---

1. For each polynomial $p(x)$ in the given polynomial rings $F[x]$, either find a nontrivial factorization or explain briefly why it is irreducible:

   (a) $p(x) = x^2 + 2$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.

   - Since this polynomial has degree 2, we need only check whether it has any roots in the field.
   - In $\mathbb{F}_2$ we have the obvious factorization $p(x) = \boxed{x \cdot x \text{ in } \mathbb{F}_2[x]}$.
   - In $\mathbb{F}_3$, we see $p(1) = 0$ so we obtain a factorization $p(x) = \boxed{(x+1)(x+2) \text{ in } \mathbb{F}_3[x]}$.
   - In $\mathbb{F}_5$, we see $p(0) = 2$, $p(1) = p(4) = 3$, and $p(2) = p(3) = 1$, so it has no roots hence is $\boxed{\text{irreducible in } \mathbb{F}_5[x]}$.
   - We can see that this polynomial has no rational roots because it does not even have any real roots, so it is $\boxed{\text{irreducible in } \mathbb{Q}[x]}$ and $\boxed{\text{irreducible in } \mathbb{R}[x]}$.
   - But it does factor over as $p(x) = \boxed{(x - i\sqrt{2})(x + i\sqrt{2}) \text{ in } \mathbb{C}[x]}$.

   (b) $p(x) = x^3 + x^2 + 2$ in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{F}_7[x]$.

   - Since this polynomial has degree 3, we need only check whether it has any roots in the field.
   - In $\mathbb{F}_3$, we see $p(0) = 2$, $p(1) = 1$, and $p(2) = 2$, so it has no roots hence is $\boxed{\text{irreducible in } \mathbb{F}_3[x]}$.
   - In $\mathbb{F}_5$, we see $p(0) = 2$, $p(1) = 4$, $p(2) = 4$, $p(3) = 3$, and $p(4) = 2$, so it has no roots hence is $\boxed{\text{irreducible in } \mathbb{F}_5[x]}$.
   - In $\mathbb{F}_7$, we see $p(2) = 0$ and so $x - 2 = x + 5$ will be a factor of $p(x)$. We obtain the factorization $p(x) = \boxed{(x+5)(x^2+3x+6) \text{ in } \mathbb{F}_7[x]}$.

   (c) $p(x) = x^4 + 1$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{R}[x]$. [Hint: This polynomial factors in each case.]

   - It is easy to see that $p(x) = \boxed{(x+1)^4 \text{ in } \mathbb{F}_2[x]}$.
   - Note that $p(x)$ has no roots in $\mathbb{F}_3$, $\mathbb{F}_5$, or $\mathbb{R}$, so the only way it could factor over any of these fields is as a product of two quadratics.
   - Searching for possibilities eventually reveals the factorizations $p(x) = \boxed{(x^2+x+2)(x^2-x+2) \text{ in } \mathbb{F}_3[x]}$, $p(x) = \boxed{(x^2+2)(x^2+3) \text{ in } \mathbb{F}_5[x]}$, and $p(x) = \boxed{(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) \text{ in } \mathbb{R}[x]}$.

---

2. For each p and $F[x]$ (note that these are the same as in problem 1), determine whether or not $F[x]$ modulo p is a field.

   (a) $p(x) = x^2 + 2$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.

   - As we proved, $F[x]$ modulo p is a field if and only if p is irreducible.
   - Thus, by the factorizations from problem 1, we see that it $\boxed{\text{is a field}}$ for $\mathbb{F}_5[x]$, $\mathbb{Q}[x]$, and $\mathbb{R}[x]$, and that it $\boxed{\text{is not a field}}$ for $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, and $\mathbb{C}[x]$.

   (b) $p(x) = x^3 + x^2 + 2$ in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{F}_7[x]$.

   - By the factorizations from problem 1, we see that it $\boxed{\text{is a field}}$ for $\mathbb{F}_3[x]$ and $\mathbb{F}_5[x]$, but $\boxed{\text{is not a field}}$ for $\mathbb{F}_7[x]$.

   (c) $p(x) = x^4 + 1$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{R}[x]$.

   - By the factorizations from problem 1, we see that it $\boxed{\text{is not a field}}$ for $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{R}[x]$.

