§4.1

4.1.1. Perform the indicated operation and simply your answer. (a)

\[
(3x^4 + 2x^3 - 4x^2 + x - 4) + (4x^3 + x^2 + 4x + 3) = 3x^4 + 6x^3 - 3x^2 + 5x - 1 \quad \text{in } \mathbb{Z}_5
\]

(b)

\[
(x + 1)^3 = x^3 + 3x^2 + 3x + 1 = x^3 + 1 \quad \text{in } \mathbb{Z}_3
\]

(c) and (d) are similar.

4.1.2. Which of the following subsets of \( \mathbb{R}[x] \) are subrings of \( \mathbb{R}[x] \)? Justify your answer.

(a) \( S = \{ \text{All polynomials with constant term } 0_R \} \).

This is a subring since

(i) This subset contains \( 0_{R[x]} = 0_R \).

(ii) This subset is closed under addition.

(iii) This subset is closed under multiplication.

(iv) If \( f(x) \in S, -f(x) \in S \); so for every \( f(x) \in S \) there is a solution of the equation \( f(x) + X = 0_R \) in \( S \).

(b) \( S = \{ \text{All polynomials of degree } 2 \} \).

Not a subring since it does not contain \( 0_{R[x]} = 0 \).

(c) \( S = \{ \text{All polynomials of degree } \leq k \in \mathbb{N}, \text{ where } 0 < k \} \).

Not a subring since it is not closed under multiplication; if \( f(x) \in S \) is a polynomial of degree \( k \), then \( f(x)f(x) \) has degree \( 2k \) and so does not lie in \( S \).

(d) \( S = \{ \text{All polynomials in which odd powers of } x \text{ have zero coefficients} \} \).

This is a subring. Properties analogous to (i)-(iv) in (a) are easily verified; perhaps the only non-trivial part is the verification that \( S \) is closed under multiplication. If \( f(x), g(x) \in S \) and

\[
f(x) = a_{2n}x^{2n} + a_{2n-2}x^{2n-2} + \cdots + a_2x^2 + a_0 \\
g(x) = b_{2m}x^{2m} + b_{2m-2}x^{2m-2} + \cdots + b_2x^2 + b_0
\]

then

\[
f(x)g(x) = a_{2n}b_{2m}x^{2n+2m} + (a_{2n}b_{2m-2} + a_{2n-2}b_2) x^{2n+2m-2} + \cdots + (a_2b_0 + a_0b_2) x^2 + a_0b_0
\]

also belongs to \( S \).

(e) \( S = \{ \text{All polynomials in which even powers of } x \text{ have zero coefficients} \} \).

This is not subring since it is not closed under multiplication. (For example, the product of two polynomials of degree 1 is a polynomial of degree 2.)
4.1.3. List all polynomials of degree 3 in \( \mathbb{Z}_2[x] \).

\[
x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1
\]

4.1.4. Let \( F \) be a field and let \( f(x) \) be a non-zero polynomial in \( F[x] \). Show that \( f(x) \) is a unit in \( F[x] \) if and only if \( \deg f(x) = 0 \).

\( \Leftarrow \) If \( \deg f(x) = 0 \), then \( f(x) = c \), a nonzero element of the field \( F \). Since \( F \) is a field and \( c \neq 0_F \), \( c^{-1} \) exists, so \( f(x) \) is a unit.

\( \Rightarrow \) Certainly, if \( f(x) \) is a unit, \( f(x) \neq 0 \). Suppose \( \deg f(x) \neq 0 \). Then \( \deg f(x) \geq 1 \). Let \( g(x) \) be the nonzero element of \( F[x] \) such that \( f(x)g(x) = 1_F[x] = 1_F \). Then

\[
0 = \deg(1_F) = \deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).
\]

Since \( \deg(f(x)) \geq 1 \), \( \deg(g(x)) \leq -1 \). But there is no elements of negative degree in \( F[x] \). Hence, \( g(x) \) does not exist; hence \( f(x) \) is not a unit.

