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

(a) $p(x) = x^2 + 2$ in $F_2[x], F_3[x], F_5[x], Q[x], R[x]$, and $C[x]$.
   - Since this polynomial has degree 2, we need only check whether it has any roots in the field.
   - In $F_2$ we have the obvious factorization $p(x) = x \cdot x$ in $F_2[x].$
   - In $F_3$, we see $p(1) = 0$ so we obtain a factorization $p(x) = (x + 1)(x + 2)$ in $F_3[x].$
   - In $F_5$, we see $p(0) = 2$, $p(1) = p(4) = 3$, and $p(2) = p(3) = 1$, so it has no roots hence is irreducible in $F_5[x].$
   - We can see that this polynomial has no rational roots because it does not even have any real roots, so it is irreducible in $Q[x]$ and irreducible in $R[x].$
   - But it does factor over as $p(x) = (x - i\sqrt{2})(x + i\sqrt{2})$ in $C[x].$

(b) $p(x) = x^3 + x^2 + 2$ in $F_3[x], F_5[x]$, and $F_7[x].$
   - Since this polynomial has degree 3, we need only check whether it has any roots in the field.
   - In $F_3$, we see $p(0) = 2$, $p(1) = 1$, and $p(2) = 2$, so it has no roots hence is irreducible in $F_3[x].$
   - In $F_5$, 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 irreducible in $F_5[x].$
   - In $F_7$, we see $p(2) = 0$ and so $x - 2 = x + 5$ will be a factor of $p(x)$. We obtain the factorization $p(x) = (x + 5)(x^2 + 3x + 6)$ in $F_7[x].$

(c) $p(x) = x^4 + 1$ in $F_2[x], F_3[x], F_5[x]$, and $R[x]$. [Hint: This polynomial factors in each case.]
   - It is easy to see that $p(x) = (x + 1)^4$ in $F_2[x].$
   - Note that $p(x)$ has no roots in $F_3, F_5$, or $R$, 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 $p(x) = (x^2 + x + 2)(x^2 - x + 2)$ in $F_3[x]$, $p(x) = (x^2 + 2)(x^2 + 3)$ in $F_5[x]$, and $p(x) = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$ in $R[x].$

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 $F_2[x], F_3[x], F_5[x], Q[x], R[x]$, and $C[x].$
   - 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 is a field for $F_3[x], Q[x]$, and $R[x]$, and that it is not a field for $F_2[x], F_5[x]$, and $C[x].$

(b) $p(x) = x^3 + x^2 + 2$ in $F_3[x], F_5[x]$, and $F_7[x].$
   - By the factorizations from problem 1, we see that it is a field for $F_3[x]$ and $F_5[x]$, but is not a field for $F_7[x].$

(c) $p(x) = x^4 + 1$ in $F_2[x], F_3[x], F_5[x]$, and $R[x].$
   - By the factorizations from problem 1, we see that it is not a field for $F_2[x], F_3[x], F_5[x]$, and $R[x].$
3. Solve the following problems:

(a) Find the number of monic irreducible polynomials in \( \mathbb{F}_3 \) of degrees 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:

<table>
<thead>
<tr>
<th>( n )</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( f_p(n) )</td>
<td>( \frac{1}{5}(p^5 - p) )</td>
<td>( \frac{1}{6}(p^6 - p^3 - p^2 + p) )</td>
<td>( \frac{1}{7}(p^7 - p) )</td>
<td>( \frac{1}{8}(p^8 - p^4) )</td>
<td>( \frac{1}{9}(p^9 - p^3) )</td>
<td>( \frac{1}{10}(p^{10} - p^5 - p^2 + p) )</td>
</tr>
<tr>
<td>( f_3(n) )</td>
<td>48</td>
<td>116</td>
<td>312</td>
<td>810</td>
<td>2184</td>
<td>5880</td>
</tr>
</tbody>
</table>

- 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.

(b) Give an explicit construction for a field having exactly 49 elements.

- From our discussion, 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 probably the easiest is \( p(x) = x^2 + 1 \), since we can see \( p(0) = 1 \), \( p(\pm 1) = 2 \), \( p(\pm 2) = 5 \), and \( p(\pm 3) = 3 \): thus, \( p \) has no roots modulo 7, so it is irreducible.

- Thus \( R/pR \), where \( R = \mathbb{F}_7[x] \) and \( p(x) = x^2 + 1 \), gives us a field of 49 elements.

(c) Find a primitive root modulo \( 17^{2020} \) and the total number of primitive roots modulo \( 17^{2020} \), or explain why there are none.

- Since \( 17^{2020} \) is an odd prime power, there is a primitive root.

- To find one, first we find a primitive root modulo 17. The order of any element mod 17 will divide \( \phi(17) = 16 \), so to see that a given element is a primitive root we need only check that its order does not divide 8. It is not hard to see that 2 has order 8 (since \( 2^4 \equiv -1 \pmod{17} \)) so 2 is not a primitive root.

