MTH 310: HW 5

Instructor: Matthew Cha

Due: June 18, 2018

1. Find all irreducible polynomials of degree 5 in $\mathbb{Z}_2[x]$. (*Hint*: There are six of them.)

   Solution. All degree 5 polynomials take the form $\{x^5 + ax^4 + bx^3 + cx^2 + dx + e : a, b, c, d, e \in \mathbb{Z}_2\}$. Thus, there are $2^5 = 32$ degree 5 polynomials in $\mathbb{Z}_2[x]$.

   Any polynomial in $\mathbb{Z}_2[x]$ with a zero constant coefficient has a factor of x and is reducible. Any polynomial with an even number of non-zero coefficients has a root of 1 and thus is reducible by the factor theorem. This leaves us with 8 possible choices: $x^5 + x^3 + 1$, $x^5 + x^2 + 1$, $x^5 + x + 1$, $x^5 + x^4 + x^3 + x^2 + 1$, $x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^3 + x^2 + x + 1$.

   We can check by hand that none of these have a root in $\mathbb{Z}_2$. Moreover, by the degree formula we have that a degree 5 polynomial with no linear factor is reducible if and only if it has exactly one irreducible degree 2 factor and one irreducible degree 3 factor.

   We proved in class that the irreducible factors of degree 2 and 3 are: $x^2 + x + 1$, $x^3 + x + 1$ and $x^3 + x^2 + 1$.

   Thus the following polynomials are reducible:

   $$(x^2 + x + 1)(x^3 + x^2 + 1) = x^5 + x + 1$$
   $$(x^2 + x + 1)(x^3 + x + 1) = x^5 + x^4 + 1.$$

   We are left with 6 irreducible polynomials of degree 5:

   $$\begin{aligned}&x^5 + x^2 + 1\\ &x^5 + x^3 + 1\\ &x^5 + x^4 + x^3 + x^2 + 1\\ &x^5 + x^4 + x^3 + x + 1\\ &x^5 + x^4 + x^2 + x + 1\\ &x^5 + x^3 + x^2 + x + 1\end{aligned}$$

2. **(Hungerford 4.3.21)** Find a non-constant polynomial in $\mathbb{Z}_9[x]$ that is a unit.

   Solution. Recall that $[3]_9[6]_9 = [18]_9 = [0]_9$. We have that

   $$(3x + 1)(6x + 1) = 18x^2 + 9x + 1 = 1 \qquad \text{in} \quad \mathbb{Z}_9[x].$$

   Thus, $3x + 1$ is a unit in $\mathbb{Z}_9[x]$.

3. **(Hungerford 4.4.4)** For what value of k is $x + 1$ a factor of $x^4 + 2x^3 - 3x^2 + kx + 1$ in $\mathbb{Z}_5[x]$.

   Solution. By the factor theorem, if $x + 1$ is a factor if and only if $[-1] = [4]$ is a root. Evaluating the polynomial at $x = [4]$ and setting to 0 gives

   $$\begin{aligned}[0] &= [4]^4 + 2[4]^3 - 3[4]^2 + k[4] + 1\\ &= [1] + [3] + [2] + [4k] + [1]\\ &= [4k + 2].\end{aligned}$$

   Thus, if $5|4k + 2$ then $[4]$ is a root. This occurs for $k = 2$.

4. **(Hungerford 4.4.19)** We say that $a \in F$ is a *multiple root* of $f(x) \in F[x]$ if $(x-a)^k$ is a factor of $f(x)$ for some $k \geq 2$. Prove that $a \in \mathbb{R}$ is a multiple root of $f(x) \in \mathbb{R}[x]$ if and only if a is a root of both $f(x)$ and $f'(x)$, where $f'(x)$ is the derivative of $f(x)$. You may use standard properties of the derivative like the product rule.

   Solution. ($\Longrightarrow$) Let $a \in \mathbb{R}$ be a multiple root of $f(x) \in F[x]$ and write $f(x) = (x-a)^k g(x)$ for some $g(x) \in \mathbb{R}[x]$ and $k \geq 2$. We can calculate the derivative by the product rule

   $$f'(x) = k(x-a)^{k-1}g(x) + (x-a)^k g'(x)$$

   where $k-1 \geq 1$. Thus, $f'(a) = k(a-a)^{k-1}g(x) + (a-a)^k g'(a) = 0$. Therefore a is a root of $f(x)$ and $f'(x)$.

   ($\Longleftarrow$) Suppose a is a root of $f(x)$ and $f'(x)$. By the factor theorem, we can write $f(x) = (x-a)g(x)$ and $f'(x) = (x-a)h(x)$ for some $g(x), h(x) \in \mathbb{R}[x]$. We can compute the derivative by the product rule

   $$f'(x) = g(x) + (x-a)g'(x).$$

   By substitution we conclude that

   $$g(x) + (x-a)g'(x) = (x-a)h(x).$$

   Thus, $x-a|g(x)$. It follows that $f(x) = (x-a)g(x) = (x-a)^2 k(x)$ for some $k(x) \in \mathbb{R}[x]$. Thus, a is a multiple root of $f(x)$.

5. The Factor Theorem as proved in class has many corollaries to it. Read through Corollary 4.17, 4.18, 4.19, and 4.20 in the text and summarize the results.

   Solution. See Hungerford.

6. **Rational Root Test:** Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ where $a_i \in \mathbb{Z}$ for each i. Let $r, s \in \mathbb{Z}$ with $r \neq 0$ and the gcd of $(r, s) = 1$. Show that if $\frac{r}{s}$ is a root, that is, $f(\frac{r}{s}) = 0$ then $r|a_0$ and $s|a_n$.

   Solution. See Hungerford, Theorem 4.21.

