Multiplicative Dynamics Modulo n (Exploration)

Katherine E. Stange, University of Colorado Boulder

This is an in-class worksheet exploration. I expect you to have completed the video “Modular Arithmetic: In Motion” and the associated follow-up worksheet. We will use the results from that worksheet.

1. Take a look at the examples of multiplicative dynamics you’ve done, and compare with your groupmates, to catch errors.

2. Do more examples if needed, in order to fill in the blanks to make this a conjecture that you, as a group, agree that you believe:

   Conjecture 1. *The multiplicative dynamics of a modulo n is bijective if and only if a and n satisfy* ____________________.

3. For each example you have done, verify the conjecture in the following table. The examples from the Video Follow-Up worksheet are entered in the table’s first two columns, so look back to that sheet for the data.

a	n	bijective according to conjecture (yes/no)	bijective in example (yes/no)
5	6		
2	6		
2	7		
2	9		
2	10		
3	7		
3	9		
3	10		

4. Carefully choose three more examples designed to test your conjecture, and add the results to your table. (Farm out the work in your group; you can also use multiplication tables for lookup.)

5. Here are a series of statements about the multiplicative dynamics of a modulo n.

   (a) The function $f(x) = ax$ is bijective.

   (b) The function $f(x) = ax$ is injective.

   (c) The element a can be cancelled modulo n. In other words, if $ax \equiv ay \pmod{n}$ then $x \equiv y \pmod{n}$.

   (d) If $az \equiv 0 \pmod{n}$ then $z \equiv 0 \pmod{n}$.

   (e) The elements a and n are coprime.

   Our goal will be to show that each step is equivalent to the next step. I’ve broken it down into steps.

   (a) Explain why 5a implies 5b.

(b) Explain why 5b implies 5a. Look back to your Video Follow-Up worksheet for the reason.

(c) Explain why 5b is equivalent to 5c.

(d) Explain why 5c implies 5d. (Hint: apply 5c with a specific x and y in terms of z.)

(e) Explain why 5d implies 5c. (Hint: apply 5d with a specific z in terms of x and y.)

(f) Explain why 5e implies 5d. To see this, rewrite the congruences in 5d in terms of divisibility.

(g) Explain why 5d implies 5e. To see this, let $g = \gcd(a, n)$ and set $z = n/g$ in 5d. This should imply $g = 1$.

6. Has what you've done above proved Conjecture 2? If not, correct the conjecture or fill in what's missing in the proof.