Exercise 1. Calculate cyclotomic polynomials

$$F_1(X), F_2(X), F_4(X), F_8(X), F_{16}(X), F_{15}(X)$$

and then calculate their images in the ring $\mathbb{Z}_3[X]$, under the homomorphism $\mathbb{Z}[X] \to \mathbb{Z}_3[X]$ induced by the quotient homomorphism $\mathbb{Z} \mapsto \mathbb{Z}_3$. Which of them are irreducible over $\mathbb{Z}_3$?

$F_1(X) = X - 1$ is easy, then $X^2 - 1 = (X-1)(X+1)$, so $F_2(x) = x + 1$ because $x = 1$ is not a primitive root of order 2.

With $F_4(X)$ I know that it cannot have degree 4 because 2 divides 4 and cannot be counted in $\phi(4)$. I use the definition of F_m from the lecture and write:

$$F_4(x) = (x - e^{\frac{\pi i}{2}})(x - e^{\frac{3\pi i}{2}}) = x^2 - x(e^{\frac{3\pi i}{2}} + e^{\frac{\pi i}{2}}) + e^{2\pi i} =$$
$$= x^2 + 1$$

However, I think I could get it from the fact that the roots of a cyclotomic polynomial F_m are all the primitive roots of 1 of order m. So

$$x^4 - 1 = (x^2 - 1)(x^2 + 1)$$

and every root that comes from $x^2 - 1$ is not primitive, so only $x^2 + 1$ has primitive roots of order 4.

A similar story is with F_8 :

$$x^8 - 1 = (x^4 - 1)(x^4 + 1) \implies F_8(x) = x^4 + 1$$

$F_{15}(x)$ should have degree 8 and so here is a lot of computation to avoid multiplying $\prod_{\substack{1 \le k < 15 \\ \gcd(k,15)=1}} (x - e^{k\frac{2\pi i}{15}})$

because why not

$$\begin{aligned}
x^{15} - 1 &= (x-1)(x^{14} + x^{13} + \dots + x + 1) = \\
&= (x-1)(x^{12}(x^2 + x + 1) + x^9(x^2 + x + 1) + \dots + x^2 + x + 1) = \\
&= (x-1)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1) = \\
&= (x-1)(x^2 + x + 1)(x^{12} + x^{11} - x^{11} + x^{10} - x^{10} + \dots + x^3 + x^2 - x^2 + x - x + 1) = \\
&= (x-1)(x^2 + x + 1)(x^8(x^4 + x^3 + x^2 + x + 1) - x^7(x^4 + 1) + x^6(x^4 + \dots + 1) - \dots + (x^4 + x^3 + x^2 + x + 1)) = \\
&= \underbrace{(x-1)}_{=F_1(x)}\underbrace{(x^2 + x + 1)}_{\text{div. } F_3(x)}\underbrace{(x^4 + x^3 + x^2 + x + 1)}_{\text{div. } F_5(x)}(x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1)
\end{aligned}$$

$$\Downarrow$$

$$F_{15}(x) = x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$$

And now for the final boss because I messed up the order in which they should appear and am too lazy to change it: $F_{16}(x)$!!! I expect it to have order 8

$$x^{16} - 1 = (x^8 - 1)(x^8 + 1) \implies F_{16}(x) = x^8 + 1$$

Images in $\mathbb{Z}_3[X]$:

$$F_1(x) = x - 1 \mapsto x + 2$$
$$F_2(x) = x + 1 \mapsto x + 1$$
$$F_4(x) = x^2 + 1 \mapsto x^2 + 1$$
$$F_8(x) = x^4 + 1 \mapsto x^4 + 1$$
$$F_{16}(x) = x^8 + 1 \mapsto x^8 + 1$$
$$F_{15}(x) = x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \mapsto x^8 + 2x^7 + x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1$$

Most of them are irreducible as they have no roots in $\mathbb{Z}_3$ but $F_{15}(2) = 681 \mod 3 = 0$