Homework 2 Solutions

Enrique Treviño

February 15, 2019

Most problems below are from Judson.

1. Compute each of the following.

   (a) $(3x^2 + 2x - 4) + (4x^2 + 2)$ in $\mathbb{Z}_5$

   (b) $(3x^2 + 2x - 4)(4x^2 + 2)$ in $\mathbb{Z}_5$

   (c) $(5x^2 + 3x - 2)^2$ in $\mathbb{Z}_{12}$

   Solution 1.

   (a) $2x^2 + 2x - 2 = 2x^2 + 2x + 3 \bmod 5$.

   (b) $12x^4 + 6x^2 + 8x^3 + 4x - 16x^2 - 8 = 2x^4 + 3x^3 + 4x + 2 \bmod 5$.

   (c) $25x^4 + 9x^2 + 4 + 30x^3 - 20x^2 - 12x = x^4 + 6x^3 + x^2 + 4 \bmod 12$.

2. Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$ for each of the following pairs of polynomials.

   (a) $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ and $b(x) = x^2 + x - 2$ in $\mathbb{Z}_7[x]$

   (b) $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ in $\mathbb{Z}_5[x]$

   (c) $a(x) = x^5 + x^3 - x^2 - x$ and $b(x) = x^3 + x$ in $\mathbb{Z}_2[x]$

   Solution 2.

   (a) $6x^4 - 2x^3 + x^2 - 3x + 1 = (6x^2 - 8x + 21)(x^2 + x - 2) + (-40x + 43) = (6x^2 - x)(x^2 + x - 2) + (2x + 1) \bmod 7$.

   (b) $4x^5 - x^3 + x^2 + 4 = (4x^2 - 1)(x^3 - 2) + (4x^2 + 2) \bmod 5$.

   (c) $x^5 + x^3 - x^2 - x = (x^3 + x)(x^2) + x^2 + x \bmod 2$.

3. Find all of the zeros for each of the following polynomials.

   (a) $5x^3 + 4x^2 - x + 9$ in $\mathbb{Z}_{12}$

   (b) $3x^3 - 4x^2 - x + 4$ in $\mathbb{Z}_5$

   (c) $5x^4 + 2x^2 - 3$ in $\mathbb{Z}_7$

   (d) $x^3 + x + 1$ in $\mathbb{Z}_2$

   Solution 3. To find the zeroes of $f(x)$ in $\mathbb{Z}_n$, one need only plug in $x = 0, 1, \ldots, n-1$ to f and see which ones are 0 modulo n.

   (a) It has no zeroes.

   (b) The only zero is $x = 2 \bmod 5$.

   (c) The zeroes are $x = 3, 4 \bmod 7$.

   (d) It has no zeroes ($f(0) = f(1) = 1$.)

4. Find a unit $p(x)$ in $\mathbb{Z}_4[x]$ such that $\deg p(x) > 1$.

   Solution 4. $(2x^2+2x+1)^2 = 4x^4+4x^2+1+8x^3+4x^2+4x = 1 \bmod 4$, so $(2x^2+2x+1)$ is a unit. In fact, $(2x^n+2x^{n-1}+\cdots+2x+1)$ is a unit for any positive integer n. Indeed, let $p(x) = x^n + x^{n-1} + \cdots + x$, then

   $$(2x^n + 2x^{n-1} + \cdots + 2x + 1)^2 = (2p(x)+1)^2 = 4(p(x))^2 + 4p(x) + 1 \equiv 1 \bmod 4.$$

   Therefore, in $\mathbb{Z}_4[x]$ we have units of every degree.

5. Which of the following polynomials are irreducible over $\mathbb{Q}[x]$?

   (a) $x^4 - 2x^3 + 2x^2 + x + 4$
   (b) $x^4 - 5x^3 + 3x - 2$
   (c) $3x^5 - 4x^3 - 6x^2 + 6$
   (d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$

   Solution 5.

   (a) It factors as $(x^2 - 3x + 4)(x^2 + x + 1)$.