§4.2

4.2.1. If \( a, b \in F \) and \( a \neq b \), show that \( x + a \) and \( x + b \) are relatively prime in \( F[x] \).

Suppose \( x + a \) and \( x + b \) are not relatively prime. Then \( \text{GCD}(x + a, x + b) \neq 1_F \). Since \( 1_F \) is the only monic polynomial of degree 0, and the \( \text{GCD} \) of \( x + a \) and \( x + b \) must be a monic polynomial of degree less than or equal to that of \( x + a \) and \( x + b \), \( \text{GCD}(x + a, x + b) \) must be a monic polynomial \( d(x) \) of degree 1. But then

\[
x + a = cd(x) \quad \text{and} \quad x + b = c'd(x).
\]

Since \( x + a \), \( x + b \) and \( d(x) \) are all monic, we must have \( c = c' = 1 \). But then

\[
x + a = x + b \quad \Rightarrow \quad a = b.
\]

We have thus shown that if \( \text{GCD}(x + a, x + b) \neq 1_F \), then \( a = b \). The contrapositive of this statement is that if \( a \neq b \), then \( \text{GCD}(x + a, x + b) = 1 \).

4.2.2. Let \( f(x), g(x) \in F[x] \). If \( f(x) \mid g(x) \) and \( g(x) \mid f(x) \), show that \( f(x) = cg(x) \) for some non-zero \( c \in F \).

Well, \( f(x) \mid g(x) \) and \( g(x) \mid f(x) \) imply, respectively, that

\[
g(x) = q(x)f(x),
\]

\[
f(x) = s(x)g(x),
\]

with neither \( q(x) \) or \( s(x) \) equal to \( 0_F \). Calculating the degrees of both sides of these two equations (applying Theorem 4.1 to calculate the right-hand sides), we find

\[
\deg(g(x)) = \deg(q(x)) + \deg(f(x)) \quad \Rightarrow \quad \deg(g(x)) \leq \deg(f(x))
\]

\[
\deg(f(x)) = \deg(s(x)) + \deg(g(x)) \quad \Rightarrow \quad \deg(f(x)) \leq \deg(g(x)).
\]

The two inequalities on the right imply that \( \deg(f(x)) = \deg(g(x)) \), and so we can infer that \( \deg(q(x)) = \deg(s(x)) = 0 \). Thus, \( q(x), s(x) \in F \). Set \( c = s(x) \in F \). We then have \( g(x) = cf(x) \).

(b) If \( f(x) \) and \( g(x) \) are monic and \( f(x) \mid g(x) \) and \( g(x) \mid f(x) \), show that \( f(x) = g(x) \).

From part (a) we know \( f(x) \) and \( g(x) \) have the same degree. Suppose \( \deg(f(x)) = \deg(g(x)) = n \). Since \( f(x) \) and \( g(x) \) are also monic, we can set

\[
f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0
\]

\[
g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0.
\]
But part (a) also tells us that \( g(x) = cf(x) \); so we must have
\[
\begin{align*}
1 &= c \\
0 &= cb_{n-1} \\
&\vdots \\
0 &= cb_1 \\
0 &= cb_0 .
\end{align*}
\]
Thus, \( a_i = b_i, \ i = 0, 1, \ldots, n-1 \), hence \( f(x) = g(x) \).

4.2.3. Let \( f(x) \in F[x] \) and assume \( f(x) \mid g(x) \) for every nonconstant \( g(x) \in F[x] \). Show that \( f(x) \) is a constant polynomial.

If \( f(x) \mid g(x) \), then any associate of \( f(x) \) divides \( g(x) \). Since every nonzero polynomial has a monic associate, we can without loss of generality take \( f(x) \) to be monic.

Thus, suppose \( f(x) \) is a monic polynomial that is a common divisor of all nonconstant polynomials. It must be in particular a common divisor of the monic polynomials of degree 1. But in order to be a divisor of a polynomial of degree 1, \( f(x) \) must have degree less than or equal to 1.

Suppose \( f(x) \) has degree 1. Then \( f(x) \) would have the form \( f(x) = x + a \). Let \( g(x) = x + b \) with \( a \neq b \). In Problem 4.2.3, it is shown if \( x + a \neq x + b \), then \( \text{GCD}(x + a, x + b) = 1 \) Thus, \( f(x) \) cannot be a divisor of \( g(x) \). Thus, \( f(x) \) cannot be of degree 1.

Suppose \( f(x) \) has degree 0. Then \( f(x) \) is a constant polynomial and so divides every nonconstant polynomial.

4.2.4. Let \( f(x), g(x) \in F[x] \), not both zero, and let \( d(x) = \text{GCD}(f(x), g(x)) \). If \( h(x) \) is a common divisor of \( f(x) \) and \( g(x) \) of highest possible degree, then prove that \( h(x) = cd(x) \) for some nonzero \( c \in F \).