---

3. Find the number of monic irreducible polynomials in $\mathbb{F}_2[x]$ and $\mathbb{F}_3[x]$ of degrees 4, 5, 6, 7, 8, 9, and 10.

- From our discussion, the number $f_p(n)$ of monic irreducible polynomials in $\mathbb{F}_p[x]$ can be computed using Mobius inversion. Explicitly, we obtain the following:

n	4	5	6	7	8	9	10
$f_p(n)$	$\frac{1}{4}(p^4-p^2)$	$\frac{1}{5}(p^5-p)$	$\frac{1}{6}(p^6-p^3-p^2+p)$	$\frac{1}{7}(p^7-p)$	$\frac{1}{8}(p^8-p^4)$	$\frac{1}{9}(p^9-p^3)$	$\frac{1}{10}(p^{10}-p^5-p^2+p)$
$f_2(n)$	3	6	9	18	30	56	99
$f_3(n)$	18	48	116	312	810	2184	5880

- Each sum for $f_p(n)$ includes the terms $p^{n/a}$ for each squarefree divisor a of n, with a sign $+$ or $-$ according to whether a has an even or odd number of prime factors.

---

4. For each integer m, either find a primitive root modulo m and the total number of primitive roots modulo m, or explain briefly why there are none:

(a) $m = 13$.

- Since 13 is prime, it has a primitive root. Testing 2 we see that the order of 2 divides 12, with $2^6 \equiv -1$ and $2^4 \equiv 3$, so in fact $\boxed{2}$ has order 12 hence is a primitive root.
- The number of primitive roots is $\varphi(\varphi(13)) = \varphi(12) = \boxed{4}$.

(b) $m = 13^3$.

- Since 13^3 is a prime power, it has a primitive root. We also have $2^{12} \equiv 80 \pmod{13}$, so 2 is also a primitive root modulo 13^2, hence modulo 13^d for any $d \geq 2$. Thus we may take $m = \boxed{2}$ as our primitive root modulo 13^3. The total number of primitive roots is $\varphi(\varphi(13^3)) = \varphi(12 \cdot 13^2) = \boxed{48 \cdot 13}$.

(c) $m = 32^{2026}$.

- Since $32^{2026} = 2^{10130}$ is not of the form 1, 2, p^n, or $2p^n$ for an odd prime p, there is $\boxed{\text{no primitive root}}$ here. (In such a case, of course the total number of primitive roots is 0.)

(d) $m = 33^{2026}$.

- Since $33^{2026} = 3^{2026}11^{2026}$ is not of the form 1, 2, p^n, or $2p^n$ for an odd prime p, there is $\boxed{\text{no primitive root}}$ here.

(e) $m = 5^{2026}$.

- First we find a primitive root modulo 5. It is easy to see that 2 is a primitive root since its powers are 2, 4, 3, 1.
- We also have $2^4 \equiv 16 \pmod{25}$, so 2 is also a primitive root modulo 25, hence modulo 5^d for any $d \geq 2$. Thus we may take $m = \boxed{2}$ as our primitive root modulo 5^{2026}.
- The total number of primitive roots is $\varphi(\varphi(5^{2026})) = \varphi(4 \cdot 5^{2025}) = \boxed{8 \cdot 5^{2024}}$.

(f) $m = 2 \cdot 5^{2026}$.

- By (e), 2 is a primitive root modulo 5^{2026}. Since 2 is even, it is not a primitive root modulo $2 \cdot 5^{2026}$: instead, we take $\boxed{2 + 5^{2026}}$ as our primitive root.
- (Alternatively, if we had started with 3 instead of 2, we would have seen that $\boxed{3}$ is also a primitive root modulo $2 \cdot 5^{2026}$.)
- The total number of primitive roots is $\varphi(\varphi(2 \cdot 5^{2026})) = \varphi(4 \cdot 5^{2025}) = \boxed{8 \cdot 5^{2024}}$.

---

5. Give an explicit construction for each of the following things, making sure to include full justification that your example has the required property:

   (a) A field having exactly 49 elements.
   - Since $49 = 7^2$ we can construct such a field as R/pR where $R = \mathbb{F}_7[x]$ and p is an irreducible polynomial of degree 2 in R.
   - There are many possibilities to choose from, but one option is $p(x) = x^2 + 1$, since $p(0) = 1$, $p(\pm 1) = 2$, $p(\pm 2) = 5$, and $p(\pm 3) = 3$: thus, p has no roots modulo 7, so it is irreducible.

