From week 5 lab.

Q1. The coefficients live in $\mathbb{Z}_{11}$, so arithmetic on coefficients is done modulo 11.

Evaluate the product polynomial.

$$(x^2 + 2x + 9) \cdot (x^3 + 10x^2 + x + 7)$$

$$\begin{aligned} = \quad & x^5 + 10x^4 + x^3 + 7x^2 \\ & \quad 2x^4 + 20x^3 + 2x^2 + 14x \\ & \quad\quad 9x^3 + 2x^2 + 9x + 1 \end{aligned}$$

ADD

$$\boxed{x^5 + x^4 + 8x^3 + x + 1}$$

$9 \cdot 10 = 90$
$\equiv 2 \mod 11.$

$9 \cdot 7 = 56$
$\equiv 1 \mod 11$

where we've reduced many coefficients modulo 11

$30 \equiv 8 \mod 11$

$11 \equiv 0 \mod 11$

Working in $GF(2^8)$

The modulus polynomial for $GF(2^8)$

is $m(x) = x^8 + x^4 + x^3 + x + 1$

Consider $p(x) = x^5 + x^3 + x^2 + 1$

1. Confirm that $\gcd(m(x), p(x)) = 1$ using Euclidean algorithm.
2. Find p^{-1} within $GF(2^8)$.

E.A. The first poly. division with remainder will look like.

$$m(x) = q_1(x)\, p(x) + r_1(x)$$

for some polys q_1, r_1 where

$$\boxed{\deg(r_1) < \deg(p) = 5}$$

we'll construct q_1, r_1 step by step.

$$x^8 + x^4 + x^3 + x + 1$$

$$= x^3(x^5 + x^3 + x^2 + 1) + \underline{\quad ? \quad}$$

$$= x^8 + x^6 + x^5 + x^3 + \underline{x^6 + x^5 + x^4 + x + 1} \quad (*)$$

$$= x^3 p + x(x^5 + x^3 + x^2 + 1) + \underline{\quad ? \quad}$$

$$= x^3 p + x^6 + x^4 + x^3 + x + \underline{x^5 + x^3 + 1} \quad (**)$$

$$= (x^3 + x)p + \underline{x^5 + x^3 + 1}$$

$= (x^3+x)p + 1(x^5+x^3+x^2+1)$

$+x^2$

$= \underbrace{(x^3+x+1)}_{q_1} \cdot p + \underbrace{x^2}_{r_1} = m(x)$ ①

, $\deg(r_1) = 4 < 5 = \deg(p)$

So we have the first polynomial division with remainder for E.A.

The E.A. will continue with.

$$p = q_2 r_1 + r_2.$$

where $\deg(r_2) < \deg(r_1)$

Discover q_2, r_2 (step-by-step) straightaway

$$x^5 + x^3 + x^2 + 1 = \underline{(x^3+x+1)}\, x^2 + \underline{1}$$

So $q_2 = x^3 + x + 1$ and $r_2 = 1$. ②

So the E.A ends here and the final remainder is 1

So therefore $\gcd(m(x), p(x)) = 1$.

To obtain $p^{-1} \bmod m(x)$, ie. p^{-1} within $GF(2^8)$, we need to apply the extended Euclidean algorithm. ~~Cl~~ From (2) we get

$$1 = p + (x^3+x+1)x^2.$$

$$= p + (x^3+x+1)(m + (x^3+x+1)p)$$

, substituted for x^2 from (1).

$$= (x^3+x+1)m +$$

$$((x^3+x+1)(x^3+x+1)+1)p.$$

$$= (x^3+x+1)m$$

$$+ (x^6 + \cancel{x^4} + \cancel{x^3} + \cancel{x^4} + x^2 + \cancel{x} + \cancel{x^3} + \cancel{x} + \cancel{1} + \cancel{1})p.$$

$$1 = (x^3+x+1)m + (\boxed{x^6+x^2})\underline{p}$$

L output from Extended E.A.

From this ~~as~~ we see that

$$P^{-1} = \boxed{x^6 + x^2}$$