1. Let $R = \mathbb{F}_3[x]$ and $p = x^2 + x$.

   (a) List the 9 residue classes in R/pR. (You may omit the bars in the residue class notation.)

   - As we have discussed, the polynomials in R of degree less than $\deg(p) = 2$ give representatives for the residue classes.
   - Thus, the residue classes are $\boxed{\overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2}}$.

   (b) Construct the addition and multiplication tables for R/pR.

   - Here is the addition table:

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

   - Here is the multiplication table:

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	$2x$	0	x	x	$2x$	0
$x+1$	0	$x+1$	$2x+2$	0	$x+1$	$2x+2$	0	$x+1$	$2x+2$
$x+2$	0	$x+2$	$2x+1$	x	$2x+2$	1	$2x$	2	$x+1$
$2x$	0	$2x$	x	x	0	$2x$	$2x$	x	0
$2x+1$	0	$2x+1$	$x+2$	$2x$	$x+1$	2	x	1	$2x+2$
$2x+2$	0	$2x+2$	$x+1$	0	$2x+2$	$x+1$	0	$2x+2$	$x+1$

   (c) Identify all of the units and zero divisors in R/pR.

   - We can see that $\boxed{\overline{1}, \overline{2}, \overline{x+2}, \overline{2x+1}}$ are units, while $\boxed{\overline{x}, \overline{x+1}, \overline{2x}, \overline{2x+2}}$ are zero divisors.
   - We can see that the units are the polynomials that are relatively prime to $x^2 + x$, while the zero divisors are the polynomials having a nontrivial common divisor with $x^2 + x$.

   (d) Find the order of each unit in R/pR. Are there any primitive roots?

   - We see $2^2 \equiv 1$, $(x+2)^2 \equiv 1$, and $(2x+1)^2 \equiv 1$, so the orders of the four units $\overline{1}, \overline{2}, \overline{x+2}, \overline{2x+1}$ are $\boxed{1, 2, 2, 2}$ respectively. Since there are 4 units, there are $\boxed{\text{no primitive roots}}$.

   (e) Verify Euler's theorem for each unit in R/pR.

   - There are 4 units, so we need to verify that $u^4 \equiv 1 \pmod{p}$ for each of the 4 units u.
   - Via successive squaring and the multiplication table, we see easily that $1^4 \equiv 2^4 \equiv (x+2)^4 \equiv (2x+1)^4 \equiv 1 \pmod{p}$, as needed.

2. Let $R = \mathbb{F}_2[x]$ and $p = x^3 + x + 1$.

(a) List the 8 residue classes in R/pR. (You may omit the bars in the residue class notation.)

- As we have discussed, the polynomials in R of degree less than $\deg(p) = 3$ give representatives for the residue classes.
- Thus, the residue classes are $\boxed{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}}$.

(b) Construct the addition and multiplication tables for R/pR.

- Here is the addition table:

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+x+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2+x	$x+1$	x	1	0

- Here is the multiplication table:

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(c) Show that R/pR is a field by explicitly identifying the inverse of every nonzero element. [Hint: Use the multiplication table from (b).]

- We can just search through the multiplication table to identify each of these inverses:

Element	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
Inverse	1	x^2+1	x^2+x	x^2+x+1	x	$x+1$	x^2

(d) Find the order of each unit in R/pR. Are there any primitive roots?

- We can take powers of each element using the multiplication table. For example, $(x^2)^2 \equiv x^2 + x$, $(x^2)^3 \equiv (x^2)^2(x^2) \equiv (x^2+x)(x^2) \equiv x^2 + 1$, $(x^2)^4 \equiv (x^2+x)^2 \equiv x$, and so forth. Checking powers yields the following orders:

Element	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
Order	1	7	7	7	7	7	7

- In fact, each unit other than 1 has order 7, so all of $\boxed{x, x+1, x^2, x^2+1, x^2+x, x^2+x+1}$ are primitive roots.

(e) Verify Fermat's little theorem for the elements $\overline{x}$ and $\overline{x+1}$ in R/pR.

- We need to verify that $u^8 \equiv u$ for each element u, which we can easily do with successive squaring using the multiplication table.
- We compute $\overline{x}^2 = \overline{x^2}$, $\overline{x}^4 = (\overline{x^2})^2 = \overline{x^2+x}$, and $\overline{x}^8 = (\overline{x^2+x})^2 = \overline{x}$.
- Likewise, $\overline{x+1}^2 = \overline{x^2+1}$, $\overline{x+1}^4 = (\overline{x^2+1})^2 = \overline{x^2+x+1}$, and $\overline{x+1}^8 = (\overline{x^2+x+1})^2 = \overline{x+1}$.

