Abstract Algebra
Day 29 Class Work Solutions

1. Consider $f(x) = 4x^3 + 5x^2 + 2$ and $g(x) = 3x^2 + 5$ in $\mathbb{Z}_7[x]$.

   (a) Use long division to compute the quotient $q(x)$ and remainder $r(x)$ when dividing $f(x)$ by $g(x)$. Keep in mind that the coefficients are in $\mathbb{Z}_7$.

   Ans: $q(x) = 6x + 4$, $r(x) = 5x + 3$.

   Solution. As shown below, we have $q(x) = 6x + 4$ and $r(x) = 5x + 3$.

$$
\begin{array}{r l}
 & \boxed{6x + 4} \longleftarrow \text{quotient} \\
3x^2 + 5 \,\big)\! & 4x^3 + 5x^2 \qquad\quad + 2 \\
 & -(4x^3 \qquad\quad + 2x) \\
\hline
 & 5x^2 + 5x + 2 \\
 & -(5x^2 \qquad\quad + 6) \\
\hline
 & \boxed{5x + 3} \longleftarrow \text{remainder}
\end{array}
$$

   (b) Verify that your result in part (a) satisfies the division algorithm for polynomials.

   Solution. We have $f(x) = (3x^2 + 5) \cdot q(x) + (5x + 3)$, where $q(x) = 6x + 4$ is the quotient. Note how the degree of the remainder $r(x) = 5x + 3$ is less than the degree of the divisor $g(x) = 3x^2 + 5$, as ensured by the division algorithm.

2. Consider $f(x) \in \mathbb{R}[x]$ where

$$f(x) = (x - 2) \cdot (7432x^{3914} - 652x^{1842} + 37x^{953} + 6x^{75} - 4321x^{59} + 1023).$$

   Explain why $f(2) = 0$.

   Solution. With $q(x) = 7432x^{3914} - 652x^{1842} + 37x^{953} + 6x^{75} - 4321x^{59} + 1023$, we have

$$f(2) = (2 - 2) \cdot q(2) = 0 \cdot q(2) = 0.$$

   Here, $q(2)$ is some (really big) real number.

3. Let $f(x) \in \mathbb{R}[x]$ and suppose $x - 2$ is a factor of $f(x)$, i.e., $f(x) = (x - 2) \cdot q(x)$ for some $q(x) \in \mathbb{R}[x]$. Explain why $f(2) = 0$.

   Solution. We have $f(2) = (2 - 2) \cdot q(2) = 0 \cdot q(2) = 0$. Here, $q(2)$ is some real number.

4. Let $f(x) = 4x^3 - 9x^2 + 5x - 6 \in \mathbb{R}[x]$.

   (a) Compute $f(2)$ and verify that $f(2) = 0$.

   Solution. We have $f(2) = 4 \cdot 2^3 - 9 \cdot 2^2 + 5 \cdot 2 - 6 = 32 - 36 + 10 - 6 = 0$.

   (b) What does your result in part (a) say about how $f(x)$ factors?

   Solution. $x - 2$ is a factor of $f(x)$, i.e., $f(x) = (x - 2) \cdot q(x)$ for some $q(x) \in \mathbb{R}[x]$.

   (c) Use long division to compute the quotient $q(x)$ and remainder $r(x)$ when dividing $f(x)$ by $x - 2$. Explain how this confirms your answer from part (b).

   ← What *should* $r(x)$ be?

   Solution. We have $q(x) = 4x^2 - x + 3$ and $r(x) = 0$, so that $f(x) = (x - 2) \cdot q(x)$. I'll leave the long division computation to you!

5. **Prove:** Let $f(x) \in \mathbb{R}[x]$. If $f(2) = 0$, then $f(x) = (x-2) \cdot q(x)$ for some $q(x) \in \mathbb{R}[x]$. ← Converse of Problem #3.

   Hint: Use the division algorithm for polynomials to write $f(x) = (x-2) \cdot q(x) + r(x)$. What can you say about the remainder $r(x)$?

   PROOF. Assume $f(2) = 0$. By the division algorithm, there exist $q(x)$, $r(x) \in \mathbb{R}[x]$ such that $f(x) = (x-2) \cdot q(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg(x-2)$. Since $\deg(x-2) = 1$, we conclude that $r(x)$ is a constant polynomial, possibly 0. Let $r(x) = \alpha$ for some $\alpha \in \mathbb{R}$, so that $f(x) = (x-2) \cdot q(x) + \alpha$. Solving for α, we obtain $\alpha = f(x) - (x-2) \cdot q(x)$. Substituting $x = 2$ and recalling that $f(2) = 0$, we obtain

   $$\alpha = f(2) - (2-2) \cdot q(2) = 0 - 0 \cdot q(2) = 0.$$

   Thus $\alpha = 0$, which implies $f(x) = (x-2) \cdot q(x)$. ■

6. Consider $f(x) = 5x^{672} + 2x^{359} + 4x^{101} + x^{77} + 3x^{23} + 6$ in $\mathbb{Z}_7[x]$.

   (a) Show that $x - 1$ is a factor of $f(x)$. **Hint:** Compute $f(1)$.

   Solution. Since $1^k = 1$ for all k, we have $f(1) = 5+2+4+1+3+6 = 21 = 0$, where the equality $21 = 0$ occurs in $\mathbb{Z}_7$. Thus, $f(1) = 0$ so that $x - 1$ is a factor of $f(x)$.

   (b) Show that $x + 1$ is *not* a factor of $f(x)$.