- On the other hand, we can calculate \( 3^1 \equiv 3 \), \( 3^2 \equiv 9 \), \( 3^4 \equiv 81 \equiv -4 \), \( 3^8 \equiv (-4)^2 \equiv -1 \), and \( 3^{16} \equiv 1 \pmod{17} \), so 3 has order 16 hence is a primitive root modulo 17.

- Then we can also compute \( 3^{16} \equiv 171 \pmod{17^2} \), so by our results we see 3 is also a primitive root modulo \( 17^2 \), hence modulo \( 17^d \) for any value of \( d \geq 2 \). We conclude that \( [3] \) is a primitive root modulo \( 17^{2020} \).

- The total number of primitive roots is then \( \phi(\phi(17^{2020})) = \phi(16 \cdot 17^{2019}) = 8 \cdot 16 \cdot 17^{2018} \).

(d) Find a primitive root modulo \( 32^{2020} \) and the total number of primitive roots modulo \( 32^{2020} \), or explain why there are none.

- Since \( 32^{2020} = 2^{10100} \) is not of the form 1, 2, \( p^n \), or \( 2p^n \) for an odd prime \( p \), there is no primitive root here. (In such a case, of course the total number of primitive roots is 0.)

(e) Find a primitive root modulo \( 33^{2020} \) and the total number of primitive roots modulo \( 33^{2020} \), or explain why there are none.

- Since \( 33^{2020} = 3^{2020} \cdot 11^{2020} \) is not of the 1, 2, \( p^n \), or \( 2p^n \) for an odd prime \( p \), there is no primitive root here.

(f) Find a primitive root modulo \( 2 \cdot 5^{2020} \) and the total number of primitive roots modulo \( 2 \cdot 5^{2020} \), or explain why there are none.

- 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 \( d \geq 2 \).

- However, since 2 is even, it is not a primitive root modulo \( 2 \cdot 5^{2020} \): instead, we take \( [2 + 5^{2020}] \) as our primitive root. (Alternatively, if we had started with 3 instead of 2, we would have seen that \( [3] \) is also a primitive root modulo \( 2 \cdot 5^{2020} \).)

- The total number of primitive roots is \( \phi(\phi(2 \cdot 5^{2020})) = \phi(4 \cdot 5^{2019}) = 8 \cdot 5^{2018} \).
4. Let \( p(x) = x^{2020} \).

(a) Find the remainder when \( p(x) \) is divided by \( x - 4 \) in \( \mathbb{R}[x] \).
   - By the remainder theorem, the remainder upon dividing \( p(x) \) by \( x - r \) is \( p(r) \).
   - Thus, the remainder upon dividing \( p(x) \) by \( x - 4 \) is \( p(4) = 4^{2020} \).

(b) Find the remainder when \( p(x) \) is divided by \( x + 1 \) in \( \mathbb{R}[x] \).
   - By the same logic as in part (a), the remainder upon dividing \( p(x) \) by \( x + 1 \) is \( p(-1) = (-1)^{2020} = 1 \).

(c) Find the remainder when \( p(x) \) is divided by \( x^2 - 3x + 4 \) in \( \mathbb{R}[x] \). [Hint: Use the Chinese Remainder Theorem.]
   - The remainder \( r(x) \) satisfies the congruence \( r(x) \equiv p(x) \pmod{x^2 - 3x + 4} \).
   - To use the Chinese Remainder Theorem, observe that \( x^2 - 3x - 4 \) factors as \( (x+1)(x-4) \).
   - Thus, by the Chinese Remainder Theorem, the congruence \( r(x) \equiv p(x) \pmod{x^2 - 3x + 4} \) is equivalent to the two congruences \( r(x) \equiv p(x) \pmod{x+1} \) and \( r(x) \equiv p(x) \pmod{x-4} \).
   - The solution to the first congruence is \( r(x) = 1 + a \cdot (x+1) \) for some \( a \).
   - Plugging into the second congruence gives \( 1 + a \cdot (x+1) \equiv 4^{2020} \pmod{x-4} \), and since \( x+1 \equiv 5 \pmod{x-4} \) this yields \( 1 + 5a \equiv 4^{2020} \pmod{x-4} \) so we can take \( a = \frac{4^{2020} - 1}{5} \).
   - Then the desired remainder is \( r(x) = 1 + a \cdot (x+1) = \left[ 1 + \frac{4^{2020} - 1}{5} \right] (x+1) \).

5. If \( R/rR \) has finitely many units, then we can use the same order-calculation algorithm we used in \( \mathbb{Z}/m\mathbb{Z} \) to find the order of an arbitrary unit residue class \( \bar{s} \). Explicitly, \( \bar{s} \) has order \( n \) if and only if \( \bar{s}^n = \bar{1} \) and \( \bar{s}^{n/p} \neq \bar{1} \) for any prime \( p \) dividing \( n \).

(a) 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 \( \bar{a} + b \bar{x} \) 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.