---

3. Let $R = \mathbb{Z}[i]$ and $p = 2 + 2i$. You are given that there are 8 residue classes modulo p, represented by 0, 1, 2, -1, $1 - i$, i, $1 + i$, and $-i$.

   (a) Construct the addition and multiplication tables for R/pR. (Please leave the elements in the order given above: when you work out the tables you will see they are given in that order for a reason!)

   - Here is the addition table:

$+$	0	1	2	-1	$1-i$	i	$1+i$	$-i$
0	0	1	2	-1	$1-i$	i	$1+i$	$-i$
1	1	2	-1	0	i	$1+i$	$-i$	$1-i$
2	2	-1	0	1	$1+i$	$-i$	$1-i$	i
-1	-1	0	1	2	$-i$	$1-i$	i	$1+i$
$1-i$	$1-i$	i	$1+i$	$-i$	0	1	2	-1
i	i	$1+i$	$-i$	$1-i$	1	2	-1	0
$1+i$	$1+i$	$-i$	$1-i$	i	2	-1	0	1
$-i$	$-i$	$1-i$	i	$1+i$	-1	0	1	2

   - Here is the multiplication table:

$\cdot$	0	1	2	-1	$1-i$	i	$1+i$	$-i$
0	0	0	0	0	0	0	0	0
1	0	1	2	-1	$1-i$	i	$1+i$	$-i$
2	0	2	0	2	0	2	0	2
-1	0	-1	2	1	$1-i$	$-i$	$1+i$	i
$1-i$	0	$1-i$	0	$1-i$	2	$1+i$	2	$1+i$
i	0	i	2	$-i$	$1+i$	-1	$1-i$	1
$1+i$	0	$1+i$	0	$1+i$	2	$1-i$	2	$1-i$
$-i$	0	$-i$	2	i	$1+i$	1	$1-i$	-1

   (b) Identify all of the units and zero divisors in R/pR.

   - We can see that $\boxed{1, -1, i, -i}$ are units, while $\boxed{2, 1-i, 1+i}$ are zero divisors.
   - The units are the elements relatively prime to $2 + 2i$, while the zero divisors are the elements not relatively prime to $2 + 2i$.

   (c) Find the order of each unit in R/pR. Are there any primitive roots?

   - We have $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, so i has order 4. Similarly, $-i$ has order 4, while -1 has order 2 and 1 has order 1. Since there are 4 units, we see that $\boxed{i, -i}$ are primitive roots.

---

4. Find the following multiplicative inverses:

   (a) The multiplicative inverse of $x + 3$ inside $\mathbb{Q}[x]$ modulo $x^2 + 1$.

   - First we apply the Euclidean algorithm in $\mathbb{Q}[x]$:

$$\begin{aligned} x^2 + 1 &= (x - 3) \cdot (x + 3) + 10 \\ x + 3 &= (\frac{1}{10}x + \frac{3}{10}) \cdot 10 \end{aligned}$$

     and so $x^2 + 1$ and $x + 3$ are relatively prime in $\mathbb{Q}[x]$, so $x + 3$ is a unit modulo $x^2 + 1$.
   - By back-solving we see that $(x^2 + 1) - (x - 3)(x + 3) = 10$, or equivalently, $\frac{1}{10}(x^2 + 1) + (-\frac{1}{10}x + \frac{3}{10})(x + 3) = 1$.
   - By reducing modulo $x^2 + 1$, we conclude that the inverse of $x + 3$ is $\boxed{-\frac{1}{10}x + \frac{3}{10}}$ modulo $x^2 + 1$.

   (b) The multiplicative inverse of $1 - 2i$ inside $\mathbb{Z}[i]$ modulo $8 + 7i$.

   - First we apply the Euclidean algorithm in $\mathbb{Z}[i]$:

$$\begin{aligned} 8 + 7i &= (-1 + 5i) \cdot (1 - 2i) + (-1) \\ 1 - 2i &= (1 + 2i) \cdot (-1) \end{aligned}$$

     and so $8 + 7i$ and $1 - 2i$ are relatively prime in $\mathbb{Z}[i]$, so $1 - 2i$ is a unit mod $8 + 7i$.

- By back-solving we see that $8+7i+(1-5i)\cdot(1-2i)=-1$ so that $-(8+7i)+(-1+5i)\cdot(1-2i)=1$.
- By reducing modulo $8+7i$, we conclude that the inverse of $1-2i$ is $\boxed{-1+5i}$ mod $8+7i$.

