<u>Q1</u>.

$$a(x) = x^2 + 2x + 9$$
$$b(x) = x^3 + 11x^2 + x + 7.$$

Find the product $a(x) \cdot b(x)$, but noting the coeffs are understood to live in $\boxed{\mathbb{Z}_{11}}$.

Multiply as normal and reduce coeffs mod 11 afterwards.

$$\boxed{a(x) \cdot b(x)} = \quad x^5 + 11x^4 + x^3 + 7x^2$$
$$2x^4 + 22x^3 + 2x^2 + 14x.$$

(adding up)
$$\underline{\qquad\qquad 9x^3 + 99x^2 + 9x + 63 \qquad\qquad}$$

$$= x^5 + 13x^4 + 32x^3 + 108x^2 + 23x + 63$$

(reduce coeffs modulo 11)

$$\boxed{= x^5 + 2x^4 + 10x^3 + 9x^2 + x + 8}$$

(since $108 \equiv 9 \pmod{11}$ etc)

Polys with coeffs from $\boxed{\mathbb{Z}_2}$

<u>Second ex</u>

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$
$$p(x) = x^5 + x^3 + x^2 + 1.$$

First, apply the E.A. and confirm that
$$\gcd(m(x), p(x)) = 1.$$
E.A. proceeds with a sequence of

"poly. divisions with remainder"
the first of which will be

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

for some polys q_1, r_1 and $\deg(r_1) < \deg(\underbrace{p}_{P})$

$$x^8 + x^4 + x^3 + x + 1 = \overbrace{x^3 (x^5 + x^3 + x^2 + 1)}^{P}$$

$$= \underbrace{(x^8 + x^6 + x^5 + x^3)}_{x^3 P} + \underbrace{(x^6 + x^5 + x^4 + x + 1)}$$

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

$$= x^3 \, p(x) + \underbrace{(x^6 + x^4 + x^3 + x)}_{x \, p(x)} + x^5 + x^3 + 1 .$$

$$= (x^3 + x) \, p(x) + x^5 + x^3 + 1$$

$$= \underbrace{(x^3 + x + 1) \, p(x)}_{q_1(x) \cdot p(x)} + \underbrace{x^2}_{+ \, r_1(x)} . \qquad \textcircled{1} \begin{array}{l} q_1(x) = x^3 + x + 1 \\ r_1(x) = x^2 \end{array}$$

Now obtain the second poly-div. with rem.

$$p(x) = q_2(x) \, r_1(x) + r_2(x)$$

$$x^5 + x^3 + x^2 + 1 = \underbrace{(x^3 + x + 1)}_{q_2(x)} \underbrace{x^2}_{r_1(x)} + \overset{r_2(x)}{1} . \qquad \textcircled{2}$$

The fact we obtain a remainder poly. 1
confirms that $\gcd(m(x), p(x)) = 1$

Now for $p^{-1}(x)$ in $GF(2^8)$.

So we seek a poly p^{-1} such that

$$p^{-1}(x) \, p(x) \equiv 1 \mod m(x)$$

From ② we get

$$1 = p(x) + q_2(x) \, x^2$$

then from eq. ①, I replace x^2
to set.

$$1 = p(x) + q_2(x) \left(m(x) + q_1(x) \, p(x) \right)$$

$$= q_2(x) \, m(x) + \left(1 + q_2(x) \, q_1(x) \right) \, p(x)$$

$$\underbrace{\qquad\qquad}_{p^{-1}(x)}$$

So $\left(1 + q_2(x) q_1(x) \right) p(x) \equiv 1 \mod m(x)$

So $p^{-1}(x) = 1 + q_2(x) \, q_1(x)$

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

$$= 1 + x^6 + x^4 + x^3 + x^4 + x^2 + x$$
$$+ x^3 + x + 1$$

$$= x^6 + x^2.$$

So finally we can say
$$p^{-1}(x) = x^6 + x^2.$$

We could go an confirm
$$(x^6 + x^2)(x^5 + x^3 + x^2 + 1)$$

$$= x^{11} + \cdots \cdots + x^2$$

$$= (\underbrace{\quad\quad}_{\text{some qoutient poly.}}) m(x) + 1.$$

$$\equiv 1 \quad (\bmod\ m(x)).$$