Session 9, July 19
Decimal Expansion Revisited
Euclid's Algorithm for Polynomials

1. For each n, find the order of 10 (mod n). Then, using long division, find the decimal expansion of $\frac{1}{n}$. Explain what is going on and why.

   (a) $n = 7$ (b) $n = 11$ (c) $n = 13$

   (d) $n = 8$ (e) $n = 39$ (f) $n = 5$

   (g) $n = 41$ (h) $n = 73$

2. Predict the period of the repeating decimal for each of the following fractions. What are the possibilities?

   (a) $\frac{1}{29}$ (b) $\frac{1}{15}$ (c) $\frac{1}{21}$ (d) $\frac{1}{107}$

3. How are unit groups, order, and Fermat's Little Theorem related to the decimal expansion problems that you did on Days 1–3? Be specific as possible, using concrete examples.

4. Write $\frac{1}{7}$ as "decimals" in base three and in base seventeen. (*Reminder*: You cannot write "7" in base three. Also, in base seventeen, you may want to introduce additional letters to represent the single digits for "10", "11", etc.) Compare your results with Problem 1(a). Explain.

5. (a) What were the orders of elements in $\mathbf{U}_7$?
   (b) Write $\frac{1}{7}$ as "decimals" in base eight, nine, ten, eleven, twelve, and thirteen.
   (c) What is the period of $\frac{1}{7}$ in base forty-five? (By the way, what is the "decimal" expansion of $\frac{1}{7}$ in base forty-five?)

6. Remember the decimal expansion of $\frac{k}{13}$ $(1 \leq k \leq 12)$ from Day 1? The repeating digits formed two separate circles of length 6.

   (a) Why are *two* circles formed?
   (b) Suppose we want one big circle of length 12. In which base should we compute the "decimal" expansion of $\frac{1}{13}$?

7. In a Reader Reflection in the *Mathematical Teacher* (March, 1997), Walt Levisee reports on a nine year old student David Cole who conjectured that if the period of the decimal (i.e., base 10) expansion of $\frac{1}{n}$ is $n - 1$, then n is prime. Prove David's conjecture.

In *Disquisitiones Arithmeticae*, published in 1801, Gauss conjectured that there are infinitely many primes p that have David's property that the decimal expansion of $\frac{1}{p}$ has period $p - 1$. This is still an open question.

8. Restate Gauss' conjecture using the notion of "order." For extra credit, prove Gauss' conjecture.

9. The decimal expansion of $\frac{1}{7}$ is $0.\overline{142857}$. Now, split the repeating digits in half and add them together:

$$142 + 857 = 999.$$

Try this with $\frac{1}{13}$, $\frac{1}{73}$, and other repeating decimals of $\frac{1}{p}$ that have even periods. Any conjectures?

Hint: $\frac{1}{7} + \frac{6}{7} = 0.\overline{9}$, right?

Here are some interesting polynomial problems. Keep in mind that $\mathbf{Z}_n[x]$ is the set of all polynomials in x with coefficients in $\mathbf{Z}_n$.

10. Consider the factorization of $x^4 - 1$ in $\mathbf{Z}_5[x]$.

$$\begin{aligned}
x^4 - 1 &= (x^2-1)(x^2+1) \\
&= (x+1)(x-1)(x^2+1) \\
&= (x-4)(x-1)(x^2-4) && \text{(Why?)} \\
&= (x-4)(x-1)(x+2)(x-2) \\
&= (x-4)(x-1)(x-3)(x-2) && \text{(Why?)} \\
&= (x-1)(x-2)(x-3)(x-4)
\end{aligned}$$

Factor $x^6 - 1$ in $\mathbf{Z}_7[x]$. Factor $x^{10} - 1$ in $\mathbf{Z}_{11}[x]$. How is this related to Fermat's Little Theorem?

11. In $\mathbf{Z}_3[x]$, consider $f(x) = x^2 + 2x + 1$ and $g(x) = 2x^2 + x + 2$. Calculate $f(x) + g(x)$ and $f(x) \cdot g(x)$.

12. Multiply $2x^3 + 3x^2 + x + 4$ by $3x^2 + 2x + 2$ in $\mathbf{Z}_5[x]$. Multiply the same two polynomials in $\mathbf{Z}_6[x]$. In each case, compare the degrees of the factors with the degree of the product. In what ways are $\mathbf{Z}_5[x]$ and $\mathbf{Z}_6[x]$ different? Explain.

    Note: degree of $f(x) = x^3 + 4x - 2$ is 3
    degree of $f(x) = x + 2$ is 1
    degree of $f(x) = 17$ is 0
    degree of $f(x) = 0$ is undefined

13. Use long division to find the quotient and the remainder when $x^3 + 2x^2 + 3x + 2$ is divided by $x + 4$ in $\mathbf{Z}_5[x]$. How is the remainder "smaller" than the divisor $(x + 4)$? Explain.

14. Consider $f(x) = x^3 + 4x^2 + 3x + 1$ and $g(x) = 2x + 1$. Divide $f(x)$ by $g(x)$ in $\mathbf{Z}_5[x]$ and in $\mathbf{Z}_6[x]$.

15. Does some form of division algorithm hold in $\mathbf{Z}_5[x]$? in $\mathbf{Z}_6[x]$? in $\mathbf{Z}_{17}[x]$? Any conjectures?

16. (Further exploration) Consider $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ and $g(x) = x^2 - 2x + 3$ in $\mathbf{Z}_5[x]$.

    (a) Use Euclid's algorithm (?!) to find the GCD of $f(x)$ and $g(x)$.

    (b) See if the method used in $\mathbf{Z}$ can be used to find a solution (X, Y) of the "Diophantine" equation

$$f(x)X(x) + g(x)Y(x) = \gcd(f(x), g(x)).$$