Since by definition \( d(x) \) is the monic polynomial that is a common divisor of \( f(x) \) and \( g(x) \) of highest possible degree. Suppose \( h(x) \) is a common divisor of \( f(x) \) and \( g(x) \) of highest possible degree. Say \( \deg(h(x)) = n \), so that
\[
\begin{align*}
h(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\
&\quad, \quad a_n \neq 0_F .
\end{align*}
\]
Then
\[
\hat{h}(x) = a_n^{-1} h(x) = x^n + a_{n-1} x^{n-1} + \cdots + a^{-1}_1 x + a_0
\]
is a monic polynomial also of degree \( n \) that divides \( f(x) \) and \( g(x) \): for
\[
\begin{align*}
h(x) \mid f(x) &\Rightarrow f(x) = \hat{r}(x) h(x) = (r(x) a_n) (a_n^{-1} h(x)) \Rightarrow \hat{h}(x) \mid f(x) , \\
h(x) \mid g(x) &\Rightarrow g(x) = q(x) h(x) = (q(x) a_n) (a_n^{-1} h(x)) \Rightarrow \hat{h}(x) \mid g(x) .
\end{align*}
\]
But by Theorem 4.4, the GCD of \( f(x) \) and \( g(x) \) is unique monic polynomial that is a common divisor of \( f(x) \) and \( g(x) \) with highest possible degree. Hence
\[
d(x) = \hat{h}(x) = a_n^{-1} h(x) \]
or
\[
h(x) = a_n d(x) .
\]

4.2.5. If \( f(x) \) is relatively prime to \( 0_F \), what can be said about \( f(x) \).

If \( f(x) \) is relatively prime to \( 0_F \), then \( \text{GCD}(f, 0_F) = 1_F \). Now the \( \text{GCD} \) of \( f \) and \( 0_F \) must be a common divisor of \( f \) and \( 0_F \). Since every polynomial is a divisor of \( 0_F \) (for \( 0_F = 0_F \cdot g(x) \) for all \( g(x) \in F[x] \)), the set of common divisors of \( f \) and \( 0_F \) is simply the set of divisors of \( f \). But if \( f \) is certainly divides \( f \), and if \( g \) is any other polynomial that divides \( f \) then \( \deg(g) \leq \deg(f) \). Therefore, the degree of the greatest
divisor of \( f \) is the degree of \( f \). Therefore, the degree of the greatest common divisor of \( f \) and \( 0_F \) is equal to the degree of \( f \). Since by hypothesis, \( \text{GCD}(f, 0_F) = 1 \), we must have \( \deg(f) = 0 \). Thus, \( f \) must be a constant.

4.2.6. Let \( f(x), g(x), h(x) \in F[x] \), with \( f(x) \) and \( g(x) \) relatively prime. If \( f(x) \mid h(x) \) and \( g(x) \mid h(x) \), prove that \( f(x)g(x) \mid h(x) \).

Since \( f(x) \) and \( g(x) \) are relatively prime, \( \text{GCD}(f(x), g(x)) = 1_F \). By Theorem 4.4, there then exist polynomials \( u(x) \) and \( v(x) \) such that

\[
1_F = f(x)u(x) + g(x)v(x)
\]

Multiplying both sides of this equation by \( h(x) \) yields

\[
h(x) = h(x)f(x)u(x) + h(x)g(x)v(x)
\]

Now if \( h(x) \) is divisible by both \( f(x) \) and \( g(x) \) we may find polynomials \( r(x) \) and \( s(x) \) such that

\[
h(x) = r(x)f(x) = s(x)g(x)
\]

Inserting these expressions for \( h(x) \) into (3) yields

\[
h(x) = s(x)g(x)f(x)u(x) + r(x)f(x)g(x)v(x) = (s(x)u(x) + r(x)v(x))f(x)g(x)
\]

Thus, \( f(x)g(x) \mid h(x) \).

4.2.7. Let \( f(x), g(x), h(x) \in F[x] \), with \( f(x) \) and \( g(x) \) relatively prime. If \( h(x) \mid f(x) \), prove that \( h(x) \) and \( g(x) \) are relatively prime.