   (b) From the rational root theorem, we see that if it has a linear factor it must have a root in $\{-2, -1, 1, 2\}$. But it doesn't have a root from there. Therefore, if it's reducible, it must be factored into the product of two quadratics. From Gauss's Lemma, the quadratics can be written with integer coefficients, i.e.,

   $$x^4 - 5x^3 + 3x - 2 = (x^2 + ax + b)(x^2 + cx + d),$$

   for some integers a, b, c, d. By looking at the coefficients, we get the following equations

   $$\begin{aligned} -5 &= a + c \\ 0 &= b + d + ac \\ 3 &= ad + bc \\ -2 &= bd \end{aligned}$$

   Since b, d are integers, then we have two possibilities $b = -2, d = 1$ or $b = 2, d = -1$ (note: there's also $b = 1, d = -2$ and $b = -1, d = 2$, but those are symmetric), In the first case we get

   $$\begin{aligned} -5 &= a + c \\ 3 &= a - 2c \end{aligned}$$

   Therefore $3c = -8$. But then c is not an integer.
   In the second case

   $$\begin{aligned} -5 &= a + c \\ 3 &= -a + 2c \end{aligned}$$

   Therefore $3c = -2$. But then c is not an integer.
   Therefore, the polynomial is irreducible.

   (c) Use Eisenstein's criterion with the prime 2. Every coefficient besides the leading coefficient is even and the constant term is not a multiple of 4. Therefore, it is irreducible.

   (d) Use Eisenstein's criterion with the prime 3. It divides every coefficient besides the leading coefficient, and 9 does not divide the constant term. Therefore, it is irreducible.

6. Let $f(x)$ be irreducible. If $f(x) \mid p(x)q(x)$, prove that either $f(x) \mid p(x)$ or $f(x) \mid q(x)$.

Solution 6. Suppose that $f(x)$ does not divide $p(x)$. Let $t(x)$ and $r(x)$ be such that $p(x) = f(x)t(x) + r(x)$ with $\deg(r) < \deg(d)$. We know $r(x) \neq 0$ because $f(x)$ does not divide $p(x)$. But then $d(x) = \gcd(f(x), p(x))$ is a divisor of $f(x)$ and $f(x)$ is irreducible, so it must be 1 or $f(x)$. Since it can't be $f(x)$, then it must be 1. Therefore $f(x)$ and $p(x)$ are relatively prime. But then, by Bezout's identity, there exist $a(x), b(x) \in \mathbb{Z}[x]$ such that

$$a(x)f(x) + b(x)p(x) = 1.$$

But then

$$a(x)f(x)q(x) + b(x)p(x)q(x) = q(x).$$

We have $f(x)|a(x)f(x)q(x)$ because $f(x)|f(x)$, and we have $f(x)|b(x)p(x)q(x)$ because $f(x)|p(x)q(x)$. Therefore $f(x)|q(x)$, which is what we wanted to prove.

7. **The Rational Root Theorem.** Let

$$p(x) = a_n x^n a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

where $a_n \neq 0$. Prove that if $p(r/s) = 0$, where $\gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

Solution 7.

$$p(r/s) = a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0.$$

Then

$$a_n r^n + a_{n-1} r^{n-1} s + a_{n-2} r^{n-2} s^2 + \cdots + a_2 r^2 s^{n-2} + a_1 r s^{n-1} + a_0 s^n = 0. \tag{1}$$

Now if you look at the equation modulo s we have

$$a_n r^n \equiv 0 \bmod s.$$

Therefore $s|a_n r^n$. Since $\gcd(r, s) = 1$, then $s|a_n$.

Similarly, looking at (1) modulo r we get

$$a_0 s^n \equiv 0 \bmod r.$$

Therefore $r|a_0$.

8. **Cyclotomic Polynomials.** The polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is called the *cyclotomic polynomial*. Show that $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ for any prime p.

Solution 8. Consider $\Phi_p(x+1)$:

$$\begin{aligned}\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} &= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}.\end{aligned}$$

Every coefficient that's not the leading coefficient has the form $\frac{p!}{k!(p-k)!}$ for some integer $1 \leq k \leq p-1$. Since $k!$ and $(p-k)!$ are not multiples of p but $p!$ is, then $\binom{p}{k}$ is a multiple of p. Therefore, every non-leading coefficient is a multiple of p. Furthermore, the constant term is p which is not a multiple of p^2. By Eisenstein's criterion $\Phi_p(x+1)$ is irreducible, but then $\Phi_p(x)$ is also irreducible.

