Systems of Congruence Equations and the Order of an Element
Pre-class, Week 7

Suppose we want to solve two or more congruence equations instead of solving one equation. For example, $2x \equiv 3 \pmod 5$ and $3x \equiv 5 \pmod 7$. This is a system of congruence equations and we will learn a method to solve such systems in the class activity.

1. Consider a special case of a system like

$$x \equiv 2 \pmod 5 \text{ and } x \equiv 2 \pmod 7$$

What are the possible solutions for x? Is the solution unique? Unique modulo some number? Justify your answer.

2. Consider the system

$$x \equiv 2 \pmod 3 \text{ and } x \equiv 3 \pmod 7$$

Does the system have a solution? If so, is it unique? Unique modulo some number? Justify.

3. Consider the system

$$x \equiv 3 \pmod 4 \text{ and } x \equiv 2 \pmod 6$$

Does the system have a solution? If so, is it unique? Unique modulo some number? Justify.

Over $\rightarrow$

In addition to solving linear congruences, we might also be interested in congruence equations involving powers of x greater than or equal to 2. It turns out that these equations are inherently related to the algebraic structure of the residue classes.

4. We will work with modulo 9 in this problem. Consider each of the residue classes a modulo 9. For each a, find the smallest positive k such that $a^k \equiv 1 \pmod 9$. For example, for $a = 4$, the smallest k is 3.

If k is the smallest positive integer such that $a^k \equiv 1 \pmod n$, we say that k is the **order** of a modulo n. Note that if $k|h$ for some h, then $a^h \equiv 1 \pmod n$ as well. From your observations in the above problem, we observed that it makes sense to define the order only for a such that $\gcd(a, n) = 1$.

5. Find the order of 2 modulo 13.

6. Suppose we know $5^{96} \equiv 1 \pmod{357}$. How can you use this information to help find the order of 5 modulo 357?