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.

$x = 5k+2 = 7j+2$

$x-2 = 5k = 7j$

1. Consider a special case of a system like

$$(1) \quad x \equiv 2 \pmod 5 \text{ and } x \equiv 2 \pmod 7 \quad (2)$$

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

$7 \cdot 5$

guess

<35

(1)	(2)
2	2
7	9
12	16
17	23
22	30
27	37
32	
37	

$x \equiv 2 \ \% 35$

$35 = 7 \cdot 5$

$= \mathrm{lcm}(5,7)$

2. Consider the system

$$(1) \quad x \equiv 2 \pmod 3 \text{ and } x \equiv 3 \pmod 7 \quad (2)$$

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

$7 \cdot 3 = 21$

(1)	(2)
2	3
5	10
8	17
11	24
14	
17	
20	
23	

$x \equiv 17 \ \% 21$

$21 = \mathrm{lcm}(3,7)$

3. Consider the system

$$(1) \quad x \equiv 3 \pmod 4 \text{ and } x \equiv 2 \pmod 6 \quad (2)$$

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

$\mathrm{lcm}(4,6) = 12$

$x = 4k+3 = 6j+2$

$4k+1 = 6j$

$4(k+1)-3 = 6j$

$0, 4, 8, 12$

$\xrightarrow{\div 6} 0, 4, 2, 0$

$\boxed{\text{no } 3}$

(1)	(2)
3	2
7	8
11	12
15	18

no Solution

Over →

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.

a	0	1	2	3	4	5	6	7	8
k	X	1	6	X	3	6	X	3	2

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.

12

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?

order of 5 modulo 357 divides 96

$96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$
$= 2^5 \cdot 3$

We could check all 12 factors

If we do, we see the order is 48.