(c) The multiplicative inverse of x^2+1 inside $\mathbb{F}_3[x]$ modulo x^4+2x+1.

- First we apply the Euclidean algorithm in R:

$$\begin{aligned} x^4+2x+1 &= (x^2+2)\cdot(x^2+1)+(2x+2) \\ x^2+1 &= (2x+1)\cdot(2x+2)+2 \\ 2x+2 &= (x+1)\cdot 2 \end{aligned}$$

  and so we see that x^4+2x+1 and x^2+1 are relatively prime in $\mathbb{F}_3[x]$, so x^2+1 is a unit mod x^4+2x+1.
- By back-solving we obtain

$$\begin{aligned} 2x+2 &= (x^4+2x+1)-(x^2+2)(x^2+1) \\ 2 &= (x^2+1)-(2x+1)(2x+2)=[2x^3+x^2+x](x^2+1)-(2x+1)(x^4+2x+1) \end{aligned}$$

  and thus by scaling by 2 we obtain $1=\left[x^3+2x^2+2x\right](x^2+1)-(x+2)(x^4+2x+1)$.
- By reducing modulo x^4+2x+1, we conclude that the inverse of x^2+1 is $\boxed{x^3+2x^2+2x}$ mod x^4+2x+1.

(d) The multiplicative inverse of $4+8i$ inside $\mathbb{Z}[i]$ modulo $11-14i$.

- First we apply the Euclidean algorithm in R:

$$\begin{aligned} 11-14i &= (-1-2i)\cdot(4+8i)+(-1+2i) \\ 4+8i &= (2-3i)\cdot(-1+2i)+i \\ -1+2i &= (2-i)\cdot i \end{aligned}$$

  and so $11-14i$ and $4+8i$ are relatively prime in $\mathbb{Z}[i]$, so $4+8i$ is a unit modulo $11-14i$.
- Thus we see $(-2+3i)\cdot(11-14i)+(-7-i)\cdot(4+8i)=i$, so that $(3+2i)\cdot(11-14i)+(-1+7i)\cdot(4+8i)=1$.
- By reducing modulo $11-14i$, we conclude that the inverse of $4+8i$ is $\boxed{-1+7i}$ modulo $11-14i$.

---

5. (a) Solve the simultaneous congruences $p\equiv 1 \pmod{x+2}$ and $p\equiv 7 \pmod{x-1}$ in $\mathbb{Q}[x]$.

- Since $x-1$ and x are relatively prime polynomials, by the Chinese Remainder Theorem all we have to do is find one polynomial satisfying the system.
- The solution of the first congruence is $p(x)=1+(x+2)a$ for some polynomial a.
- Plugging into the second congruence yields $1+(x+2)a\equiv 7 \pmod{x-1}$.
- Since $1+(x+2)a\equiv 1+3a \pmod{x-1}$ since $x+2\equiv 3 \pmod{x-1}$, we can take $a=2$.
- Hence the polynomial $q(x)=1+2(x+2)=2x+5$ is a solution to the system.
- The general solution is therefore $\boxed{q(x)=2x+5+(x-1)(x+2)\cdot s(x)}$ for an arbitrary polynomial $s(x)\in R$. Equivalently, the solution is $\boxed{q(x)\equiv 2x+5 \pmod{x^2+x-2}}$.

(b) Solve the simultaneous congruences $z\equiv 1 \pmod{2+2i}$ and $z\equiv -i \pmod{4+5i}$ in $\mathbb{Z}[i]$.

- The solution of the second congruence is $z=-i+(4+5i)a$ for some $a\in\mathbb{Z}[i]$.
- Plugging into the first congruence yields $-i+(4+5i)a\equiv 1 \pmod{2+2i}$, which reduces to $ia\equiv 1+i \pmod{2+2i}$ since $4+5i\equiv i \pmod{2+2i}$.
- Multiplying both sides by $-i$ yields $a\equiv 1-i \pmod{2+2i}$, so $a=(1-i)+(2+2i)b$ for an arbitrary $b\in\mathbb{Z}[i]$.
- Hence the solution is $z=-i+(4+5i)a=-i+(4+5i)[(1-i)+(2+2i)b]=\boxed{9+(4+5i)(2+2i)b}$ for an arbitrary $b\in\mathbb{Z}[i]$. Equivalently, the solution is $\boxed{z\equiv 9 \pmod{-2+18i}}$.

---

6. Suppose $r, s \in \mathbb{Z}[\sqrt{D}]$ and that $N(r)$ and $N(s)$ are relatively prime integers. Show that 1 is a greatest common divisor of r and s in $\mathbb{Z}[\sqrt{D}]$.

