







Q3 Second part.

$a(x) = x^4 + 8x^3 + 7x + 8$ ,  $b(x) = 2x^3 + 9x^2 + 10x + 1$   
as polys. with coeffs in  $\mathbb{GF}(11)$ , i.e.  $\mathbb{Z}_{11} = \{0, 1, \dots, 10\}$   
with  $+$ ,  $\times$  done modulo 11.

Execute the E.A. to find  $\gcd(a(x), b(x))$ .

First division we need is

$$a(x) = q(x)b(x) + r(x), \quad \deg(r(x)) < \deg(b(x))$$

Might need inverses mod 11

$x$	1	2	3	4	5	6	7	8	9	10
$x^{-1}$	1	6	4	3	9	2	8	7	5	10

$$\begin{aligned}
 a(x) &= 6x b(x) + r(x) \\
 &= (x^4 + 10x^3 + 5x^2 + 6x) + (-2x^3 - 5x^2 + x + 8) \\
 &= 6x b(x) + \underline{9x^3 + 6x^2 + x + 8} \\
 &= 6x b(x) + 10b(x) + r(x) \\
 &= 6x b(x) + \underline{9x^3 + 2x^2 + x + 10} + r(x) \\
 &= \underbrace{(6x + 10)}_{q_1(x)} b(x) + \underbrace{4x^2 - 2}_{r_1(x)}
 \end{aligned}$$

1st  
division.

$$2x^3 + 9x^2 + 10x + 1$$

$$b(x) = q_1(x)r_1(x) + r_2(x)$$

$$= 6x r_1(x) + r_2(x)$$

$$= (2x^3 + 10x) + 9x^2 + 1$$

$$\begin{aligned}
 &= 6x r(x) + 5r(x) + r_2(x) \\
 &= 6x r(x) + 9x^2 + 1 + \underline{\underline{0}} \\
 &= \underline{(6x + 5) r(x) + 0}
 \end{aligned}$$

So E.A. stops. And reports the last non-zero remainder as the gcd.

So finally,

$$\gcd(a(x), b(x)) = r(x) = 4x^2 - 2.$$

---

When working over  $GF(2)$  we can be quicker.

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

$$b(x) = x^2 + x + 1$$

$$\boxed{a(x) = q(x) b(x) + r(x)}$$

$$= x b(x) + r(x)$$

$$= \underbrace{(x^3 + x^2 + x)}_{x b(x)} + \underbrace{x^2 + x + 1}_{b(x)}$$

$$= x b(x) + b(x)$$

$$= \underline{(x+1) b(x) + \underline{\underline{0}}}$$

we have exact divisibility here

and  $\gcd(a(x), b(x)) = b(x)$











