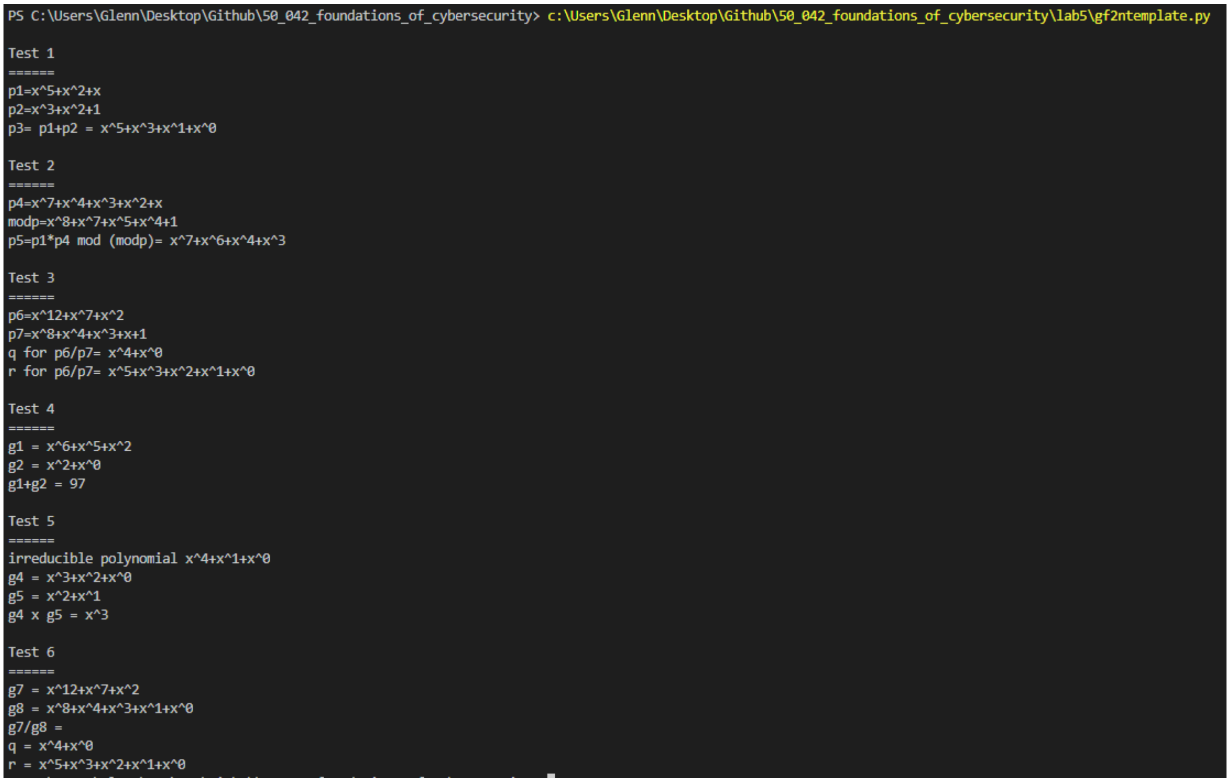
	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7
$x^7+x^3+x^2+1$	1		1	1				1
$x^7+x^5+x^3+x+1$	1	1		1		1		1
Result	0	1	1	0	0	1	0	0

Doing the second addition

	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7
x^5+x^2+x		1	1			1		
$x^7+x^6+x^5+x^4+x^3+x^2+x$		1	1	1	1	1	1	1
Result	0	0	0	1	1	0	1	1

The result is $x^7+x^6+x^4+x^3$

3. Lab's test case



```
PS C:\Users\Glenn\Desktop\Github\50_042_foundations_of_cybersecurity> c:\Users\Glenn\Desktop\Github\50_042_foundations_of_cybersecurity\lab5\gf2ntemplate.py

Test 1
======
p1=x^5+x^2+x
p2=x^3+x^2+1
p3= p1+p2 = x^5+x^3+x^1+x^0

Test 2
======
p4=x^7+x^4+x^3+x^2+x
modp=x^8+x^7+x^5+x^4+1
p5=p1*p4 mod (modp)= x^7+x^6+x^4+x^3

Test 3
======
p6=x^12+x^7+x^2
p7=x^8+x^4+x^3+x+1
q for p6/p7= x^4+x^0
r for p6/p7= x^5+x^3+x^2+x^1+x^0

Test 4
======
g1 = x^6+x^5+x^2
g2 = x^2+x^0
g1+g2 = 97

Test 5
======
irreducible polynomial x^4+x^1+x^0
g4 = x^3+x^2+x^0
g5 = x^2+x^1
g4 x g5 = x^3

Test 6
======
g7 = x^12+x^7+x^2
g8 = x^8+x^4+x^3+x^1+x^0
g7/g8 =
q = x^4+x^0
r = x^5+x^3+x^2+x^1+x^0
```