   (b) An integral domain that is not a Euclidean domain.
   - There are many options but since we know Euclidean domains have unique factorization, we can use any of the rings $\mathbb{Z}[\sqrt{D}]$ that do not have unique factorization, such as $\mathbb{Z}[\sqrt{-5}]$. These rings are all integral domains, but cannot be Euclidean.

   (c) An integral domain R with exactly 125 elements in which $r^{125} = r$ for every $r \in R$.
   - By our generalization of Fermat's Little Theorem, if R is a field with 125 elements, then $r^{125} = r$ for every $r \in R$, and R will also be an integral domain since fields are domains.
   - Since $125 = 5^3$, we can construct such a field as $\mathbb{F}_5[x]$ modulo an irreducible polynomial $p(x)$ of degree 3.
   - One such polynomial is $p(x) = x^3 + x + 1$: since $p(0) = 1$, $p(1) = 3$, $p(2) = 1$, $p(3) = 1$, and $p(4) = 4$, it has no roots hence since it has degree 3 it is irreducible. Alternatively, we could use the polynomial $x^3 + x^2 + 2$ since in 1(b) we saw it was irreducible modulo 5.

---

6. Let $r \in \mathbb{Z}[\sqrt{D}]$ be nonzero and not a unit. Prove that r has at least one factorization as a product of irreducibles: namely, $r = r_1 \cdots r_k$ for some irreducible elements $r_1, \ldots, r_k$. [Hint: Induct on $|N(r)|$.]

- We show the result by (strong) induction on the absolute value of the norm $N(r)$. If $N(r) = 0$ then $r = 0$, while if $N(r) = \pm 1$ then r is a unit.
- For the base case we take $|N(r)| = 2$: then since the absolute value of its norm is prime, r is irreducible as proven in class.
- For the inductive step, suppose that $|N(r)| = n$ for $n \geq 3$. If r is irreducible we are done: otherwise we have $r = ab$ for some a, b with $1 < |N(a)|, |N(b)| < n$.
- By the inductive hypothesis, both a and b have factorizations as a product of irreducibles, so r does too.

---

7. Suppose p and q are distinct odd primes. The goal of this problem is to give another approach to show that there is no primitive root modulo pq.

   (a) Suppose a is a unit modulo pq, and that its order is d_p modulo p and d_q modulo q. Show that the order of a modulo pq divides $\operatorname{lcm}(d_p, d_q)$.
   - Let $l = \operatorname{lcm}(d_p, d_q)$. Then $a^l \equiv 1 \pmod{p}$ since the order d_p of a mod p divides the exponent l, and similarly $a^l \equiv 1 \pmod{q}$ since the order d_q of a mod q also divides l.
   - But now since p, q are relatively prime, by the Chinese Remainder Theorem $a^l \equiv 1 \pmod{p}$ and $a^l \equiv 1 \pmod{q}$ imply $a^l \equiv 1 \pmod{pq}$. Then by properties of order, the order of a modulo pq divides $l = \operatorname{lcm}(d_p, d_q)$, as required.

   (b) Show that the order of any unit modulo pq divides $\operatorname{lcm}(p-1, q-1)$ and that this lcm is at most $\frac{1}{2}\varphi(pq)$. Deduce that there is no primitive root modulo pq.
   - If a unit a has order d_p mod p and d_q mod q, then by Euler's theorem d_p divides $p-1$ and d_q divides $q-1$, and thus $\operatorname{lcm}(d_p, d_q)$ divides $\operatorname{lcm}(p-1, q-1)$.
   - Furthermore, since p and q are odd primes, $p-1$ and $q-1$ are both even, so their gcd is at least 2. Then $\operatorname{lcm}(p-1, q-1) = \dfrac{(p-1)(q-1)}{\gcd(p-1, q-1)} \leq \dfrac{(p-1)(q-1)}{2} = \frac{1}{2}\varphi(pq)$ as claimed.
   - Thus, since the order of any unit is at most $\frac{1}{2}\varphi(pq)$ there cannot be a unit of order $\varphi(pq)$, so there is no primitive root mod pq.

