1. Let $a(x) = (x-2)^2$ and $b(x) = (x-3)^2$ in $\mathbb{R}[x]$.

(a) Find polynomials $u(x)$ and $v(x)$ in $\mathbb{R}[x]$ so that $a(x)u(x) + b(x)v(x) = 1$.

(b) Find reconstruction polynomials $c_1(x)$, $c_2(x) \in \mathbb{R}[x]$ so that given any $f_1(x)$ and $f_2(x)$ in $\mathbb{R}[x]$ the polynomial $f(x) = c_1(x)f_1(x) + c_2(x)f_2(x)$ satisfies

$$f(x) \equiv f_1(x) \pmod{a(x)} \text{ and}$$
$$f(x) \equiv f_2(x) \pmod{b(x)}.$$

Your solution should include the polynomials $c_1(x)$ and $c_2(x)$, and an explanation why they have the properties above.

(c) For any polynomial $f(x) \in \mathbb{R}[x]$ the numbers $f(2)$, $f(3)$, $f'(2)$, and $f'(3)$, determine the polynomial $f(x)$ uniquely up to multiples of $m(x) = (x-2)^2(x-3)^2$, i.e., mod $m(x)$. The remainder when dividing by $m(x)$ is a polynomial of degree ≤ 3, and so can be written in the form $c_0 + c_1x + c_2x^2 + c_3x^3$.

Find the formulas for c_0, c_1, c_2, and c_3 in the remainder above in terms of the numbers $a_0 = f(2)$, $a_1 = f'(2)$, $b_0 = f(3)$, and $b_1 = f'(3)$.

2. Let p be a prime number, and $F = \mathbb{Z}/p\mathbb{Z}$. Is it possible that there are irreducible polynomials of every degree d in $F[x]$? Let's at least check some small cases:

(a) How many monic polynomials of degree exactly d are there in $F[x]$?

(b) How many reducible monic polynomials are there of degree 2 in $F[x]$?
(HINT: Unique Factorization).

(c) How many monic irreducible polynomials are there of degree 2 in $F[x]$?

(d) How many monic irreducible polynomials are there of degree 3 in $F[x]$?

3. Suppose that F is a field, and that $m(x) \in F[x]$ is a nonzero polynomial. To make notation easier, let R be the ring $R = F[x]/m(x)F[x]$.

(a) If $m(x)$ is reducible, show that R is not a domain.

(b) If $m(x)$ is irreducible, show that R is a domain.

(c) Suppose that $m(x)$ is irreducible, and $a \in R$ a nonzero element. Explain why the map $f\colon R \longrightarrow R$ given by multiplication by a (i.e. $f(b) = ab$ for any $b \in R$) is injective. (HINT: First check that the map is linear).

(d) If $m(x)$ is irreducible, show that for any nonzero $a \in R$ the multiplication by a map f defined above is also surjective.

POSSIBLE METHOD #1: Isn't R some kind of vector space over F?

POSSIBLE METHOD #2: Explicitly (using $\gcd(a(x), m(x))$, where $a(x)$ is some element in the equivalence class a) show how to get any given element b in the image.

(e) Use part (d) to show that if $m(x)$ is irreducible then R is a field.

4. Let $F = \mathbb{Z}/2\mathbb{Z}$.

(a) Show that $m(x) = x^3 + x + \bar{1}$ is an irreducible polynomial in $F[x]$.

(b) Let $R = F[x]/m(x)F[x]$. By part (a) and question 3 above, R is a field. Write out the multiplication table for this field (you can omit multiplication by zero).