due April 18 | Homework Set 12 (section 5.1 – 5.2) | Name: _____

When writing a proof, be sure to cite all of the properties, theorems, corollaries, and definitions you use. Be sure to write all of your answers in complete sentences (even the non-proof questions).

1. 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 $ab \equiv 1 \ mod \ p$.

Let p be a prime. Then x^2+1 is reducible in $\mathbb{Z}_p[x]$ exactly when there exist integers a and b such that $x^2+1 = (x+a)(x+b)$. Multiplying these out we have that $x^2+1 = x^2+(a+b)x+ab$. This is true in $\mathbb{Z}_p[x]$ exactly when $a+b \equiv 0 \bmod p$ and $ab \equiv 1 \bmod p$ by theorem 2.3.

Now assuming $(x+a), (x+b) \in \mathbb{Z}_p[x]$, we know that $0 \le a < p$ and $0 \le b < p$. Obviously, $a+b \neq 0$ since that would mean that $a=0=b$, which contradicts $ab \equiv 1 \bmod p$. Hence, $0 < a+b < 2p$. Thus, $a+b = p$ using the definition of congruence.

2. Prove or disprove: If $p(x)$ is relatively prime to $k(x)$ and $f(x)k(x) \equiv g(x)k(x) \ mod \ p(x)$, then $f(x) \equiv g(x) \ mod \ p(x)$.

Let F be a field and $p(x), k(x), f(x), g(x) \in F[x]$, where $p(x)$ is relatively prime to $k(x)$ and $f(x)k(x) \equiv g(x)k(x) \bmod p(x)$.

By definition, $f(x)k(x) - g(x)k(x) = p(x)h(x)$ for some $h(x) \in F[x]$.

Hence $[f(x)-g(x)]k(x) = p(x)h(x)$. Since $\gcd(p(x), k(x)) = 1$, we apply Theorem 4.7 to get that $p(x)$ divides $f(x)-g(x)$. By definition, this means that $f(x) \equiv g(x) \bmod p(x)$.

However, consider the case when $p(x) = x^2+1$, $k(x) = 2x+1$, $f(x) = 3x+2$, and $g(x) = x+3$. Then in $\mathbb{Z}_6[x]$, we have that $f(x)k(x) = x+2$ and $g(x)k(x) = x+1$. Here $f(x)k(x) \not\equiv g(x)k(x) \bmod p(x)$.

3. Answer the following two questions:
   a. List all of the monic irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$.

x^2+1

x^2+x+2

x^2+2x+2

   b. Is $[2x-3]$ a unit in $\mathbb{Q}[x]/\langle x^2-2\rangle$? If so, find its inverse.

$[2x-3]$ is a unit in $\mathbb{Q}[x]/\langle x^2-2\rangle$,

and $[2x-3]^{-1} = [-2x-3]$

4. Let $f(x), g(x)$, and $p(x)$ be in $\mathbb{Q}[x]$. Determine whether $f(x) \equiv g(x) \bmod p(x)$.

   a. $f(x) = x^5 - 2x^4 + 4x^3 - 3x + 1$; $g(x) = 3x^4 + 2x^3 - 5x^2 + 2$; $p(x) = x^2 + 1$

   $f(x) - g(x) = p(x) \cdot (x^3 - 5x^2 + x + 10) + (-4x - 11)$

   Hence $f(x) \not\equiv g(x) \bmod p(x)$.

   b. $f(x) = x^5 + 4x^4 - x^3 + 13x^2 + 20x + 1$; $g(x) = x^3 - x^2 - 8x - 4$; $p(x) = x^2 + 5x + 1$

   $f(x) - g(x) = p(x) \cdot (x^3 - x^2 + 2x + 5)$

   Hence $f(x) \equiv g(x) \bmod p(x)$

5. Write out the multiplication and addition tables for each ring given below. Is the ring a field?

   a. $\mathbb{Z}_2[x]/\langle x^2 + 1\rangle$

+	[0]	[1]	[x]	[x+1]
[0]	[0]	[1]	[x]	[x+1]
[1]	[1]	[0]	[x+1]	[x]
[x]	[x]	[x+1]	[0]	[1]
[x+1]	[x+1]	[x]	[1]	[0]

·	[0]	[1]	[x]	[x+1]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x+1]
[x]	[0]	[x]	[1]	[x+1]
[x+1]	[0]	[x+1]	[x+1]	[0]

The ring $\mathbb{Z}_2[x]/\langle x^2+1\rangle$ is not a field because $[x+1][x+1] = [0]$ or by Theorem 5.10 since $x^2+1 = (x+1)^2$ in $\mathbb{Z}_2[x]$.

   b. $\mathbb{Z}_3[x]/\langle x^2 + 1\rangle$

The ring $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field.

- In the multiplication table, each nonzero element has an inverse.
- x^2+1 is irreducible in $\mathbb{Z}_3[x]$. Then Theorem 5.10, tells us that we have a field.

See attached for tables.