(b) Find the orders of \( \bar{2}, \bar{x}, \) and \( \bar{x+1} \) in \( \mathbb{F}_5[x] \) modulo \( x^2 + 2 \). Are any of them primitive roots?
   - 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 2 has order 4.
   - Also, \( x^8 \equiv 1 \) but \( x^4 \equiv 4 \), so \( x \) has order 8.
   - Finally, \( x+1 \) has \( (x+1)^{24} \equiv 1 \), but \( (x+1)^8 \equiv x + 2 \) and \( (x+1)^{12} \equiv 4 \). Thus, \( x+1 \) has order 24, and is a primitive root.
6. The goal of this problem is to give some examples of $R/rR$ for $R = \mathbb{F}_5[x]$ where there do and do not exist primitive roots.

(a) In $\mathbb{F}_5[x]$ modulo the irreducible polynomial $x^2 + x + 1$, show that the element $\overline{x + 2}$ is a primitive root.

- There is a primitive root, because $\mathbb{F}_5[x]/(x^2 + x + 1)$ is a field with 25 elements, since $x^2 + x + 1$ is irreducible.
- A primitive root here has order 24, so by Euler’s theorem, $a$ will be a primitive root as long as $a^8 \not\equiv 1$ and $a^{12} \not\equiv 1 \pmod{x^2 + x + 1}$.
- We can then check using successive squaring that $(x+2)^8 \equiv 4x+4$ and $(x+2)^{12} \equiv 4 \pmod{x^2 + x + 1}$.
- Thus, $\overline{x + 2}$ is a primitive root.

(b) In $\mathbb{F}_5[x]$ modulo the reducible polynomial $x^2$, show that there are 20 units and that $\overline{x + 3}$ has order 20 (and thus is a primitive root).

- Note that this ring is not a field, because $x^2 = x \cdot x$ is not irreducible. In fact, the residue class $\overline{ax+b}$ will be a unit precisely when $ax+b$ is relatively prime to $x$.
- This will happen whenever $b \not\equiv 0 \pmod{5}$: thus, there are 5 choices for $a$ and 4 choices for $b$, for a total of $5 \cdot 4 = 20$ units, as claimed.
- A primitive root here has order 20, so by Euler’s theorem, $a$ will be a primitive root as long as $a^{10} \not\equiv 1$ and $a^4 \not\equiv 1 \pmod{x^2}$.
- We can then check using successive squaring that $(x+3)^{10} \equiv 4$ and $(x+3)^4 \equiv 3x + 1$.
- Thus, $\overline{x + 3}$ is a primitive root.

(c) In $\mathbb{F}_5[x]$ modulo the reducible polynomial $x^2 + x$, show that there are 16 units but that all of them have order dividing 4. Deduce that there are no primitive roots in this case. [Hint: Show that $u^4 \equiv 1 \pmod{x}$ and $u^4 \equiv 1 \pmod{x+1}$ for each possible unit, and then use the Chinese Remainder Theorem.]

- Note that this ring is not a field, because $x^2 = x \cdot (x+1)$ is not irreducible. In fact, the residue class $\overline{ax+b}$ will be a unit precisely when $ax+b$ is relatively prime to $x$ and to $x+1$.
- The polynomials not relatively prime to $x$ are 0, $x$, $2x$, $3x$, $4x$ while the polynomials not relatively prime to $x+1$ are 0, $x+1$, $2x+2$, $3x+3$, $4x+4$. In total, there are 9 polynomials not relatively prime to $x$ or $x+1$ (note 0 is on both lists), so there are 25 - 9 = 16 polynomials that are units.
- For the second part, per the hint, we can use the Chinese Remainder Theorem: notice that for each unit, we have $u^4 \equiv 1 \pmod{x}$, since $\mathbb{F}_5[x]$ modulo $x$ is simply the constant polynomials (and every unit has order dividing 4 by Euler’s theorem), and likewise $u^4 \equiv 1 \pmod{x+1}$.
- Then by the Chinese Remainder Theorem, since $u^4 \equiv 1 \pmod{x}$ and $u^4 \equiv 1 \pmod{x+1}$, we see that $u^4 \equiv 1 \pmod{x(x+1)}$. This implies that every unit has order dividing 4. In particular, there is no unit of order 16, so there is no primitive root.

(d) Based on the results of parts (a)-(c), and in analogy with the case for $\mathbb{Z}/m\mathbb{Z}$, can you conjecture when there will be a primitive root in $R/rR$ when $R = \mathbb{F}_5[x]$?

- We know that there is a primitive root in $\mathbb{Z}/m\mathbb{Z}$ when $m = 1, 2, p^n$, or $2p^n$ where $p$ is an odd prime.
- If we ignore the business about 2, this suggests that $R/rR$ will have a primitive root whenever $r$ is a prime power (i.e., a power of an irreducible polynomial).
- This conjecture agrees with all of our known information: we have already shown that $R/rR$ will have a primitive root when $r$ is irreducible. Furthermore, in the two non-irreducible cases above, there was a primitive root in $R/rR$ when $r = x^2$, which is a power of an irreducible polynomial, but not when $r = x^2 + x$, which is not a power of an irreducible polynomial.
- Remark: This conjecture is in fact true for $R = \mathbb{F}_p[x]$ whenever $p$ is an odd prime, and it can be proven using an argument similar to the one we gave for $\mathbb{Z}/m\mathbb{Z}$, utilizing the Chinese Remainder Theorem. (When $p = 2$ the situation is more complicated.)