1. I briefly mentioned solving linear equations in the system \( \mathbb{Z}/m\mathbb{Z} \). Experiment with this. Try solving
\[
19X = 7
\]
in \( \mathbb{Z}/31\mathbb{Z} \) for example. There are several ways to approach this. One is to try to use multiplicative inverses much as you do in algebra. Do that. Then consider the equation
\[
12X = 9
\]
in \( \mathbb{Z}/51\mathbb{Z} \). The inverse trick doesn’t work here! Try to solve it anyway. What do you notice about the solution set?

2. I’ll just reiterate problem 4 from the previous problem set. If you didn’t get a chance to dig much into that, this is the perfect place to explore.

3. In exploring quadratic congruences like \( X^2 = a \) in \( \mathbb{Z}/p\mathbb{Z} \) you may have noticed that the solutions tend to come in pairs just like in the real numbers. Plus/minus pairs. This is related to a familiar feature of polynomials: they don’t have any more roots than the degree. Is this generally true over \( \mathbb{Z}/m\mathbb{Z} \)? That is, suppose you have a polynomial
\[
f(X) = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0
\]
where \( a_i \in \mathbb{Z}/m\mathbb{Z} \) for all \( i \) and \( a_d \neq \overline{0} \), so \( f(X) \) has degree \( d \). Is it true that \( f \) has at most \( d \) roots in \( \mathbb{Z}/m\mathbb{Z} \)? As usual, experiment with this. Write down some polynomials. Think about examples you’ve seen before, maybe. Also, consider special cases - like what happens if \( m \) is prime? Does the situation improve in that case?

4. Here’s a fun one. Let \( \varphi(m) \) denote the number of units in \( \mathbb{Z}/m\mathbb{Z} \). Looking at the remainders description of classes and the relatively prime characterization of units, \( \varphi(m) \) can also be realized as the number of positive integers not exceeding \( m \) and relatively prime to \( m \).

It’s easy to compute \( \varphi(m) \) for small \( m \) just by writing the table out and counting units. That unfeasible for large \( m \). We’ll have a tool that will help give a formula for \( m \) soon (The Chinese Remainder Theorem), but it turns out there’s a clever workaround using probability of all things.

What’s the probability that a class in \( \mathbb{Z}/m\mathbb{Z} \) is a unit? Clearly it’s
\[
\frac{\varphi(m)}{m}
\]
Now let’s compute this probability a different way. The class \( \overline{a} \) is a unit if and only if \( a \) fails to be divisible by each prime dividing \( m \). This is a bunch of independent conditions on the class \( \overline{a} \), and they’re independent because of the Fundamental Theorem of Arithmetic! Now use tools of probability to try to find another formula for this probability and ultimately a formula for \( \varphi(m) \).