CSCI-4116
Assignment 7

Anas Alhadi

B00895875

March 12, 2025

Question 1

Given a polynomial $f \in (\mathbb{Z}/2\mathbb{Z})[x]$ where $deg(f) = 5$. The possible factors of f are polynomials $g, h \in (\mathbb{Z}/2\mathbb{Z})[x]$ such that g and h either have degrees 1 and 4, or 2 and 3.

To test for polynomials of degrees 1 and 4, all we need to do is determine if f has a zero of 1 or 0. If not then there is no linear polynomial that factors it (aka neither $x + 1$ nor x factor it, respectively).

To test for polynomials of degrees 2 and 3 we divide f by all the possible degree 2 polynomials in $(\mathbb{Z}/2\mathbb{Z})[x]$. Those being: $x^2, x^2 + 1, x^2 + x, x^2 + x + 1$.

1. $\mathbf{x^5+x^4+1}$**:**
   - <u>Degrees 1 and 4:</u>
   $$(1)^5 + (1)^4 + 1 = 1$$
   $$(0)^5 + (0)^4 + 1 = 1$$
   So neither $x + 1$ nor x factor it.

   - <u>Degrees 2 and 3:</u>
   $$\begin{aligned} x^5 + x^4 + 1 &= (x^2) \times (x^3 + x^2) && +1 \\ &= (x^2 + 1) \times (x^3 + x^2 + x + 1) && +x \\ &= (x^2 + x) \times (x^3) && +1 \\ &= (x^2 + x + 1) \times (x^3 + x + 1) && +0 \end{aligned}$$
   So $x^2 + x + 1$ and $x^3 + x + 1$ are factors of $x^5 + x^4 + 1$ in $(\mathbb{Z}/2\mathbb{Z})[x]$ thus it is <u>reducible</u>

2. $\mathbf{x^5+x^3+x^2+1}$**:**

   - Degrees 1 and 4:

     Observe that:

     $$(1)^5 + (1)^3 + (1)^2 + 1 = 0$$

     This means that $x - 1 = x + 1$ is a factor, thus it is reducible.

     Side note: we can confirm the degree 4 factor by dividing $\frac{x^5+x^3+x^2+1}{x+1} = x^4 + x^3 + x + 1$

3. $\mathbf{x^5+x^2+1}$

   - Degrees 1 and 4:

     $$(1)^5 + (1)^2 + 1 = 1$$
     $$(0)^5 + (0)^2 + 1 = 1$$

   - Degrees 2 and 3:

     $$\begin{aligned} x^5 + x^2 + 1 &= (x^2) \times (x^3 + 1) && +1 \\ &= (x^2 + 1) \times (x^3 + x + 1) && +x \\ &= (x^2 + x) \times (x^3 + x^2 + x) && +1 \\ &= (x^2 + x + 1) \times (x^3 + x^2) && +1 \end{aligned}$$

     Thus the polynomial is irreducible as it cannot be represented by the multiplication of any two non-zero polynomials $g, h \in (\mathbb{Z}/2\mathbb{Z})[x]$

Question 2

Part A

Given polynomials $f, g, h \in R[x]$ we say that $g \equiv h(\text{mod } f)$ iff $f|g - h$. So for this question, we divide $(g - h)$ by f in module 2, and if the remainder is 0 then the congruence holds.

1. $x^4 \equiv x + 1(\text{mod } x^4 + x + 1)$:
$$g - h = x^4 - (x + 1) = x^4 + x + 1$$
   Here $g - h = f$ so it clearly divides it and the congruence holds.

2. $x^8 \equiv x^2 + 1(\text{mod } x^4 + x + 1)$:
$$g - h = x^8 + x^2 + 1$$
   Dividing $(g - h)$ by f (using long division) we get a quotient:
$$\frac{x^8 + x^2 + 1}{x^4 + x + 1} = x^4 + x + 1$$
   So $g - h = f \times (x^4 + x + 1) + 0$. Thus f divides it and the congruence holds.

3. $x^{16} \equiv x(\text{mod } x^4 + x + 1)$:

   Similar to the previous cases, we have $g - h = x^{16} + x$ and dividing it by f in modulo 2 results in a quotient: $x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x$, and a remainder of 0

Part B

We know that $x^{16} + x = q \times f$ (where q is the quotient in part A). Dividing both sides by x, we get that $x^{15} + 1 = \frac{q}{x} \times f$. Where $\frac{q}{x}$ is a valid polynomial and is equal to: $x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$. Thus the congruence holds.

Question 3

To compute the product in the field, we simply multiply the 2 polynomials then reduce modulo $x^5 + x^2 + 1$ (by dividing and getting the remainder)

$$\begin{aligned}(x^4 + x^3) \times (x^3 + x^2 + 1) &= x^7 + x^6 + x^4 + x^6 + x^5 + x^3 \\ &= x^7 + x^5 + x^4 + x^3\end{aligned}$$

Then performing the long division: $\frac{x^7+x^5+x^4+x^3}{x^5+x^2+1}$, results in a quotient value $x^2 + 1$ and a remainder of $x^3 + 1$.

So, $(x^4 + x^3) \times (x^3 + x^2 + 1) = x^3 + 1$

Question 4

The Rijndael polynomial is: $x^8 + x^4 + x^3 + x + 1$.

The 2 bytes can be represented as the polynomials:

- $00000111 = x^2 + x + 1$
- $10101011 = x^7 + x^5 + x^3 + x + 1$

We now mutiply the 2 bytes and reduce them modulo the standard polynomial:

$$(x^2 + x + 1) \times (x^7 + x^5 + x^3 + x + 1) \quad = \quad x^9 + x^8 + x^6 + x^4 + 1$$

Dividing the resulting product by $x^8 + x^4 + x^3 + x + 1$. Results in a quotient value of: $x + 1$ and a remainder: $x^6 + x^5 + x^4 + x^3 + x^2$

Thus the result of the multiplication in $GF(2^8)$ is $x^6 + x^5 + x^4 + x^3 + x^2$, which corresponds to the byte: 01111100

Question 5

Part A

Here we need to show that x^2 has no linear factors (so polynomials of degree = 1). We repeat the process used in Question 1 to test for degrees 1 and 4, however in this case, that values that we subsitute in place of x are $a \in (\mathbb{Z}/3\mathbb{Z}) = \{0, 1, 2\}$.

$$(0)^2 + 1 = 1$$
$$(1)^2 + 1 = 2$$
$$(2)^2 + 1 = 5 = 2$$

Thus the polynomial has no linear factors, which means that it is irreducible.

Part B

The residue classes of the polynomial are $0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2$.

We set α to be the root of the polynomial so $\alpha^2 + 1 = 0$. Thus $\alpha^2 = -1 = 2$

$+$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	0
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	$\alpha+2$	α	$\alpha+1$

$\times$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	2	$\alpha+2$	$2\alpha+2$	1	$\alpha+1$	$2\alpha+1$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$\alpha+2$	2α	1	$2\alpha+1$	2	α
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$2\alpha+2$	1	α	$\alpha+1$	2α	2
2α	0	2α	α	1	$2\alpha+1$	$\alpha+1$	2	$2\alpha+2$	$\alpha+2$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$\alpha+1$	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$2\alpha+1$	α	2	$\alpha+2$	1	2α