Set

\[
d(x) = \text{GCD}(h(x), g(x))
\]

By definition \( d(x) \mid h(x) \) and \( d(x) \mid g(x) \) and so we can write

\[
h(x) = q(x)d(x), \quad g(x) = r(x)d(x)
\]

If \( h(x) \mid f(x) \), then we can write \( f(x) = s(x)h(x) \), for some nonzero \( s(x) \in F[x] \). But this together with (4) implies

\[
f(x) = s(x)g(x)d(x)
\]

Now since \( f(x) \) and \( g(x) \) are relatively prime

\[
1_F = \text{GCD}(f(x), g(x)),
\]

so by Theorem 4.4, there exists polynomials \( u(x) \) and \( v(x) \) such that

\[
1_F = u(x)f(x) + v(X)g(x) = (u(x)s(x)q(x) + v(x)r(x))d(x)
\]

This implies that \( 1_F \) is divisible by \( d(x) \), a monic polynomial of degree greater than or equal to 0. This is impossible, unless \( d(x) \) is a monic polynomial of degree 0; i.e., unless \( d(x) = 1_F \).

4.2.8. Let \( f(x), g(x), h(x) \in F[x] \), with \( f(x) \) and \( g(x) \) relatively prime. Prove that the \( \text{GCD} \) of \( f(x)h(x) \) and \( g(x) \) is the same as the \( \text{GCD} \) of \( h(x) \) and \( g(x) \).

Since \( f(x) \) and \( g(x) \) are relatively prime, there exist polynomials \( u(x) \) and \( v(x) \) such that

\[
1_F = u(x)f(x) + v(x)g(x)
\]

Multiplying both sides of this equation by \( h(x) \) yields

\[
h(x) = u(x)h(x)f(x) + h(x)v(x)g(x)
\]

Suppose \( c(x) \) is a common divisor of \( h(x)f(x) \) and \( g(x) \). Then we can write

\[
h(x)f(x) = q(x)c(x), \quad g(x) = r(x)c(x)
\]
and (5) can be rewritten as
\[ h(x) = (u(x)q(x) + h(x)v(x)r(x))c(x) \]
so \( c(x) \mid h(x) \). Thus, if \( c(x) \) is a common divisor of \( f(x)h(x) \) and \( g(x) \) then it is a common divisor of \( h(x) \) and \( g(x) \).

Alternatively, if \( c(x) \) is a common divisor of \( h(x) \) and \( g(x) \), then it is certainly a common divisor of \( f(x)h(x) \) and \( g(x) \). Thus, the sets
\[
R = \{\text{common divisors of } h(x) \text{ and } g(x)\}
\]
\[
S = \{\text{common divisors of } f(x)h(x) \text{ and } g(x)\}
\]
are identical. Hence, the monic polynomials of highest degree in \( R \) and \( S \) are identical. Hence \( \text{GCD} (h(x), g(x)) = \text{GCD} (f(x)h(x), g(x)) \). \]

4.3.1 Prove that \( f(x) \) and \( g(x) \) are associates in \( F[x] \) if and only if \( f(x) \mid g(x) \) and \( g(x) \mid f(x) \).
\[
\Rightarrow \text{ Suppose } f(x) \text{ and } g(x) \text{ are associates in } F[x]. \text{ Then there exists a nonzero } c \in F \text{ such that } f(x) = cg(x)
\]
thus \( g(x) \mid f(x) \). But since every nonzero \( c \in F \) is a unit, \( c^{-1} \) also exists and
\[
g(x) = c^{-1}cg(x) = c^{-1}f(x)
\]
so \( f(x) \mid g(x) \).
\[
\Leftarrow \text{ Suppose } f(x) \mid g(x) \text{ and } g(x) \mid f(x). \text{ Then we have nonzero elements } q(x), p(x) \in F[x] \text{ such that }
\]
(6) \[ g(x) = q(x)f(x) \]
(7) \[ f(x) = p(x)g(x) \]
Computing the degrees of both sides of these equations gives us
\[
\deg(g(x)) = \deg(q(x)) + \deg(f(x)) \geq \deg(f(x)) \]
\[
\deg(f(x)) = \deg(p(x)) + \deg(g(x)) \geq \deg(g(x))
\]
Comparing these two inequalities we conclude that
\[
\deg(f(x)) = \deg(g(x))
\]
and
\[
\deg(p(x)) = 0 = \deg(q(x))
\]
Thus, \( p(x) \) and \( q(x) \) must be nonzero constants. Say \( p(x) = c \in F \) and \( q(x) = k \in F \). Then the relations (7) become
\[
g(x) = kf(x) \]
\[
f(x) = qf(x)
\]
which is to say that \( f(x) \) and \( g(x) \) are associates. \]