   - Solution 1: Suppose d is a common divisor of r and s: then $N(d)$ divides $N(r)$ and $N(s)$. But since $N(r)$ and $N(s)$ are relatively prime, this implies $N(d)$ divides 1, hence that d is a unit. Thus, the only possible common divisors of r and s are units, so since all units divide 1, that means 1 is a gcd of r and s.
   - Solution 2: Since $N(r)$ and $N(s)$ are relatively prime, there exist integers x and y such that $xN(r) + yN(s) = 1$. But this says $x(r\overline{r}) + y(s\overline{s}) = 1$ so that $(x\overline{r})r + (y\overline{s})s = 1$, so then if $d|r$ and $d|s$ then $d|[(x\overline{r})r + (y\overline{s})s] = 1$, so d divides 1. Hence all common divisors of r, s divide 1, so 1 is a gcd.

---

7. Show the following things:

   (a) Show that the element $4 + 5i$ is irreducible and prime in $\mathbb{Z}[i]$.
   - Note that $N(4 + 5i) = 4^2 + 5^2 = 41$ is a prime number, so $4 + 5i$ is irreducible.
   - Since $\mathbb{Z}[i]$ is a Euclidean domain, irreducible and prime elements are the same, so $4+5i$ is also prime.

   (b) Show that the element $x^2 + 4x + 5$ is irreducible and prime in $\mathbb{R}[x]$.
   - Note that $x^2 + 4x + 5$ is irreducible because it has no nontrivial factorization in $\mathbb{R}[x]$, since it is quadratic and has no roots in $\mathbb{R}$. Indeed, by the quadratic formula, its roots are $-2 \pm i$.
   - Since $\mathbb{R}[x]$ is a Euclidean domain, irreducible and prime elements are the same, so x^2+4x+5 is also prime.

   (c) Show that the element $x^2 + 4x + 5$ is neither irreducible nor prime in $\mathbb{C}[x]$ by finding a factorization.
   - As noted in (b), this quadratic polynomial has roots $-2\pm i$ so we obtain the factorization $x^2+4x+5 = (x + 2 - i)(x + 2 + i)$.

   (d) Show that the element $3 + 5i$ is neither irreducible nor prime in $\mathbb{Z}[i]$ by finding a factorization.
   - Note that $N(3 + 5i) = 3^2 + 5^2 = 34$, so if there were a factorization of $3 + 5i$, it would be into a product of an element of norm 2 with an element of norm 17.
   - Since the elements of norm 2 are $\pm 1 \pm i$, we can simply try dividing by some of them: indeed, $3 + 5i = \boxed{(1 + i)(4 + i)}$, so $3 + 5i$ has a nontrivial factorization and is therefore not irreducible. It is also not prime, again since $\mathbb{Z}[i]$ is a Euclidean domain.

   (e) Show that the element $2 + \sqrt{-10}$ is irreducible but not prime in $\mathbb{Z}[\sqrt{-10}]$. [Hint: Show it divides 14 and that there are no elements of norm 2 or 7.]
   - If we had a factorization $2+\sqrt{-10} = bc$ then taking norms would give $14 = N(2+\sqrt{-10}) = N(b)N(c)$.
   - But there are no elements of norm ± 2 or ± 7, since $N(a+b\sqrt{-10}) = a^2 + 10b^2$, and there are clearly no integer solutions to $a^2 + 10b^2 = \pm 2, \pm 7$.
   - Thus, there is no possible factorization of $2 + \sqrt{-10}$, so it is irreducible.
   - To show it is not prime, observe that $(2 + \sqrt{-10})(2 - \sqrt{-10}) = 14 = 2 \cdot 7$, so $2 + \sqrt{-10}$ divides 14.
   - But $2 + \sqrt{-10}$ does not divide 2 or 7: explicitly doing the divisions yields $\dfrac{2}{2 + \sqrt{-10}} = \dfrac{2 - \sqrt{-10}}{7}$ and $\dfrac{7}{2 + \sqrt{-10}} = \dfrac{2 - \sqrt{-10}}{2}$, and neither of these is an element of $\mathbb{Z}[\sqrt{-10}]$.
   - Therefore, $2 + \sqrt{-10}$ is not prime.

---

8. We can use successive squaring and the same order-calculation procedure we used in $\mathbb{Z}/m\mathbb{Z}$ to establish the order of an arbitrary unit residue class $\overline{s}$ in R/rR: explicitly, $\overline{s}$ has order n if and only if $\overline{s}^n = \overline{1}$ and $\overline{s}^{n/p} \neq \overline{1}$ for any integer prime p dividing n.

