Abstract Algebra
Day 35 Class Work

1. Consider the element $8 \in \mathbb{Z}_{29}$. Since 8 and 29 are relatively prime, the GCD theorem says there exist x, $y \in \mathbb{Z}$ such that $8x + 29y = 1$. ← i.e., $\gcd(8, 29) = 1$.

   (a) Find integers x and y such that $8x + 29y = 1$. **Hint:** $88 + (-87) = 1$.

   (b) Using your answer in part (a), find the multiplicative inverse of 8 in $\mathbb{Z}_{29}$.

2. Consider the element $8 + \langle 29 \rangle$ in the quotient ring $\mathbb{Z}/\langle 29 \rangle$.

   (a) Using your result in Problem #1(a), complete the following:

   $$(8 + \langle 29 \rangle) \cdot (\_\_ + \langle 29 \rangle) = 8 \cdot \_\_ + \langle 29 \rangle = 1 + \langle 29 \rangle, \text{ because } \_\_\_\_\_ \in \langle 29 \rangle.$$ **Ans:** $8 \cdot 11 - 1 \in \langle 29 \rangle$.

   Recall: In $\mathbb{Z}/\langle 29 \rangle$, $\alpha + \langle 29 \rangle = \beta + \langle 29 \rangle$ if and only if...

   (b) Let $a + \langle 29 \rangle$ be a *nonzero* element of $\mathbb{Z}/\langle 29 \rangle$, so that $a \notin \langle 29 \rangle$. Explain why a and 29 are relatively prime, so that there exist x, $y \in \mathbb{Z}$ such that $ax + 29y = 1$. ← $a \notin \langle 29 \rangle$ means a is *not* a multiple of 29.

   (c) Using your result in part (b), complete the following:

   $$(a + \langle 29 \rangle) \cdot (\_\_ + \langle 29 \rangle) = a \cdot \_\_ + \langle 29 \rangle = 1 + \langle 29 \rangle, \text{ because } \_\_\_\_\_ \in \langle 29 \rangle.$$ **Ans:** $a \cdot x - 1 \in \langle 29 \rangle$.

   (d) Anita says, "In (b) and (c), we proved that $\mathbb{Z}/\langle 29 \rangle$ is a field." What might she mean?

   (e) Elizabeth wonders, "But how did we use the fact that 29 is prime?"

Here is the GCD theorem *for polynomials*.

> Let $f(x)$, $g(x) \in F[x]$. If $f(x)$ and $g(x)$ are relatively prime, then there exist $p(x)$, $q(x) \in F[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$.

Note: $f(x)$ and $g(x)$ are *relatively prime* if they don't share a non-constant common factor.

---

3. Fix $g(x) = x^2 + 1 \in \mathbb{Z}_7[x]$.

   (a) Compute $g(0)$, $g(1)$, $g(2)$, ..., $g(6)$ in $\mathbb{Z}_7$.

   (b) Using your work in part (a), explain why $g(x)$ is unfactorable in $\mathbb{Z}_7[x]$.

   (c) Based on our conjectures thus far, is $\mathbb{Z}_7[x]/\langle g(x) \rangle$ a field? ← It should be!

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

   (a) Explain why $f(x)$ and $g(x)$ are relatively prime. Problem #3 should help. ← i.e., $g(x)$ is unfactorable.

   (b) By the GCD theorem, let $p(x)$, $q(x) \in \mathbb{Z}_7[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$. Explain why $(f(x) + \langle g(x) \rangle) \cdot (p(x) + \langle g(x) \rangle) = 1 + \langle g(x) \rangle$ in $\mathbb{Z}_7[x]/\langle g(x) \rangle$.

   Note: In other words, $f(x) + \langle g(x) \rangle$ has a multiplicative inverse $p(x) + \langle g(x) \rangle$.

5. **Prove:** Fix $g(x) \in F[x]$. If $g(x)$ is unfactorable, then $F[x]/\langle g(x) \rangle$ is a field. ← Here, F is a field.

   Hint: Let $\alpha(x) \in F[x]$ such that $\alpha(x) + \langle g(x) \rangle \neq 0 + \langle g(x) \rangle$. Then...

   - Explain why $\alpha(x)$ and $g(x)$ are relatively prime.
   - Show that $\alpha(x) + \langle g(x) \rangle$ has a multiplicative inverse.

6. (a) Once again, let $g(x) = x^2+1 \in \mathbb{Z}_7[x]$. How many elements does $\mathbb{Z}_7[x]/\langle g(x)\rangle$ contain? **Ans:** 49 elements.

   (b) Find a prime p and a polynomial $g(x) \in \mathbb{Z}_p[x]$ such that the quotient ring $\mathbb{Z}_p[x]/\langle g(x)\rangle$ is a field containing 121 elements. Explain your reasoning.

   (c) Same as part (b), but with 343 elements. **Ans:** $x^3 + 2 \in \mathbb{Z}_7[x]$.

7. As in Problem #4, let $f(x) = 3x + 5$ and $g(x) = x^2 + 1$ in $\mathbb{Z}_7[x]$.

   (a) Find $p(x)$, $q(x) \in \mathbb{Z}_7[x]$ such that $f(x) \cdot p(x) + g(x) \cdot q(x) = 1$.

   Hint: Use polynomials $p(x)$ and $q(x)$ such that $\deg p(x) = 1$ and $\deg q(x) = 0$.

   (b) Find the multiplicative inverse of $(3x + 5) + \langle x^2 + 1\rangle$ in $\mathbb{Z}_7[x]/\langle x^2 + 1\rangle$. ← You already found it!

8. Consider the quotient ring $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

   (a) Explain why $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ is a field.

   (b) Find the multiplicative inverse of $(7x + 4) + \langle x^2 - 2\rangle$ in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

   Hint: Observe that $x^2 + \langle x^2 - 2\rangle = \boxed{?} + \langle x^2 - 2\rangle$ in $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

9. **(Some Food for Thought)** Let $f(x) = x^2 + 1$.

   (a) Explain why $f(x)$ is unfactorable in $\mathbb{Z}_3[x]$.

   (b) Explain why $f(x)$ is factorable in $\mathbb{Z}_5[x]$.

   (c) Explain why $f(x)$ is unfactorable in $\mathbb{Z}_7[x]$.

   (d) Explain why $f(x)$ is unfactorable in $\mathbb{Z}_{11}[x]$.

   (e) Explain why $f(x)$ is factorable in $\mathbb{Z}_{13}[x]$.

   (f) Determine if $f(x)$ is factorable or unfactorable in $\mathbb{Z}_{17}[x]$, $\mathbb{Z}_{19}[x]$, $\mathbb{Z}_{23}[x]$, and $\mathbb{Z}_{29}[x]$.

   (g) For which primes p is $f(x)$ factorable in $\mathbb{Z}_p[x]$? unfactorable in $\mathbb{Z}_p[x]$?