4.3.2 Prove that \( f(x) \) is irreducible in \( F[x] \) if and only if its associates are irreducible.
\[
\Rightarrow \text{ Suppose that } f(x) \text{ is irreducible. Then its only divisors are nonzero constant polynomials and its associates. Suppose }
\]
\[
g(x) = cf(x)
\]
were an associate of \( f(x) \) that was not irreducible. Then \( g(x) \) would have a factorization
\[
g(x) = r(x)q(x)
\]
in which one factor, say \( r(x) \) is neither a constant nor an associate of \( g(x) \). But then
\[
f(x) = c^{-1}r(x)q(x)
\]
would have a divisor \( r(x) \) that is neither a constant nor an associate of \( f(x) \) \( (r(x) \) is an associate of \( f(x) \) if and only if it is an associate of \( g(x) \)). But this contradicts the hypothesis that \( f(x) \) is irreducible. Hence \( g(x) \) cannot be irreducible.

\(< \) Use the same argument as above, exchanging the roles of \( f(x) \) and \( g(x) \) (i.e., assume an associate \( g(x) \) of \( f(x) \) is irreducible and then conclude that \( f(x) \) is irreducible). ■

4.3.3. If \( p(x) \) and \( q(x) \) are nonassociate irreducibles in \( F[x] \), prove that \( p(x) \) and \( q(x) \) are relatively prime.

Set
\[
d(x) = \gcd(p(x), q(x))
\]
We aim to show that if \( p(x) \) and \( q(x) \) are nonassociate irreducibles then \( d(x) = 1_F \). Suppose \( p(x) \) and \( q(x) \) are nonassociate irreducible polynomials of degree \( m \) and \( n \), respectively:
\[
p(x) = a_m x^m + \cdots + a_1 x + a_0 \quad a_m \neq 0_F \\
q(x) = b_n x^n + \cdots + b_1 x + b_0 \quad b_n \neq 0_F
\]
Now because \( p(x) \) and \( q(x) \) are irreducibles, their only monic divisors are, respectively, \( 1_F \) and \( a_m^{-1} p(x) \); and \( 1_F \) and \( b_n^{-1} q(x) \). Thus,
\[
d(x) \in \{1_F, a_m^{-1} p(x), b_n^{-1} q(x)\}
\]
Suppose \( d(x) = a_m^{-1} p(x) \). Then \( a_m^{-1} p(x) \mid q(x) \). But the only nonconstant monic divisor of \( q(x) \) is \( b_n^{-1} q(x) \).
Hence,
\[
a_m^{-1} p(x) = b_n^{-1} q(x) \quad \Rightarrow \quad p(x) = a_m b_n^{-1} q(x)
\]
so \( p(x) \) and \( q(x) \) are associates. But this contradicts our hypothesis. And the same contradiction would be arise if \( d(x) = b_n^{-1} q(x) \). Hence, we must have
\[
d(x) = \gcd(p(x), q(x)) = 1_F
\]
if \( p(x) \) and \( q(x) \) are nonassociate irreducibles ■

\( \S 4.4 \)

4.4.1. Verify that every element of \( \mathbb{Z}_3 \) is a root of \( f = x^3 - x \in \mathbb{Z}_3 \).

We have
\[
f([0]_3) = [0]_3 - [0]_3 = [0]_3 \\
f([1]_3) = [1]_3 - [1]_3 = [0]_3 \\
f([2]_3) = [2]_3 - [2]_3 = [0]_3
\]
and so every \( a \in \mathbb{Z}_3 \) is a root of \( f \).