9. Let $p(x)$ and $q(x)$ be polynomials in $R[x]$, where R is a commutative ring with identity. Prove that $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$.

Solution 9. Suppose $p(x) = a_n x^n + \cdots + a_1 x + a_0$ and $q(x) = b_m x^m + \cdots + b_1 x + b_0$ with $a_n \neq 0$ and $b_m \neq 0$. We may assume without loss of generality that $n \geq m$ because R is commutative. If $n \neq m$, then

$$p(x)+q(x) = a_n x^n + \cdots + a_{m+1}x^{m+1} + (a_m + b_m)x^m + (a_{m-1}+b_{m-1})x^{m-1} + \cdots + (a_1+b_1)x + (a_0+b_0).$$

Since $a_n \neq 0$, then the degree of $p(x)+q(x)$ is n, which is the same as the max of $(\deg(p(x)), \deg(q(x)))$.

If $n = m$, then

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

If $a_n + b_n \neq 0$, then the degree of $p(x)+q(x)$ is n, which is the same as the max of $(\deg(p(x)), \deg(q(x)))$. If $a_n + b_n = 0$, then the degree is at most $n-1$, which is smaller than the max of $(\deg(p(x)), \deg(q(x)))$. In all cases we have

$$\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x)).$$

10. We call a polynomial $p(x) \in \mathbb{Z}_2[x]$ perfect if the sum of its divisors $\sigma(p(x))$ equals $p(x)$. For example $x^2 + x$ is perfect because $\sigma(x^2 + x) = 1 + x + (x + 1) + (x^2 + x) = x^2 + x \bmod 2$. Suppose $p(x)$ is perfect. Prove that $x|p(x)$ if and only if $(x + 1)|p(x)$.

Solution 10. For notation purposes, let $\sigma(f(x))$ be the sum of the divisors of the polynomial $f(x) \in \mathbb{Z}_2[x]$. It is useful to use that σ is multiplicative, i.e., if $a(x), b(x)$ are relatively prime, then $\sigma(a(x)b(x)) = \sigma(a(x))\sigma(b(x))$.

Suppose $x|p(x)$. We want to show that $(x + 1)|p(x)$. Note that this is equivalent to showing $p(1) = 0$.

Consider the factorization of $p(x)$, i.e.,

$$p(x) = x^k p_1(x)^{\alpha_1} p_2(x)^{\alpha_2} \cdots p_r(x)^{\alpha_r}.$$

Since $p(x)$ is perfect, then $\sigma(p(x)) = p(x)$, but also

$$\sigma(p(x)) = \sigma(x^k) \prod_{i=1}^{r} \sigma(p_i(x)^{\alpha_i}) = (1 + x + x^2 + \cdots + x^k) \prod_{i=1}^{r} (1 + p_i(x) + p_i(x)^2 + \cdots + p_i(x)^{\alpha_i}).$$

If k is odd, then $a(x) = 1 + x + x^2 + \cdots + x^k$ satisfies $a(1) = 0$. Therefore, at $x = 1$, $\sigma(p(x)) = 0$, so $p(1) = 0$. This implies $(x+1)|p(x)$ whenever k is odd. Let's assume k is even. We have x^k is relatively prime with $1 + x + \cdots + x^k$, so $x^k|\sigma(\prod_{i=1}^{r} p_i(x)^{\alpha_i})$. Therefore, (from problem 6), there is an i such that $x|\sigma(p_i(x)^{\alpha_i})$.

But that means that when $x = 0$, we have

$$\sigma((p_i(0)^{\alpha_i}) = 1 + p_i(0) + p_i(0)^2 + \cdots + p_i(0)^{\alpha_i} = 0 \bmod 2.$$

Therefore $p_i(0) = 1$ and α_i is odd. If $p_i(1) = 1$, then $\sigma(p_i(1)^{\alpha_i}) = 0$ because α_i is odd. But that means $\sigma(p(1)) = 0$, which means $p(1) = 0$. This is a contradiction.Therefore $p_i(1) = 0$. But $p_i(x)|p(x)$, therefore $p(1) = 0$. Therefore $(x + 1)|p(x)$.

The proof that $(x + 1)|p(x)$ implies $x|p(x)$ is analogous.