Homework 11
Abstract Algebra
Math 320
Stephen Giang

Problem 5.1.3: How many distinct congruence classes are there modulo x^3+x+1 in $\mathbb{Z}_2[x]$.

By Corollary 5.5, all congruence classes can be written in the form ax^2+bx+c.

$$\begin{array}{rrr} x^2+x+1 & x^2+x & x^2+1 \\ x^2 & x+1 & x \\ 1 & 0 & \end{array}$$

There are 8 distinct congruence classes.

Problem 5.1.4: Show that, under congruence modulo x^3+2x+1 in $\mathbb{Z}_3[x]$, there are exactly 27 distinct congruence classes.

All distinct congruence classes can be written in the form $ax^2 + bx + c$. Because $a, b, c \in \mathbb{Z}_3$, each coefficient can only be either $0, 1,$ or 2. And because there are a total of 3 terms, that can only be one of 3 choices, the amount of combinations is $3^3 = 27$.

Problem 5.1.5: Show that there are infinitely many distinct congruence classes modulo $x^2 - 2$ in $\mathbb{Q}[x]$. Describe them.

All distinct congruence classes can be written in the form $ax + b$. Because $a, b \in \mathbb{Q}$, there are infinitely many choices that a and b can be, meaning there will be infinitely many distinct congruence classes

Problem 5.1.10: Prove or disprove: If $p(x)$ is irreducible in $F[x]$ and $f(x)g(x) \equiv 0_F(\text{mod } p(x))$,then $f(x) \equiv 0_F(\text{mod } p(x))$ or $g(x) \equiv 0_F(\text{mod } p(x))$.

Notice the following:

Solution 5.1.10. $f(x)g(x) \equiv 0_F(\text{mod } p(x)) \to p(x)|f(x)g(x)$

Because $p(x)$ is irreducible, the only factors are its associates and nonzero constants.

If $(p(x), f(x)) = c$, then that makes $f(x) = cq(x)$, with $p(x) \nmid q(x)$. So then we have $p(x)|cq(x)g(x)$. Because $p(x) \nmid q(x)$, then $p(x)|cg(x)$. Meaning that $g(x) \equiv 0_F(\text{mod } p(x))$.

If $(p(x), f(x)) = cp(x)$, then that makes $f(x) = cp(x)q(x)$. That means that $f(x) \equiv 0_F(\text{mod } p(x))$.

□

Problem 5.1.12: If $f(x)$ is relatively prime to $p(x)$, prove that there is a polynomial $g(x) \in F[x]$ such that $f(x)g(x) \equiv 1_F (\text{mod } p(x))$.

Because $f(x)$ is relatively prime to $p(x)$, notice that for some $g(x), u(x) \in F[x]$:

$$\begin{aligned} f(x)g(x) + p(x)u(x) &= 1_F \\ f(x)g(x) - 1_F &= p(x)(-u(x)) \end{aligned}$$

The result is the same as $f(x)g(x) \equiv 1_F (\text{mod } p(x))$ by definition of polynomial modulo.

Problem 5.2.1: Write out the addition and multiplication tables for the congruence class ring $F[x]/p(x)$. In each case, is $F[x]/p(x)$ a field?

$F = \mathbb{Z}_2$, $p(x) = x^3 + x + 1$

$+$	0	1	x	$x+1$	x^2	x^2+x	x^2+1	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+x	x^2+1	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2+x+1	x^2	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2	x^2+x+1	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+1	x^2+x	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	x	1	$x+1$
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	0	$x+1$	1
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	$x+1$	0	x
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	1	x	0

$\times$	0	1	x	$x+1$	x^2	x^2+x	x^2+1	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+x	x^2+1	x^2+x+1
x	0	x	x^2	x^2+x	x^3	x^3+x^2	x^3+x	x^3+x^2+x
$x+1$	0	$x+1$	x^2+x	x^2+1	x^3+x^2	x^3+x	x^3+x^2+x+1	x^3+1
x^2	0	x^2	x^3	x^3+x^2	x^4	x^4+x^3	x^4+x^2	$x^4+x^3+x^2$
x^2+x	0	x^2+x	x^3+x^2	x^3+x	x^4+x^3	x^4+x^2	$x^4+x^3+x^2+x$	x^4+x
x^2+1	0	x^2+1	x^3+x	x^3+x^2+x+1	x^4+x^2	$x^4+x^3+x^2+x$	x^4+1	x^4+x^3+x+1
x^2+x+1	0	x^2+x+1	x^3+x^2+x	x^3+1	$x^4+x^3+x^2$	x^4+1	x^4+x^3+x+1	x^4+x^2+1

This is not a field because not every nonzero element has a multiplicative inverse.

Problem 5.2.7: Determine the rules for addition and multiplication of congruence classes. (In other words, if the product $[ax+b][cx+d]$ is the class $[rx+s]$, describe how to find r and s from a, b, c, d, and similarly for addition.)

$\mathbb{Q}[x]/(x^2-3)$.

Notice: $[x^2] = [3]$, for multiplication:

$$\begin{aligned}(ax+b)(cx+d) &= acx^2 + adx + bcx + bd \\ &= 3ac + adx + bcx + bd \\ &= (ad+bc)x + (3ac+bd)\end{aligned}$$

So we get

$$r = ad + bc \qquad\qquad s = 3ac + bd$$

Notice for addition:

$$(ax+b) + (cx+d) = (a+c)x + (b+d)$$

So we get

$$r = a + c \qquad\qquad s = b + d$$

Problem 5.2.8: Determine the rules for addition and multiplication of congruence classes. (In other words, if the product $[ax+b][cx+d]$ is the class $[rx+s]$, describe how to find r and s from a, b, c, d, and similarly for addition.)

$\mathbb{Q}[x]/(x^2)$.

Notice: $[x^2] = [0]$, for multiplication:

$$\begin{aligned}(ax+b)(cx+d) &= acx^2 + adx + bcx + bd \\ &= adx + bcx + bd \\ &= (ad+bc)x + (bd)\end{aligned}$$

So we get

$$r = ad + bc \qquad\qquad s = bd$$

We can also see that because $[x^2] = [0]$, then $[x] = [0]$. So we can write the product as just bd, where:

$$r = 0 \qquad\qquad s = bd$$

Notice for addition:

$$(ax+b) + (cx+d) = (a+c)x + (b+d)$$

So we get

$$r = a + c \qquad\qquad s = b + d$$

We can also see that because $[x^2] = [0]$, then $[x] = [0]$. So we can write the sum as just $b+d$, where:

$$r = 0 \qquad\qquad s = b + d$$