7. **(Hungerford 5.1.6)** Let $a \in F$ and $f(x) \in F[x]$.

   (a) Show that $f(x) \equiv f(a) \mod (x-a)$.

   (b) Use (a) to show that $x^3 + 2 \equiv x^4 + 2x^2 + 1 \mod (x-2)$ in $\mathbb{Z}_5$.

   This problem shows that the congruence class of $f(x)$ modulo $x-a$ is determined only by the value of the polynomial when evaluated at a.

   Solution.

   (a) By the Division Algorithm $\exists!\, q(x), r(x) \in F[x]$ such that $f(x) = (x-a)q(x) + r(x)$ with $\deg r(x) = 0$ or $r(x) = 0_F$ and thus, $r(x) = r$ is a constant polynomial in F. Evaluating at a we have that $f(a) = (a-a)q(a) + r = r$. It follows that $[f(x)] = [r] = [f(a)]$ if and only if $f(x) \equiv f(a) \mod (x-a)$.

   (b) Let $f(x) = x^3 + 2$ and $g(x) = x^4 + 2x^2 + 1$ in $\mathbb{Z}_5[x]$. Notice that $f(2) = 0$ and $g(2) = 0$ in $\mathbb{Z}_5[x]$. Thus, by (a) we conclude that $f(x) \equiv 0 \mod (x-2)$ and $g(x) \equiv 0 \mod (x-2)$. By symmetry and transitivity of congruence, we conclude that $f(x) \equiv g(x) \mod (x-2)$.

8. **(Hungerford 5.1.12)** Let $f(x), p(x) \in F[x]$. If $f(x)$ is relatively prime to $p(x)$, prove that there is a $g(x) \in F[x]$ such that $f(x)g(x) \equiv 1_F \mod p(x)$.

   Solution. Suppose $(f(x), p(x)) = 1_F$. Then, there exist $u(x), v(x) \in F[x]$ such that $f(x)u(x) + p(x)v(x) = 1$. Moreover, $f(x)u(x) - 1_F = p(x)v(x) \implies f(x)u(x) \equiv 1_F \mod p(x)$.

9. Write out the addition and multiplication tables for the ring $\mathbb{Z}_2[x]/(x^2+x)$. Is $\mathbb{Z}_2[x]/(x^2+x)$ a field?

Solution. We have that $\mathbb{Z}_2[x]/(x^2+x) = \{[0],[1],[x],[x+1]\}$ where $[f]$ is a congruence class modulo x^2+x.

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

The tables are filed by definition of modular arithmetic. The last entries in the multiplication table must be calculated by division and remainder

$$x^2 = (x^2+x)+x \quad \Longrightarrow \quad [x]^2 = [x]$$
$$(x+1)^2 = (x^2+x)+(x+1) \quad \Longrightarrow [x+1]^2 = [x+1].$$
$$x(x+1) = x^2+x \quad \Longrightarrow [x][x+1] = [0]$$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x]$	$[0]$
$[x+1]$	$[0]$	$[x+1]$	$[0]$	$[x+1]$

.

Since $[x]$ is not a unit, as is made clear by the multiplication table, this implies that $\mathbb{Z}_2[x]/(x^2+x)$ is not a field.

10. In $\mathbb{Z}_2[x]/(x^3+x+1)$, find the multiplicative inverse of $[x+1]$.

Solution. Since x^3+x+1 is irreducible in $\mathbb{Z}_2[x]$ we know that the gcd of $(x^3+x+1, x+1) = 1$. We want to write $1 = (x+1)u(x) + (x^3+x+1)v(x)$ for some $u(x), v(x) \in \mathbb{Z}_2[x]$.

We can apply the Euclidean algorithm as follows

$$x^3+x+1 = (x+1)(x^2+x)+1$$

Therefore, $1 = (x^3+x+1) - (x+1)(x^2+x)$ and we conclude that $[x+1]^{-1} = [x^2+x]$.

11. **(EC–worth .5% of final grade)** Let $p > 2$ be prime and consider the function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ defined by $f(x) = x^2$. Let $f(\mathbb{Z}_p)$ denote the image of f and find the cardinality $|f(\mathbb{Z}_p)|$. [*Hint*: $a \in f(\mathbb{Z}_p)$ if and only if the polynomial $x^2 - a$ is reducible in $\mathbb{Z}_p[x]$.]

Solution. Let's prove the hint: $a \in f(\mathbb{Z}_p)$ if and only if $f(x) = a$ for some $x \in \mathbb{Z}_p$ if and only if $x^2 = a$ or $x^2 - a = 0$. Thus, the polynomial $x^2 - a$ has a root. By the Factor theorem thats if and only if $x^2 - a$ is reducible.

$x^2 - a$ is reducible if and only if, by the factor theorem and degree formula, it has exactly two linear factors. That is, there exist $b, c \in \mathbb{Z}_p$ such that $x^2 - a = (x-b)(x-c) = x^2 - (b+c) + bc$. Equating coefficients we conclude that $b + c = 0$ and $a = bc$ in $\mathbb{Z}_p$. By substitution we have

$$a \equiv b(-b) \mod p$$

Since our logic was exactly reversible using if and only if statements we have shown that

$$f(\mathbb{Z}_p) = \{[a] = [b][-b] : b \in \mathbb{Z}_p\}.$$

If $p > 2$ then $b \equiv -b \mod p$ if and only if $b \equiv 0 \mod p$. Thus, there are exactly $\frac{p-1}{2}$ non-zero pairs $[b], [-b]$ such that $[b][-b] \in f(\mathbb{Z}_p)$ and $[0][0] \in f(\mathbb{Z}_p)$. Therefore, $|f(\mathbb{Z})| = \frac{p-1}{2} + 1 = \frac{p+1}{2}$.