1. Set \( f(x) = 3x^3 + 5x^2 + 6x \), \( g(x) = 3x^4 + 5x^3 + x^2 + 3x + 2 \), both in \( \mathbb{Z}_7[x] \). Use the extended Euclidean algorithm to find \( \gcd(f, g) \) and to find polynomials \( s(x), t(x) \) such that \( \gcd(f, g) = f(x)s(x) + g(x)t(x) \).

We perform the division algorithm repeatedly to get:
\[
3x^4 + 5x^3 + x^2 + 3x + 2 = (3x^3 + 5x^2 + 6x) + (2x^2 + 3x + 2)
\]
\[
3x^3 + 5x^2 + 6x = (5x + 2)(2x^2 + 3x + 2) + (4x + 3)
\]
\[
2x^2 + 3x + 2 = (4x + 3)(4x + 3) + 0
\]
Hence \( \gcd(f, g) \) is the monic multiple of \( 4x + 3 \), namely \( 2(4x + 3) = x + 6 \). We now back-substitute twice, simplify, and double both sides, to get:
\[
4x + 3 = (3x^3 + 5x^2 + 6x) + (2x + 5)(2x^2 + 3x + 2)
\]
\[
4x + 3 = (3x^3 + 5x^2 + 6x) + (2x + 5)((3x^3 + 5x^2 + x^2 + 3x + 2) + (-x)(3x^3 + 5x^2 + 6x))
\]
\[
4x + 3 = (1 + (2x + 5)(-x))(3x^3 + 5x^2 + 6x) + (2x + 5)(3x^4 + 5x^3 + x^2 + 3x + 2)
\]
\[
4x + 3 = (5x^2 + 2x + 1)(3x^3 + 5x^2 + 6x) + (2x + 5)(3x^4 + 5x^3 + x^2 + 3x + 2)
\]
\[
x + 6 = (3x^2 + 4x + 2)(3x^3 + 5x^2 + 6x) + (4x + 3)(3x^4 + 5x^3 + x^2 + 3x + 2)
\]
Hence we want \( s(x) = 3x^2 + 4x + 2 \) and \( t(x) = 4x + 3 \).

2. Factor \( f(x) = x^4 + x^3 + 6x^2 - 14x + 16 \in \mathbb{Q}[x] \) into irreducibles.

We calculate \( f(x + 1) = x^4 + 5x^3 + 15x^2 + 5x + 10 \). Note that \( p = 5 \) divides each coefficient except the leading one, and \( p^2 = 25 \) does not divide the constant. Hence by Eisenstein’s criterion \( f(x + 1) \) is irreducible. By the translation trick, \( f(x) \) is irreducible.

3. Let \( F \) be a field. We define the “derivative” operator \( D : F[x] \to F[x] \) via
\[
D(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) = na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \cdots + 1a_1.
\]
This operator satisfies, for all \( f, g \in F[x] \) and for all \( c \in F \):
(a) \( D(f + g) = D(f) + D(g) \); (b) \( D(cf) = cD(f) \); (c) \( D(fg) = fD(g) + D(f)g \)
Suppose \( f, g \in F[x] \) and \( f^2 \mid g \). Prove that \( f \mid D(g) \).

Because \( f^2 \mid g \) there is some polynomial \( h \in F[x] \) such that \( g(x) = f(x)f(x)h(x) \). We apply property (c) twice to get \( D(g) = D(f(f(h))) = fD(f(h)) + D(f)f(h) = f(fD(h) + D(f)h) + D(f)fh = f(fD(h) + D(f)h + D(f)h) = f(fD(h) + 2D(f)h) \). Since \( fD(h) + 2D(f)h \in F[x] \), we have \( f \mid D(g) \), as desired.

4. Set \( f(x) = x + 2x^2, g(x) = x + 4x^2 \), both in \( \mathbb{Z}_5[x] \). Prove that \( fg \) and \( gf \).

All solutions involve at least some trial and error.
Direct Solution: \( (x + 2x^2)(1 + 2x + 4x^2) = x + 4x^2 \) and \( (x + 4x^2)(1 + 6x) = x + 2x^2 \).
Alternate Solution: \( (x + 2x^2)(1 + 2x + 4x^2) = x + 4x^2. \) But \( 1 + 2x + 4x^2 \) is a unit, since \( (1 + 2x + 4x^2)(1 + 6x) = 1 \), so in fact \( f, g \) are associates.

5. Set \( f(x) = x^n + x^{n-1} \in F[x] \). Carefully determine all divisors of \( f(x) \).

Polynomial \( f \) splits into \( n \) linear factors, namely \( x^{n-1}(x+1) \). Because \( F[x] \) has unique factorization, any factor must be an associate of a product of some subset of those \( n \) linear factors. Hence, the factors are precisely \( ax^i(x+1)^j \), where \( a \) is any nonzero element of \( F \), \( i \) satisfies \( 0 \leq i \leq n - 1 \), and \( j \) satisfies \( 0 \leq j \leq 1 \).

6. For ring \( R, a \in R \), and \( n \in \mathbb{N} \), we say \( a \) has additive order \( n \) if \( a + a + \cdots + a = 0_R \), and for \( m < n \) we have \( a + a + \cdots + a \neq 0_R \). We write this \( ord_R(a) = n \). Suppose every element of \( R \) has an order (not necessarily the same one). Prove that every element of \( R[x] \) has an order.

Let \( f(x) = a_n x^n + \cdots + a_1 x + a_0 \), an arbitrary element of \( R[x] \). Set \( t = \prod_{i=0}^{n} ord_R(a_i) \). We calculate \( f + f + \cdots + f = (a_n + \cdots + a_n)x^n + \cdots + (a_1 + \cdots + a_1)x + (a_0 + \cdots + a_0) = 0 \), since \( t \) is a multiple of the orders of each coefficient.

Hence \( f \) has some order, and that order is at most \( t \). [If we choose \( t \) as the lcm of the orders of the coefficients, instead of their product, then we get the order of \( f \) exactly (instead of a bound).]