Solve #15 Solutions

5.1 #1 Is \( f(x) = x^5 - 2x^4 + 4x^3 - 3x + 1 \) congruent to \( g(x) = 3x^4 + 2x^3 - 5x^2 + 2 \) modulo \( p(x) = x^2 + 1 \)?

\[
\begin{align*}
\text{Check if } p(x) & \mid (f(x) - g(x)) : \text{(Long division)} \\
\text{Trick: if it did divide then } i & \text{ is a root of } \\
& f(x) - g(x) = x^5 - 5x^4 + 2x^3 + 5x^2 - 3x - 1 \\
& \text{But } i^5 - 5i^4 + 2i^3 + 5i^2 - 3i - 1 \\
& = i - 5 - 2i - 5 - 3i - 1 
eq 0.
\end{align*}
\]

So, \( f(x) \) is not congruent to \( g(x) \) modulo \( p(x) \).

5.1 #2 Suppose \( p(x) \) is a non-constant polynomial in \( \mathbb{F}[x] \). Prove that any two polynomials are congruent modulo \( p(x) \).

If \( p(x) = c \neq 0 \), then since \( c \in \mathbb{F} \), \( c \neq 0 \), \( c \) is a unit. Thus \( c \mid f(x) \) for every \( f(x) \in \mathbb{F}[x] \) because \( f(x) = c (c^{-1} \cdot f(x)) \).

In particular, \( c \mid (f(x) - g(x)) \) for every \( f(x), g(x) \in \mathbb{F}[x] \).

5.1 #4 Let \( p(x) = x^3 + 2x + 1 \in \mathbb{Z}_3[x] \). Show there are 27 congruence classes modulo \( p(x) \).

Given \( f(x) \in \mathbb{Z}_3[x] \), we conclude (using the division algorithm) to find a representative \([g(x)] \) of \([f(x)]\) such that \( g(x) = 0 \) or degree \( g(x) < 3 \). So \( g(x) = ax^2 + bx + c \) for some \( a, b, c \in \mathbb{Z}_3 \). There are 27 possibilities, these classes are distinct since \( p(x) \) does not divide a polynomial of degree \( ≤ 3 \).
5.1 #6 Let \( \mathbb{F} \) be a field. Describe \( \mathbb{F}[x]/(x-a) \).

By the division algorithm, the classes are represented by polynomials of degree 0 and the zero polynomial. So we see that \( \mathbb{F}[x]/(x-a) \cong \mathbb{F} \).

5.1 #8 Prove or Disprove: If \( \gcd(p(x), k(x)) = 1 \) and \( f(x) k(x) \equiv g(x) k(x) \) (mod \( p(x) \)), then \( f(x) \equiv g(x) \) (mod \( p(x) \)).

This is true. \([k(x)] \) is a unit in \( \mathbb{F}[x]/p(x) \).

5.2 #2 Multiplication table addition tables for \( \mathbb{Z}_3/(x^2+1) \):

\[
\begin{array}{cccc}
0 & 1 & x & x+1 \\
0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 \\
x & 0 & 0 & x \\
x+1 & 0 & 0 & x+1 \\
x & 0 & 0 & x \\
x+1 & 0 & 0 & x+1 \\
x+2 & 0 & 0 & x+2 \\
x & 0 & 0 & x \\
x+1 & 0 & 0 & x+1 \\
x+2 & 0 & 0 & x+2 \\
\end{array}
\]

Selected multiplications:
\[
\begin{align*}
(x+1)(x+1) &= x^2 + 2x + 1 = 2x + 1 \\
(x+1)(x+2) &= x^2 + 3x + 2 = 1 \\
(2x+1)(x+1) &= 2x^2 + 3x + 1 = x^2 \\
(2x+1)(x+2) &= 2x^2 + 5x + 2 = 2x \\
\end{align*}
\]
5.2 #14(b) Why is \([x^2 + x + 1] \not\in \mathbb{Z}_2[x]/(x^3 + 1)\) a unit? What is its inverse?

It is a unit since \(x^2 + 1\) is irreducible over \(\mathbb{Z}_2[x]\) and hence the quotient ring is a field.

To find the inverse, we use the Euclidean algorithm on \(x^2 + 1\) and \(x^2 + 1\):
\[
x^2 + x + 1 = 1 \cdot (x^2 + 1) + x
\]
\[
x^2 + 1 = x \cdot x + 1
\]

\[
\Rightarrow 1 = (x^2 + 1) + (-x)x
\]

\[
1 = (x^2 + 1) + (-x)(x^2 + x + 1)
\]

\[
= (x^2 + 1)(1 + x) + (-x)(x^2 + x + 1)
\]

\[
\left[1\right] = \left[0\right] + \left[-x\right] \left[x^2 + x + 1\right]
\]

So \(\left[-x\right] = \left[2x\right]\) is the inverse of \(\left[x^2 + x + 1\right]\) in \(\mathbb{Z}_2[x]/(x^3 + 1)\).

5.2 #16 Is \(\mathbb{Z}_2[x]/(x^3 + x^2 + 1)\) a field?

\(x^3 + x^2 + 1\) is not irreducible, so it is not a field. (\(x^2 + x + 1\) is a zero divisor)

5.3 #2 done in class

5.3 #6 Find an inverse \(\left[f(x)\right]^{-1}\). So, the equation \(\left[f(x)\right] \left[f_2(x)\right] = \left[f_1(x)\right]\) can be solved for \(f_2(x)\) by multiplying by \(\left[f(x)\right]^{-1}\). (Inverse exists since \(\mathbb{F}[x]/(f(x))\) is a field.)