   (a) Show that the element $2+i$ has order 8 in $\mathbb{Z}[i]$ modulo $r = 3+5i$.

   - Using successive squaring, we can compute $(2+i)^2 \equiv -i \pmod{r}$, so that $(2+i)^4 \equiv -1 \pmod{r}$ and then $(2+i)^8 \equiv 1 \pmod{r}$.
   - Since $(2+i)^8$ is congruent to 1 but $(2+i)^{8/2}$ is not, we conclude that $2+i$ has order 8.

   (b) Show that the element $\overline{x}$ has order 6 in $\mathbb{F}_7[x]$ modulo $r = x^2+x+5$.

   - Using successive squaring, we can compute $x^2 \equiv 6x+2$ and $x^4 \equiv 2x+6 \pmod{r}$, so that $x^6 \equiv x^4 \cdot x^2 \equiv 1$, while $x^2 \equiv 6x+2$ and $x^3 \equiv 3x+5$.
   - Since x^6 is congruent to 1 but $x^{6/2}$ and $x^{6/3}$ are not, we conclude that $\overline{x}$ has order 6.

   (c) Show that $R = \mathbb{F}_5[x]$ modulo $r = x^2+2$ is a field with 25 elements, and deduce that the order of any nonzero residue class in R/rR divides 24.

   - Note that x^2+2 is irreducible in R because it is of degree 2 and has no roots. Thus, by our results, R/rR is a field.
   - The elements of this field are precisely the residue classes of the form $\overline{a+bx}$ for $a, b \in \mathbb{F}_5$, and since there are exactly $5^2 = 25$ such residue classes, we see R/rR has 25 elements.
   - Then we see immediately that there are 24 units in R/rR, and so by Euler's theorem, the order of any element divides 24.

   (d) Find the orders of $\overline{2}$, $\overline{x}$, and $\overline{x+1}$ in $\mathbb{F}_5[x]$ modulo x^2+2. Are any of them primitive roots? [Hint: By (c), the order of each element divides 24, so search among divisors of 24.]

   - To determine the order of a, we can compute a, a^2, a^3, a^4, a^6, a^8, a^{12} mod x^2+2 using successive squaring, and then test which of these are congruent to 1 modulo x^2+2.
   - We have $2^4 \equiv 1$ but $2^2 \equiv 4$, so $\overline{2}$ has order $\boxed{4}$.
   - Also, $x^8 \equiv 1$ but $x^4 \equiv 4$, so $\overline{x}$ has order $\boxed{8}$.
   - Finally, $x+1$ has $(x+1)^{24} \equiv 1$, but $(x+1)^8 \equiv x+2$ and $(x+1)^{12} \equiv 4$. Thus, $\overline{x+1}$ has order $\boxed{24}$, and is a primitive root.

   (e) Show that the element $\overline{ax+b}$ in $R = \mathbb{F}_5[x]$ modulo $q = x^2$ is a unit precisely when $b \neq 0$ in $\mathbb{F}_5$. Deduce that R/qR has exactly 20 units.

   - As we have shown, the residue class $\overline{ax+b}$ will be a unit precisely when $ax+b$ is relatively prime to the modulus x^2.
   - The only way $ax+b$ could fail to be relatively prime to the modulus x^2 is if $ax+b$ is divisible by x, which happens precisely when $b = 0$. So the element is a unit if and only if $b \neq 0$, as claimed.
   - To count the number of units note that there are 5 choices for a and 4 choices for b, for a total of $5 \cdot 4 = 20$ unit residue classes.

   (f) Find the orders of $\overline{2}$, $\overline{x+1}$ and $\overline{x+2}$ in $\mathbb{F}_5[x]$ modulo x^2. Are any of them primitive roots? [Hint: The orders divide 20, by (e).]

   - By Euler's theorem, the order of any unit divides 20. So we can compute a, a^2, a^4, a^5, and a^{10} mod x^2 using successive squaring, and then test which of these are congruent to 1 modulo x^2.
   - We have $2^4 \equiv 1$ but $2^2 \equiv 4$, so $\overline{2}$ has order $\boxed{4}$.
   - Also, $(x+1)^5 \equiv 1$ but $(x+1)^1 \equiv x+1$, so $\overline{x+1}$ has order $\boxed{5}$.
   - Finally, $(x+2)^{20} \equiv 1$ but $(x+2)^{10} \equiv 4$ and $(x+2)^4 \equiv 2x+1$, so $\overline{x+2}$ has order $\boxed{20}$, and is a primitive root.