   Solution. Since $(-1)^k = 1$ when k is even and $(-1)^k = -1$ when k is odd, we obtain

   $$f(-1) = 5 \cdot 1 + 2 \cdot (-1) + 4 \cdot (-1) + (-1) + 3 \cdot (-1) + 6 = 1,$$

   so that $f(-1) \neq 0$. Thus, $x - (-1)$, or equivalently $x + 1$, is *not* a factor of $f(x)$.

7. (a) Find the remainder when $f(x) = 5x^{451} + 11x^{274} + 1$ is divided by $x - 1$ in $\mathbb{Z}_{13}[x]$.

   Hint: Use the division algorithm for polynomials.

   Solution. By the division algorithm, there exist $q(x)$, $r(x) \in \mathbb{Z}_{13}[x]$ such that $f(x) = (x-1) \cdot q(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg(x-1)$. Since $\deg(x-1) = 1$, we note that $r(x)$ is a constant polynomial, possibly 0. Let $r(x) = \alpha$ for some $\alpha \in \mathbb{Z}_{13}$, so that $\alpha = f(x) - (x-1) \cdot q(x)$. Setting $x = 1$, we obtain $\alpha = f(1) - (1-1) \cdot q(1) = f(1) - 0 \cdot q(1) = f(1)$. Thus, $\alpha = f(1) = 5 \cdot 1^{451} + 11 \cdot 1^{274} + 1 = 5 + 11 + 1 = 17 = 4$, where the equality $17 = 4$ occurs in $\mathbb{Z}_{13}$. Therefore, the remainder is the constant polynomial $r(x) = \alpha = 4$.

   (b) Find the remainder when x^{50} is divided by $x + 2$ in $\mathbb{Z}_5[x]$. **Ans:** Remainder = 4.

   Solution. Proceeding as in part (a), we find that the remainder is the constant polynomial $r(x) = \alpha$ where $\alpha = (-2)^{50} \in \mathbb{Z}_5$. To compute $(-2)^{50}$ or 3^{50} in $\mathbb{Z}_5$, we note that $3^4 = 1 \pmod 5$. Therefore,

   $$3^{50} = 3^{4 \cdot 12 + 2} = (3^4)^{12} \cdot 3^2 = 1^{12} \cdot 3^2 = 4 \pmod 5.$$

   Hence, the remainder is $r(x) = \alpha = 4$.

8. (a) Find $p(x)$, $q(x) \in \mathbb{Z}_{10}[x]$, both with degree 1, such that $p(x) \cdot q(x) = x + 7$. ← Bonus fun!

   (b) What if $p(x)$ and $q(x)$ must each have degree greater than 1? Do such polynomials exist in $\mathbb{Z}_{10}[x]$? If so, find them. If not, explain why not.

9. Let $f(x) = x^3$ and $g(x) = 2x$ in $\mathbb{Z}[x]$.

   (a) Explain why there does *not* exist $q(x)$, $r(x) \in \mathbb{Z}[x]$ such that $x^3 = 2x \cdot q(x) + r(x)$, with either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

   Solution. Suppose for contradiction that such $q(x), r(x) \in \mathbb{Z}[x]$ exist. Since $\deg g(x) = 1$, we know that $r(x)$ is a constant polynomial, possibly 0. So, let $r(x) = m$ for some $m \in \mathbb{Z}$. For the equation $x^3 = 2x \cdot q(x) + r(x)$ to be true, $q(x)$ must be a quadratic, i.e., $q(x) = ax^2 + bx + c$ for some integers a, b, c. Thus, we have $x^3 = 2x \cdot (ax^2 + bx + c) + m$, so that $x^3 = 2ax^3 + 2bx^2 + 2cx + m$. Matching the coefficients of x^3, we get $1 = 2a$, which cannot occur in $\mathbb{Z}$. Thus, $q(x)$ and $r(x)$ cannot exist.

   (b) Does your answer in part (a) contradict the division algorithm for polynomials?

   Ans: No. (Why not?)

   Solution. No, because the division algorithm (for polynomials) requires that the coefficients of the polynomials involved be in a field. Recall that $\mathbb{Z}$ is an integral domain but not a field, since not every non-zero integer has a multiplicative inverse.

Definition. A ring element r is said to be *nilpotent* if $r^n = 0$ for some positive integer n.

← In any ring, 0 is nilpotent, since $0^1 = 0$.

Example: $3 \in \mathbb{Z}_{81}$ is nilpotent, because $3^4 = 0$ in $\mathbb{Z}_{81}$.

---

10. (a) Find all nilpotent elements of $\mathbb{Z}_9$.

   Ans: 0, 3, and 6.

   Solution. 0, 3, and 6.

   (b) Find all nilpotent elements of $\mathbb{Z}_{10}$; of $\mathbb{Z}_{12}$; of $\mathbb{Z}_{36}$.

   Solution.

   - $\mathbb{Z}_{10}$: 0 only.
   - $\mathbb{Z}_{12}$: 0 and 6.
   - $\mathbb{Z}_{36}$: 0, 6, 12, 18, 24, and 30.

   (c) Any conjectures about which $\mathbb{Z}_m$ has nonzero nilpotent elements?

11. In the polynomial ring $\mathbb{Z}_4[x]$, 1 and 3 are units and 0 and 2 are nilpotent elements.

   ← Do you see why?

   (a) In $\mathbb{Z}_4[x]$, find five more units and five more nilpotent elements.

   (b) Explain why $\mathbb{Z}_4[x]$ has infinitely many units and infinitely many nilpotent elements.