1. Consider the ring \( \mathbb{Z}_4[x] \). Prove that \( x + 2x^k \) divides \( x^3 \), for every \( k \in \mathbb{N} \).

We have \( (x + 2x^k)(x^2 + 2x^{k+1}) = x^3 + 4x^{k+2} + 4x^{2k+1} = x^3 \), in \( \mathbb{Z}_4[x] \). This is really bad for factoring.

2. Find a monic associate of \((1 + 2i)x^3 + x - 1\) in \( \mathbb{C}[x] \).

Since \( \mathbb{C} \) is a field, every nonzero element has a reciprocal. We calculate \( \frac{1}{1+2i} = \frac{1-2i}{(1+2i)(1-2i)} = \frac{1-2i}{5} \), so we multiply by this to get \( x^3 + \frac{1-2i}{5}x + \frac{2i-1}{5} \).

3. For each \( a \in \mathbb{Z}_7 \), factor \( x^2 + ax + 1 \) into irreducibles in \( \mathbb{Z}_7[x] \).

\( x^2 + ax + 1 \) is reducible exactly when it has a root; so for each \( a \) we must check each value of \( x \in \{0, 1, \ldots, 6\} \). This is at most 49 calculations. Alternatively, we can try to combine linear terms in every possible way; however, we must be careful. We have \( x^2 + x + 1 = (x + 3)(x + 5) \), \( x^2 + 2x + 1 = (x + 1)^2 \), \( x^2 + 5x + 1 = (x + 6)^2 \), \( x^2 + 6x + 1 = (x + 2)(x + 4) \). The others, namely \( x^2 + 1, x^2 + 3x + 1, x^2 + 4x + 1 \), are irreducible.

4. For each \( a, b \in \mathbb{Z}_3 \), factor \( x^2 + ax + b \) into irreducibles in \( \mathbb{Z}_3[x] \).

This is similar to the previous problem. We have \( x^2 = (x)^2 \), \( x^2 + 2 = (x + 1)(x + 2) \), \( x^2 + x = x(x + 1) \), \( x^2 + x + 1 = (x + 2)^2 \), \( x^2 + 2x = x(x + 2) \), \( x^2 + 2x + 1 = (x + 1)^2 \). The others, namely \( x^2 + 1, x^2 + x + 2, x^2 + 2x + 2 \), are all irreducible.

5. Find some \( f(x) \in \mathbb{Z}_5[x] \) that is monic, of degree 4, reducible, but with no roots.

The only such \( f(x) \) are the product of two monic degree-2 irreducible polynomials. There are ten of them: \( x^2 + 2, x^2 + 3, x^2 + x + 1, x^2 + x + 2, x^2 + 2x + 3, x^2 + 2x + 4, x^2 + 3x + 3, x^2 + 3x + 4, x^2 + 4x + 1, x^2 + 4x + 2 \). There are \( \binom{10}{2} = 45 \) ways of picking two different ones, such as \( f(x) = (x^2 + 2)(x^2 + x + 1) \), and 10 ways of picking the square of one, such as \( f(x) = (x^2 + 2)^2 \). Hence there are 45 + 10 = 55 answers to this question.

6. Factor \( x^7 - x \) as a product of irreducibles in \( \mathbb{Z}_7[x] \).

By Fermat’s Little Theorem, \( x^7 \equiv x \pmod{7} \), for all integer \( x \). Hence each element of \( \mathbb{Z}_7 \) is a root, so \( f(x) = x(x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6) \) divides \( x^7 - x \). Since both polynomials are monic and of degree 7, in fact \( f(x) = x^7 - x \).

7. Let \( a, b \in \mathbb{N} \) be distinct, and each greater than 1. Set \( n = ab \). Find a quadratic polynomial in \( \mathbb{Z}_n[x] \) with at least three distinct roots.

Consider \( f(x) = (x - a)(x - b) \). We have \( f(a) = f(b) = 0 \) by construction, and also \( f(0) = (-a)(-b) = ab = n = 0 \). Hence we have three roots, now we show that they are distinct. \( 0 \neq a \) because \( 1 < a < n \). Similarly, \( 0 \neq b \). \( a \neq b \) by hypothesis, so \( \{0, a, b\} \) are distinct.
8. Let $a, b, c \in F$ with $a \neq 0$. Set $f(x) = ax^2 + bx + c$. Suppose that $r, s \in F$ are distinct roots of $f(x)$. Prove that $r + s = -a^{-1}b$ and that $rs = a^{-1}c$.

Set $g(x) = (x - r)(x - s)$ By the Factor Theorem twice, we have $g(x)|f(x)$; i.e. there is some $h(x) \in F[x]$ with $f(x) = g(x)h(x)$. Since $2 = \deg(f) = \deg(g)$, and $F$ is a field, we must have $0 = \deg(h)$. But also $f(x)$ has leading coefficient $a$, while $g(x)$ is monic. Hence $f(x) = ag(x) = a(x^2 - (r+s)x + rs) = ax^2 - (r+s)a + rsa$. Equating coefficients, we see that $b = -(r+s)a$ and $c = rsa$. Multiplying by $-a^{-1}$ and $a^{-1}$ respectively gives the desired equalities.

9. Let $a \in F$ and define $\tau_a : F[x] \to F$ via $\tau_a : f(x) \mapsto f(a)$. Prove that $\tau_a$ is a surjective (ring) homomorphism, but not an isomorphism.

First, let $f(x), g(x) \in F[x]$. We have $\tau_a(f(x) + g(x)) = \tau_a((f + g)(x)) = (f + g)(a) = f(a) + g(a) = \tau_a(f(x)) + \tau_a(g(x))$. Also, $\tau_a(f(x)g(x)) = \tau_a((fg)(x)) = (fg)(a) = f(a)g(a) = \tau_a(f(x))\tau_a(g(x))$. Hence $\tau_a$ is a ring homomorphism. Let $b \in F$. Setting $f(x) = b$, the constant polynomial, we have $\tau_a(f(x)) = b$. Hence $\tau_a$ is surjective. Lastly, we have $\tau_a(x - a) = \tau_a((x - a)^2) = 0$, but $(x - a) \neq (x - a)^2$, so $\tau_a$ is not injective.

10. Set $f(x) = x^6 + 2x^4 + 3x^3 + 1$. Find some prime $p$ such that $x - 2$ is a divisor of $f(x)$ in $\mathbb{Z}_p[x]$. Then factor $f(x)$ into irreducibles in $\mathbb{Z}_p[x]$.

If $x - 2$ is a divisor, then 2 is a root. We calculate $f(2) = 121 = 11^2$. Hence $121 \equiv 0 \pmod{p}$. The only possible $p$ is $p = 11$. Checking each of $\{0, 1, \ldots, 10\}$, we see that 2 is the only root. We now use trial and error (or computing help) to determine that $f(x) = (x - 2)(x^2 + 3x - 1)(x^3 - x^2 - x + 6)$. Since there are no other roots, all three terms are irreducible.