---

8. Let $n \geq 3$. We have seen that there are no primitive roots modulo 2^n for $n \geq 3$, so there exists no element of order $\varphi(2^n) = 2^{n-1}$. The goal of this problem is to show that there does exist an element of the next largest possible order, namely 2^{n-2}, modulo 2^n, and to show every unit is a power of this element up to a $\pm$ sign.

   (a) Prove that $5^{2^{n-3}} - 1$ is divisible by 2^{n-1} but not by 2^n for all integers $n \geq 3$. [Hint: Induct on n, using the factorization $5^{2a} - 1 = (5^a - 1)(5^a + 1)$, and count the factors of 2 in each term.]

   - Following the hint, we induct on n.
   - For the base case $n = 3$ we see $5^{2^0} - 1 = 5^1 - 1 = 4$ is divisible by 2^2 but not 2^3 as claimed.
   - For the inductive step suppose that $5^{2^{n-3}} - 1$ is divisible by 2^{n-1} but not by 2^n: we need to show that $5^{2^{n-2}} - 1$ is divisible by 2^n but not by 2^{n+1}.
   - Per the hint, we observe that $5^{2^{n-2}} - 1 = (5^{2^{n-3}} - 1)(5^{2^{n-3}} + 1)$. The first term is divisible by 2^{n-1} but not 2^n by the inductive hypothesis, while the second term is congruent to 2 modulo 4, hence is divisible by 2 but not 2^2.
   - Thus, the product $5^{2^{n-1}} - 1$ is divisible by 2^{n+1} but not 2^{n+2}, as required.

   (b) Deduce that $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ for $n \geq 3$.

   - By (a), we know that $5^{2^{n-3}} - 1$ is divisible by 2^{n-1}, so $5^{2^{n-3}} = 1 + 2^{n-1}a$ for some integer a.
   - Modulo 2^n we see that there are two possibilities: either $5^{2^{n-3}} \equiv 1 \pmod{2^n}$ for a even, or $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ for a odd.
   - But also by (a) we know $5^{2^{n-3}} - 1$ is not divisible by 2^n, so we must have $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$.

   (c) Show that 5 has order 2^{n-2} modulo 2^n for $n \geq 3$.

   - From (b) we know $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$. Squaring this yields $5^{2^{n-2}} \equiv (1 + 2^{n-1})^2 \equiv 1 + 2^n + 2^{2n-2} \equiv 1 \pmod{2^n}$.
   - Thus, the order of 5 divides 2^{n-2}. But the order does not divide 2^{n-3} since $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$ also by (b). Therefore, the order is exactly 2^{n-2}.

   (d) Show that there is no solution to $5^a \equiv -1 \pmod{2^n}$ for $n \geq 3$.

   - Suppose by way of contradiction that $5^a \equiv -1 \pmod{2^n}$. Squaring yields $5^{2a} \equiv 1 \pmod{2^n}$ so since 5 has order 2^{n-2} by (c), that means $2a$ is divisible by 2^{n-2} hence a is divisible by 2^{n-3}, say with $a = 2^{n-3}b$.
   - But then $5^a = (5^{2^{n-3}})^b \equiv (1 + 2^{n-1})^b \pmod{2^n}$ by (b), but the powers of $1 + 2^{n-1}$ alternate between $1 + 2^{n-1}$ and 1 modulo 2^n. This is a contradiction.

   (e) Show that every unit modulo 2^n is of the form 5^a or -5^a for some $1 \leq a \leq 2^{n-2}$. [Hint: Show that all these elements are distinct units.]

   - First, all the elements 5^a and -5^a for $1 \leq a \leq 2^{n-2}$ are units. They are also distinct: the powers of 5 are all distinct since 5 has order 2^{n-2}, and so their negatives are also distinct. Furthermore, if $5^a \equiv -5^b \pmod{2^n}$ then $5^{a-b} \equiv -1 \pmod{2^n}$ but there is no solution to this equation by part (d).
   - So these elements 5^a and -5^a represent $2 \cdot 2^{n-2} = 2^{n-1}$ distinct units. But there are only $\varphi(2^n) = 2^{n-1}$ units in total, so these are all of them.