4.4.2. Use the Factor Theorem to show that \( f = x^7 - x \) factors in \( \mathbb{Z}_7 \) as
\[
f = x (x - [1]_7) (x - [2]_7) (x - [3]_7) (x - [4]_7) (x - [5]_7) (x - [6]_7)
\]
We first verify that every \( a \in \mathbb{Z}_7 \) is a root of \( f \).
\[
f([0]_7) = [0]_7 - [0]_7 = [0]_7 \\
f([1]_7) = [1]_7 - [1]_7 = [0]_7 \\
f([2]_7) = [128]_7 - [2]_7 = [0]_7 \\
f([3]_7) = [2187]_7 - [7]_7 = [0]_7 \\
f([4]_7) = [16384]_7 - [4]_7 = [0]_7 \\
f([5]_7) = [78125]_7 - [5]_7 = [0]_7 \\
f([6]_7) = [279936]_7 - [6]_7 = [0]_7
\]
Applying Theorem 4.12, we conclude that every polynomial \( x - a, a \in \mathbb{Z}_7 \), is a factor of \( f \). Since \( x - a \) does not divide \( x - b \) unless \( a = b \), we can conclude that

\[
f = x(x - 1)(x - 2)(x - 3)(x - 4)(x - 5)(x - 6)q
\]

for some \( q \in \mathbb{Z}_3[x] \). Comparing degrees and the coefficient of \( x^7 \) on both sides we conclude \( q = 1 \) and the statement then follows. \[ \square \]

4.4.3. If \( a \in F \) is a nonzero root of

\[
f = c_0x^n + \ldots + c_1x + c_0 \in F[x],
\]

show that \( a^{-1} \) is a root of

\[
g = a_0x^n + c_1x^{n-1} + \cdots + c_n.
\]

Well,

\[
0_F = \tilde{f}(a) = c_0a^n + \cdots + c_1a + c_0.
\]

Multiplying both sides by \((a^{-1})^n\), we get

\[
0 = c_n + \cdots + c_1(a^{-1})^{n-1} + c_0(a^{-1})^n = \tilde{g}(a^{-1}).
\]

and so \( a^{-1} \) is a root of \( g \). \[ \square \]

4.4.4. Prove that \( x^2 + 1 \) is reducible in \( \mathbb{Z}_p[x] \) if and only if there exists integers \( a \) and \( b \) such that \( p = a + b \) and \( ab \equiv 1 \pmod{p} \).

\[
\Rightarrow
\]

Suppose \( p = a + b \) with \( ab \equiv 1 \pmod{p} \) and consider the polynomial

\[
([1]_p x + [d]_p)([1]_p x + [b]_p).
\]

Expanding this polynomial we get

\[
(x + [a]_p)(x + [b]_p) = [1]_p x^2 + ([a]_p + [b]_p)x + [a]_p[b]_p = [1]_p x^2 + [a + b]_p x + [ab]_p = [1]_p x^2 + [0]_p x + [1]_p = [1]_p x^2 + [1]_p
\]

and so we have factorized \([1]_p x^2 + [1]_p \) in \( \mathbb{Z}_p[x] \).

\[
\Leftarrow \text{Now suppose } f = [1]_p x^2 + [1]_p \text{ is reducible. Then there must be a nontrivial factorization of } f. \text{ Since } f \text{ has degree 2, the most general form of this factorization is}
\]

\[
[1]_p x^2 + [1]_p = (cx + d)(ex + f)
\]

with \( c, d, e, f \in \mathbb{Z}_p \). Expanding the right hand side of (??) and identifying the coefficients of like powers of \( x \), we find

\[
e c = [1]_p
\]

(10)

\[
cf + de = [0]_p
\]

(11)

\[
df = [1]_p
\]

Let \( a, b \in \mathbb{Z} \) be any integers such that \([a]_p = cf\) and \([b]_p = de\). Then (??) implies

\[
[a]_p + [b]_p = cf + de = [0]_p \Rightarrow a + b \equiv 0 \pmod{p}
\]

and

\[
[a]_p [b]_p = (cf)(de) = (cf)(de) = [1]_p [1]_p = [1]_p \Rightarrow ab \equiv 1 \pmod{p}
\]

4.4.5. Find a polynomial of degree 2 in \( \mathbb{Z}_a[x] \) that has four roots in \( \mathbb{Z}_a \). Does this contradict Corollary 4.13?

Consider

\[
f = [3]_a x^2 + [3]_a x
\]
Then
\[ f ([0]_6) = [0]_6 + [0]_6 = [0]_6 \]
\[ f ([2]_6) = [12]_6 + [6]_6 = [0]_6 \]
\[ f ([3]_6) = [27]_6 + [9]_6 = [0]_6 \]
\[ f ([4]_6) = [48]_6 + [12]_6 = [0]_6 \]
and so \( f \) has four roots. This does not contradict Corollary 4.13, since \( \mathbb{Z}_6 \) is not a field (it is not even an integral domain). \( \blacksquare \)